ETSI TS 123 558 V18.9.0 (2025-01)

5G;
Architecture for enabling Edge Applications
(3GPP TS 23.558 version 18.9.0 Release 18)

Reference
RTS/TSGS-0623558vi90

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

Edge Computing is a network architecture concept that enables cloud computing capabilities and service environments, which are deployed close to the UE. It promises several benefits such as lower latency, higher bandwidth, reduced backhaul traffic and prospects for new services compared to the cloud environments. This technical specification provides application layer architecture and related procedures for enabling edge applications over 3GPP networks.

1 Scope

The present document specifies the application layer architecture, procedures and information flows necessary for enabling edge applications over 3GPP networks. It includes architectural requirements for enabling edge applications, application layer architecture fulfilling the architecture requirements and procedures to enable the deployment of edge applications.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2".

[3] 3GPP TS 23.502: "Procedure for the 5G System (5GS); Stage 2".

[4] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[5] 3GPP TS 29.122: "T8 reference point for northbound Application Programming Interfaces (APIs)".

[6] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[7] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[8] 3GPP TS 36.305: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN".

[9] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[10] 3GPP TS 38.305: "NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[11] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[12] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[13] 3GPP TS 23.434: "Service enabler architecture layer for verticals; Functional architecture and information flows; Stage 2".

[14] 3GPP TS 23.286: "Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows ".

[15] ETSI ISG MEC ETSI GS MEC 003 V2.1.1 (2019-01), "Multi-access Edge Computing (MEC); Framework and Reference Architecture"

[16] Void

[17] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[18] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[19] GSMA PRD OPG.02 Operator Platform Telco Edge Requirements version 4.0, available at https://www.gsma.com/futurenetworks/resources/operator-platform-telco-edge-requirements/

[20] 3GPP TS 23.548: "5G System Enhancements for Edge Computing".

[21] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[22] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".

[23] 3GPP TS 33.558: "Security aspects of enhancement of support for enabling edge applications".

[24] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[25] 3GPP TS 32.257: "Telecommunication management;Charging management;Edge computing domain charging".

[26] 3GPP TS 23.433: "Service Enabler Architecture Layer for Verticals (SEAL); Data Delivery enabler for vertical applications".

[27] 3GPP TR 23.958: "Edge Application Standards in 3GPP and Alignment with External Organizations".

[28] 3GPP TS 23.436: "Functional architecture and information flows for Application Data Analytics Enablement Service"

[29] 3GPP TS 24.558: "Enabling Edge Applications; Protocol specification"

[30] 3GPP TS 29.558: "Enabling Edge Applications; Application Programming Interface (API) specification"

[31] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Application Context: A set of data about the Application Client that resides in the Edge Application Server.

Application Context Relocation: Refers to the end-to-end service continuity procedure described in clause 8.8.

Application Context Transfer: Refers to the transfer of the Application Context between the source Edge Application Server and the target Edge Application Server, which is a part of the service continuity procedure described in clause 8.8.

Application Server: Application software resident in the cloud performing the server function.

Associated EES: One or multiple EES(s) which support all bundled EAS within the same EDN, and each EES of the associated EES(s) serving all or part of EAS list of the bundle EAS.

Common EAS: An EAS which can serve a group of UEs using the same application.

Common EES: An EES which has a Common EAS registered with it.

Edge Computing: A concept, as described in 3GPP TS 23.501 [2], that enables operator and 3rd party services to be hosted close to the UE's access point of attachment, to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

Edge Computing Service Provider: A mobile network operator or a 3rd party service provider offering Edge Computing service.

Edge Data Network: A local Data Network that supports the architecture for enabling edge applications.

EEC Context: A set of data about the Edge Enabler Client that resides in the Edge Enabler Server.

Edge Enabler Layer: Refers to the overall functionality provided by the entities such as Edge Enabler Client, Edge Enabler Server, Edge Configuration Server and Cloud Enabler Server, in support of applications as per the architecture defined in clause 6.

Edge Hosting Environment: An environment providing support required for Edge Application Server's execution.

Instantiable EAS: EAS type for which the instantiation trigger from the Edge Enabler Layer is considered by the ECSP management system for instantiating EAS.

Main EAS: An EAS in EAS bundle taking the role of controlling the ACR for EAS bundle in network side decided ACR scenario.

Partner ECS: Refers to an ECS deployed by a partner ECSP.

Partner ECSP: An ECSP with whom there is a service level agreement for resource sharing for roaming or federation or both.

3.2 Symbols

None.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AC	Application Client
ACID	Application Client Identification
ACR	Application Context Relocation
ACT	Application Context Transfer
AEF	API Exposing Function
AF	Application Function
APN	Access Point Name
ASP	Application Service Provider
CAPIF	Common API Framework
CAS	Cloud Application Server
CES	Cloud Enabler Server
DN	Data Network
DNAI	Data Network Access Identifier
DNN	Data Network Name
H-ECS	Home Edge Configuration Server
H-EES	Home Edge Enabler Server
EAS	Edge Application Server
EASID	Edge Application Server Identification
ECI	Edge and Cloud Interworking
ECS	Edge Configuration Server
ECS-ER	Edge Configuration Server – Edge Repository
ECSP	Edge Computing Service Provider
EDN	Edge Data Network
EEC	Edge Enabler Client
EECID	Edge Enabler Client Identification
ENS	Edge Node Sharing
ETSI	European Telecommunications Standards Institute
EEL	Edge Enabler layer

EES	Edge Enabler Server
EESID	Edge Enabler Server Identification
FQDN	Fully Qualified Domain Name
GPSI	Generic Public Subscription Identifier
GSM	Global System for Mobile Communications
GSMA	GSM Association
LADN	Local Area Data Network
MEC	Multi-access Edge Computing
NEF	Network Exposure Function
OP	Operator Platform
OPG	Operator Platform Group
PCF	Policy Control Function
PSA	PDU Session Anchor
S-EAS	Source Edge Application Server
S-EES	Source Edge Enabler Server
SCEF	Service Capability Exposure Function
SEAL	Service Enabler Layer Architecture
SMF	Session Management Function
SSID	Service Set Identifier
T-EAS	Target Edge Application Server
T-EES	Target Edge Enabler Server
TAI	Tracking Area Identity
URSP	UE Route Selection Policy
V-ECS	Visited Edge Configuration Server
V-EES	Visited Edge Enabler Server

4 Overview

4.1 General

For edge computing, it is essential that the ACs are able to locate and connect with the most suitable application server available in the EDN, depending on the needs of the application. The edge enabler layer exposes APIs to support such capabilities.

The edge computing capabilities supported by 3GPP are illustrated in the figure 4.1-1.

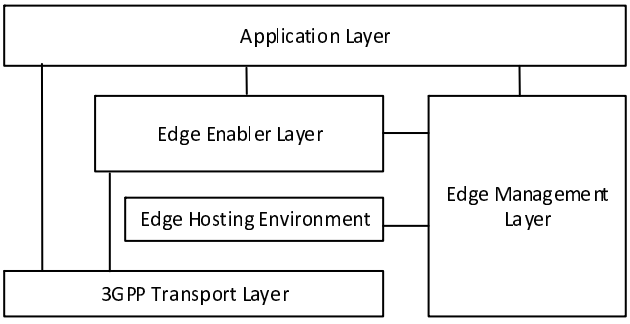

Figure 4.1-1: Overview of 3GPP edge computing

The application layer is a consumer of 3GPP specified edge computing capabilities. The 3GPP edge computing capabilities are typically organized as follows:

- Edge enabler layer, specified in this specification;
- Edge hosting environment, details of which are outside the scope of 3GPP;
- 3GPP transport layer, specified in 3GPP TS 23.401 [11] and 3GPP TS 23.501 [2]; and
- Edge management layer, specified in 3GPP TS 28.538 [22].

Following clauses provide an overview of the features of edge enabler layer.

The edge computing features defined in this specification are applicable to PLMN(s) and to SNPN(s) as 3GPP transport layer. In this specification, when PLMN is mentioned, it is also applicable for SNPN unless stated otherwise.

4.2 Service provisioning

Service provisioning procedures supply the information required by the UE to access the edge services. The procedure takes UE's location, service requirements, service preferences and connectivity information into account to provide the required configuration. Service provisioning procedures are specified in clause 8.3.

4.3 Registration

Registration procedures specified in clause 8.4, allow entities (e.g. UE and Application Server) in the edge enabler layer to provide information about itself to other entities of the edge enabler layer.

4.4 EAS discovery

EAS discovery procedures enable the UE to obtain information about suitable EASs of interest (specified as discovery filters) in the EDN. EAS discovery procedures are specified in clause 8.5.

4.5 Capability exposure to EAS and EEC

The edge enabler layer exposes services towards the EASs and EECs. The exposed capabilities include the services of the Edge Enabler Layer and the re-exposed and enhanced services of the 3GPP core network. The capabilities exposed by the edge enabler layer are specified in clause 8.6 and the 3GPP network capability exposure is specified in clause 8.7. Other application layer capabilities like application enabler services and SEAL services may be exposed via edge enabler layer as per CAPIF as illustrated in Annex A.4.

The edge enabler layer also supports for an EAS to expose its Service APIs (i.e., EAS Service APIs) towards the other EASs via CAPIF as specified in 3GPP TS 23.222 [6] by deploying CAPIF core function within the EES to support publish and discovery of EAS Service APIs. The details are provided in Annex A.5.4.

4.7 Security

The edge enabler layer supports secure communication amongst the enabler layer entities. Clause 8.11 provides details on EEC authentication and authorization.

4.8 Dynamic EAS instantiation triggering

The Edge Enabler Layer can interact with the ECSP management system to trigger instantiation of a suitable EAS as per application needs. Details of the EAS instantiation triggering are specified in clause 8.12.

4.6 Support for service continuity

When a UE moves to a new location, different EASs can be more suitable for serving the UE. When no suitable EAS can be found for serving the UE, the service session may transition to a CAS. Such transitions can result from a non-mobility event also, requiring support from the edge enabler layer to maintain the continuity of the service. Support for service continuity provides several features for minimizing the application layer service interruption by replacing the S-EAS connected to the AC in the UE, with a T-EAS or CAS. Support for service continuity is further specified in clause 8.8.

4.9 Charging

The general architecture and principles applicable for charging of Edge enabling services provided by an ECSP to an ASP, is specified in 3GPP TS 32.240 [24].

5 Architectural requirements

5.1 General

This clause specifies architectural requirements for enabling edge applications in different functional aspects.

5.2 Architectural requirements

5.2.1 General requirements

5.2.1.1 General

This clause specifies general requirements for the architecture.

5.2.1.2 Requirements

[AR-5.2.1.2-a] The application layer architecture shall support deployment of EAS(s) and AC(s) with or without modifications compared to their existing deployments.

[AR-5.2.1.2-b] The application layer architecture shall support different deployment models in conjunction with an operator's 3GPP network.

[AR-5.2.1.2-c] The application layer architecture shall be compatible with the 3GPP network system.

5.2.2 Edge configuration data

5.2.2.1 General

This clause specifies the requirements for edge configuration data.

5.2.2.2 Requirements

[AR-5.2.2.2-a] The application layer architecture shall provide mechanisms to provide configuration parameters to an authorized EEC to access the EES(s).

5.2.3 Registration

5.2.3.1 General

This clause specifies the requirements for EEC, EAS and EES registration.

5.2.3.2 EEC registration

[AR-5.2.3.2-a] The application layer architecture shall provide mechanisms for an EEC to register onto the EES.

[AR-5.2.3.2-b] The application layer architecture shall provide mechanisms for an EEC to de-register from the EES.

[AR-5.2.3.2-c] The application layer architecture shall provide mechanisms for the EES to detect an abnormal termination of an EEC registration.

5.2.3.3 EAS registration

[AR-5.2.3.3-a] The application layer architecture shall provide mechanisms for an EAS to register to the EES.

[AR-5.2.3.3-b] The application layer architecture shall support EAS exposing its availability, which varies with time, location, etc.

[AR-5.2.3.3-c] The application layer architecture shall provide mechanisms so that the EASs are uniquely identifiable.

[AR-5.2.3.3-d] The application layer architecture shall provide mechanisms for an EAS to de-register from the EES.

[AR-5.2.3.3-e] The application layer architecture shall provide mechanisms for the EES to detect an abnormal termination of an EAS registration.

5.2.3.4 EES registration

[AR-5.2.3.4-a] The application layer architecture shall provide mechanisms for an EES to register onto the ECS.

[AR-5.2.3.4-b] The application layer architecture shall support EES to publish EAS information on the ECS.

[AR-5.2.3.4-c] The application layer architecture shall support EES to update the published EAS information on the ECS.

[AR-5.2.3.4-d] The application layer architecture shall provide mechanisms for an EES to de-register from the ECS.

[AR-5.2.3.4-e] The application layer architecture shall provide mechanisms for the ECS to detect an abnormal termination of an EES registration.

5.2.4 EAS discovery

5.2.4.1 General

This clause specifies the requirements for EAS discovery.

5.2.4.2 Requirements

[AR-5.2.4.2-a] The application layer architecture shall provide mechanisms for an EEC to discover available EASs.

[AR-5.2.4.2-b] The application layer architecture shall provide relevant configuration information of the EASs to the EEC, in order to enable communication between ACs and the EASs.

5.2.5 Capability exposure to EASs

5.2.5.1 General

This clause specifies the requirements for capability exposure to EAS.

5.2.5.2 Requirements

[AR-5.2.5.2-a] The application layer architecture shall support exposure of 3GPP network's capabilities to the EASs.

[AR-5.2.5.2-b] The application layer architecture shall support exposure of EES's capabilities to the EASs.

[AR-5.2.5.2-c] The application layer architecture shall support exposure of EAS's capabilities to the other EASs.

5.2.6 Security

5.2.6.1 General

This clause specifies the security requirements.

5.2.6.2 Requirements

[AR-5.2.6.2-a] The application layer architecture shall provide mechanisms for the Edge Computing Service Provider to authorize the usage of Edge Computing services by the EEC.

[AR-5.2.6.2-b] The application layer architecture shall provide mechanisms for the Edge Computing Service Provider to authorize the usage of Edge Computing services by the EASs.

[AR-5.2.6.2-c] Communication between the functional entities of the application layer architecture shall be protected.

[AR-5.2.6.2-d] The authentication and authorization for the use of Edge Computing services shall support the deployment where the functional entities providing the Edge Computing services are in the same trust domain as the 3GPP system, different trust domains or both.

[AR-5.2.6.2-e] The application layer architecture shall support the use of either 3GPP credentials or application specific credentials or both for different deployment needs, for the communication between the UE and the functional entities providing the Edge Computing service.

[AR-5.2.6.2-f] The application layer architecture shall support mutual authentication and authorization check between clients and servers or servers and servers that interact.

[AR-5.2.6.2-g] The application layer architecture shall support EASs to obtain user's authorization in order to access to user's sensitive information (e.g. user's location).

[AR-5.2.6.2-h] The application layer architecture shall provide mechanisms to support privacy protection of the user.

NOTE 1: Security and privacy related procedures are specified in 3GPP TS 33.558 [23].

NOTE 2: EAS obtained user consent requirement in [AR-5.2.6.2-g] is not supported in the current release.

5.2.7 Subscription service

5.2.7.1 General

This clause specifies the requirements for a subscription service.

5.2.7.2 Requirements

[AR-5.2.7.2-a] The application layer architecture shall provide subscription and notification mechanisms enabling an EEC to receive changes in dynamic information of EASs from an EES.

[AR-5.2.7.2-b] The application layer architecture shall provide subscription and notification mechanisms enabling an EEC to receive changes in availability of EASs from an EES.

[AR-5.2.7.2-c] The application layer architecture shall provide subscription and notification mechanisms enabling an EEC to receive changes in EES's information and availability status (e.g. EES endpoint change or EES is about to become unavailable due to overload, maintenance window, etc.) from an ECS.

[AR-5.2.7.2-d] The application layer architecture shall provide subscription and notification mechanisms enabling an EAS to receive information about relevant changes in AC(s) information of a UE.

[AR-5.2.7.2-e] The application layer architecture shall provide subscription and notification mechanisms enabling an EAS to receive information about relevant reports in UE location.

[AR-5.2.7.2-f] The application layer architecture shall provide subscription and notification mechanisms enabling to receive changes in service continuity.

5.2.8 Traffic management

5.2.8.1 General

This clause specifies the requirements for traffic management.

5.2.8.2 Requirements

[AR-5.2.8.2-a] The application layer architecture shall support AF influence on traffic routing over N6 interface.

[AR-5.2.8.2-b] The application layer architecture should be able to monitor the network status (e.g. traffic volume, throughput, network load, etc.) that may impact the application KPIs.

5.2.9 Lifecycle management

5.2.9.1 General

This clause specifies the requirements for lifecycle management.

5.2.9.2 Requirements

[A.5.2.9.2-a] The application layer architecture shall support interactions with a lifecycle management system.

5.2.10 Edge application KPIs

5.2.10.1 General

This clause specifies the requirements for edge application KPIs.

5.2.10.2 Requirements

[AR-5.2.10.2-a] The application layer architecture shall provide mechanisms for the EAS to publish its KPIs or application level requirements when available (e.g. upon new application on-boarding).

[AR-5.2.10.2-b] The application layer architecture shall provide mechanisms for the EAS to update its KPIs or application level requirements.

5.2.11 Service continuity

5.2.11.1 General

This clause specifies the requirements for service continuity.

5.2.11.2 Requirements

[AR-5.2.11.2-a] The application layer architecture shall provide mechanisms to support service continuity such that the Application Context with a S-EAS is transferred to a T-EAS.

[AR-5.2.11.2-b] The application layer architecture shall provide mechanisms to support service continuity such that the Application Context with an EAS is transferred to a CAS.

[AR-5.2.11.2-c] The application layer architecture shall provide mechanisms to support service continuity such that the Application Context with a CAS is transferred to an EAS.

6 Application layer architecture

6.1 General

This clause provides the overall architecture description:

- Clause 6.2 describes the functional architecture and corresponding considerations to support roaming and federation scenarios as well as interactions with cloud services;

- Clause 6.3 describes the functional entities;
- Clause 6.4 describes the service-based interfaces;
- Clause 6.5 describes the reference points;
- Clause 6.6 describes the cardinality of functional entities and reference points; and
- Clause 6.7 describes the capabilities exposed for enabling edge applications.

6.2 Architecture

This clause describes the architecture for enabling edge applications in the following representations:

- A service-based representation, where the Edge Enabler Layer functions (e.g. ECS) enable other authorized Edge Enabler Layer functions (e.g. EES) to access their services. This representation also includes point-to-point reference points where necessary;
- A service-based representation as specified in 3GPP TS 23.501 [2], where the Network Functions (e.g. NEF) enable authorized Edge Enabler Layer functions (e.g. ECS) i.e. Application Functions, to access their services;
- A service-based representation, where the Core Network Northbound APIs as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], are utilized by authorized Edge Enabler Layer functions via CAPIF core function specified in 3GPP TS 23.222 [6]; and
- A reference point representation, where existing interactions between any two functions (e.g. EES, ECS) is shown by an appropriate point-to-point reference point (e.g. EDGE-6, EDGE-7).

Edge Enabler Layer functions shown in the service-based representation of the edge architecture shall only use service-based interfaces for their interactions.

Figure 6.2-1 illustrates the service based representation of architecture for enabling edge applications.

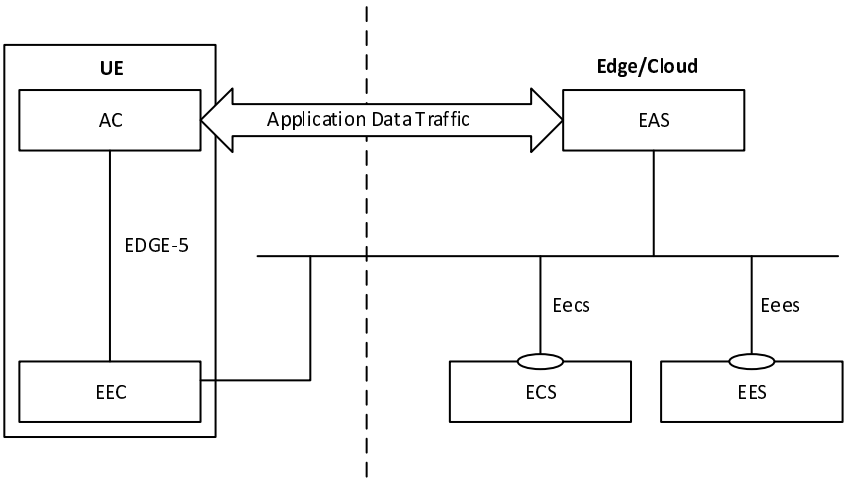

Figure 6.2-1: Architecture for enabling edge applications - service-based representation

NOTE: The EEC function and EAS function in figure 6.2-1 do not expose any service to the other functions.

The mechanisms for service discovery in the service-based representation depicted in figure 6.2-1 are as follows:

- The EES discovers the ECS via pre-configuration or by using CAPIF as specified in 3GPP TS 23.222 [6];
- The EAS discovers the EES via pre-configuration or by using CAPIF as specified in 3GPP TS 23.222 [6];
- The EAS discovers the other EAS(s) as specified in clause 8.8.3.2;
- The EEC discovers the ECS as specified in clause 8.3.2; and
- The EEC discovers the EES via service provisioning as specified in clause 8.3.3.

Figure 6.2-2 illustrates the service-based representation for utilization of the 5GS network services based on the 5GS SBA specified in 3GPP TS 23.501 [2].

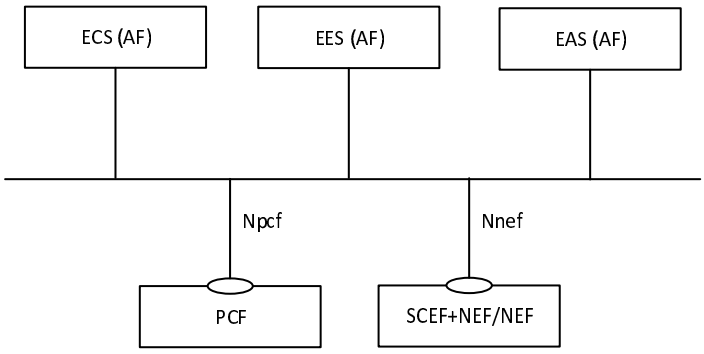

Figure 6.2-2: Utilization of 5GS network services based on the 5GS SBA – service based representation

The ECS, EES and EAS act as AFs for consuming network services from the 3GPP 5G Core Network entities over the Service Based Architecture specified in 3GPP TS 23.501 [7].

Figure 6.2-3 illustrates the service-based representation for utilization of the Core Network (5GC, EPC) northbound APIs via CAPIF.

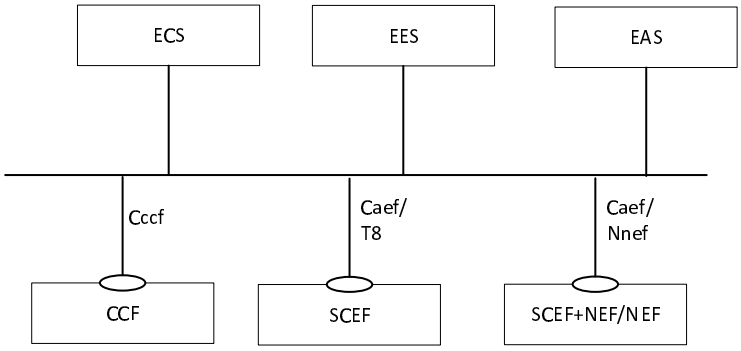

Figure 6.2-3: Utilization of Core Network Northbound APIs via CAPIF – service based representation

The ECS, EES and EAS act as authorized API invoker to consume services from the Core Network (5GC, EPC) northbound API entities like SCEF, NEF, SCEF+NEF which act as API Exposing Function as specified in 3GPP TS 23.222 [6].

The mechanism for northbound APIs discovery using the service-based interfaces depicted in figure 6.2-3 is as specified in 3GPP TS 23.222 [6].

Figure 6.2-4 illustrates the reference point representation of the architecture for edge enabling applications.

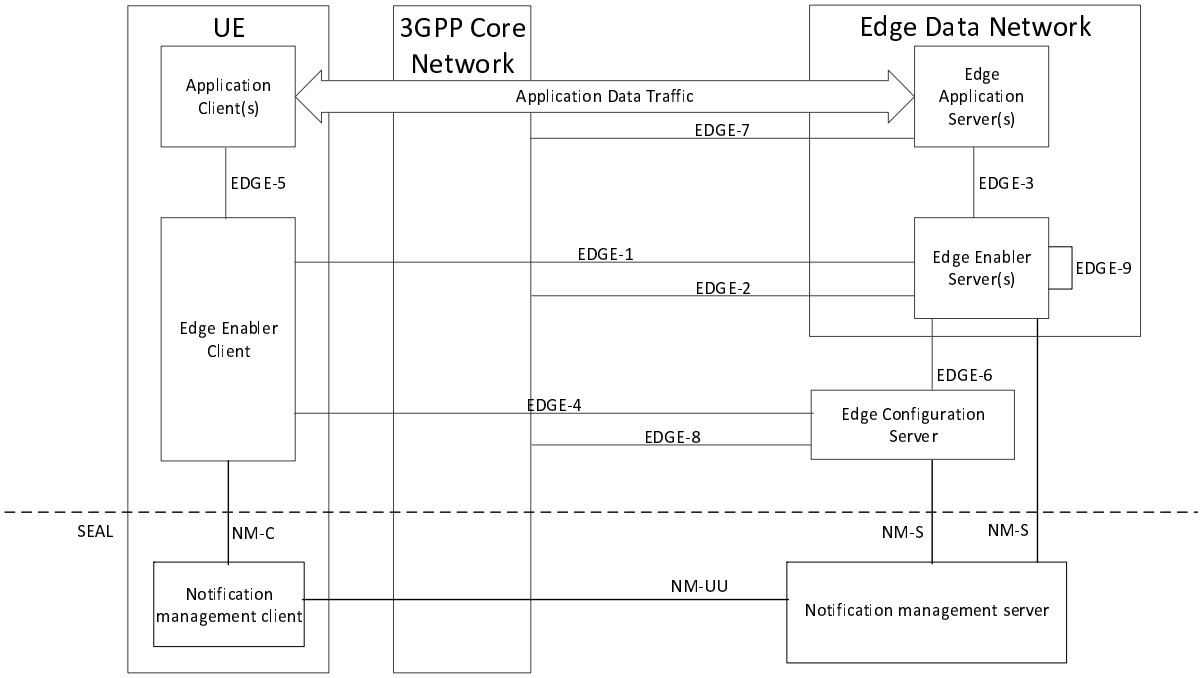

Figure 6.2-4: Architecture for enabling edge applications - reference points representation

The EDN is a local Data Network. EAS(s) and the EES are contained within the EDN. The ECS provides configurations related to the EES, including details of the EDN hosting the EES. The UE contains AC(s) and the EEC. The EAS(s), the EES and the ECS can interact with the 3GPP Core Network. When SEAL notification management service is used, the EES and the ECS interact with the SEAL notification management server and the SEAL EEC interacts with SEAL Notification management client.

6.2a Architecture for Roaming support

6.2a.1 General

This clause describes the architectures for roaming UEs. To support UEs that are roaming, the EEL uses ECSs provided in HPLMN and VPLMN. The EEC in the UE obtains edge enabler layer services from V-ECS and V-EES. EDGE-10 reference point is used between the H-ECS and the V-ECS. Two roaming models are supported for edge enabling applications:

- Local breakout (LBO)roaming architecture; and
- Home routed (HR) roaming architecture.

In both architecture options, the EDN is located in the V-PLMN and is accessed via an LBO or HR-SBO session.

NOTE: H-ECS, H-EES and V-ECS, V-EES can be provided by the same ECSP.

6.2a.2 Local breakout roaming architecture: Local breakout to access H-ECS

Figure 6.2a.2-1 shows the roaming architecture for enabling edge applications as the reference point representation when the local breakout (LBO) PDU Session is used for routing EDGE-4 traffic between the EEC and the H-ECS.

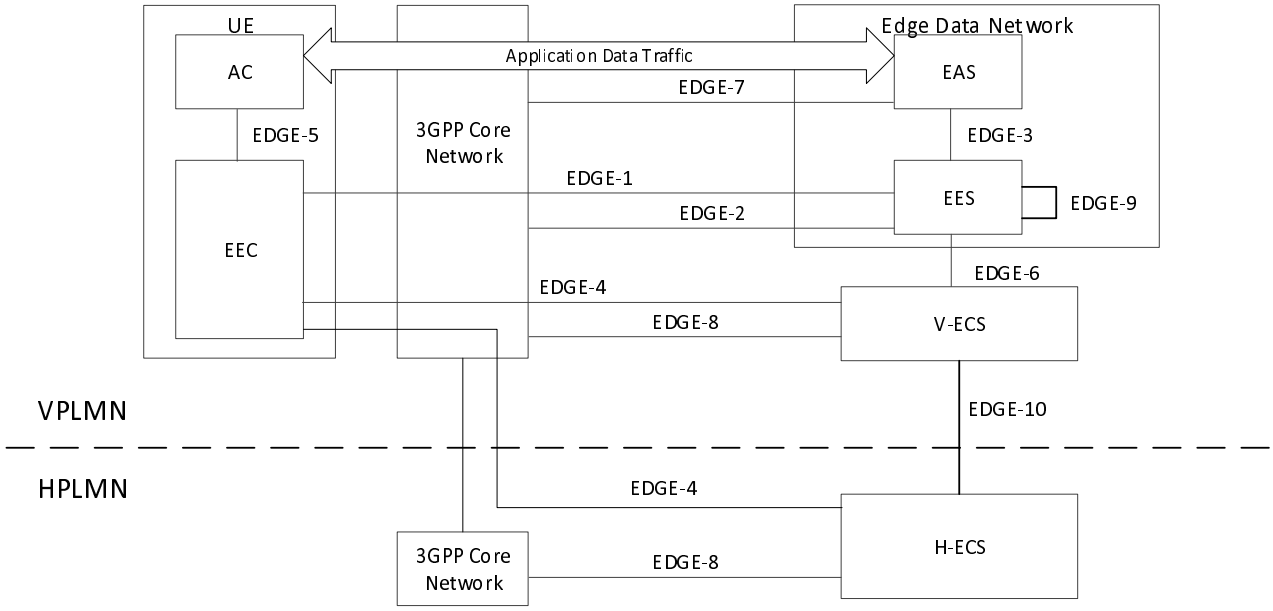

Figure 6.2a.2-1: Architecture for enabling edge applications for local breakout roaming scenarios

6.2a.3 Home-routed EDGE-4 access to H-ECS

Figure 6.2a.3-1 shows the roaming architecture for enabling edge applications as the reference point representation when the home routed (HR) PDU Session is used for routing EDGE-4 traffic between the EEC and the H-ECS.

The traffic toward the EDN of the VPLMN (i.e. EDGE-1 traffic and application data traffic) is not routed via the HPLMN while the traffic between the EEC and H-ECS is routed via VPLMN toward HPLMN. Such a local access to the EDN of the VPLMN in the scenario is supported when a home routed session breakout (HR-SBO) PDU Session is used as described in clause 6.7 of 3GPP TS 23.548 [20].

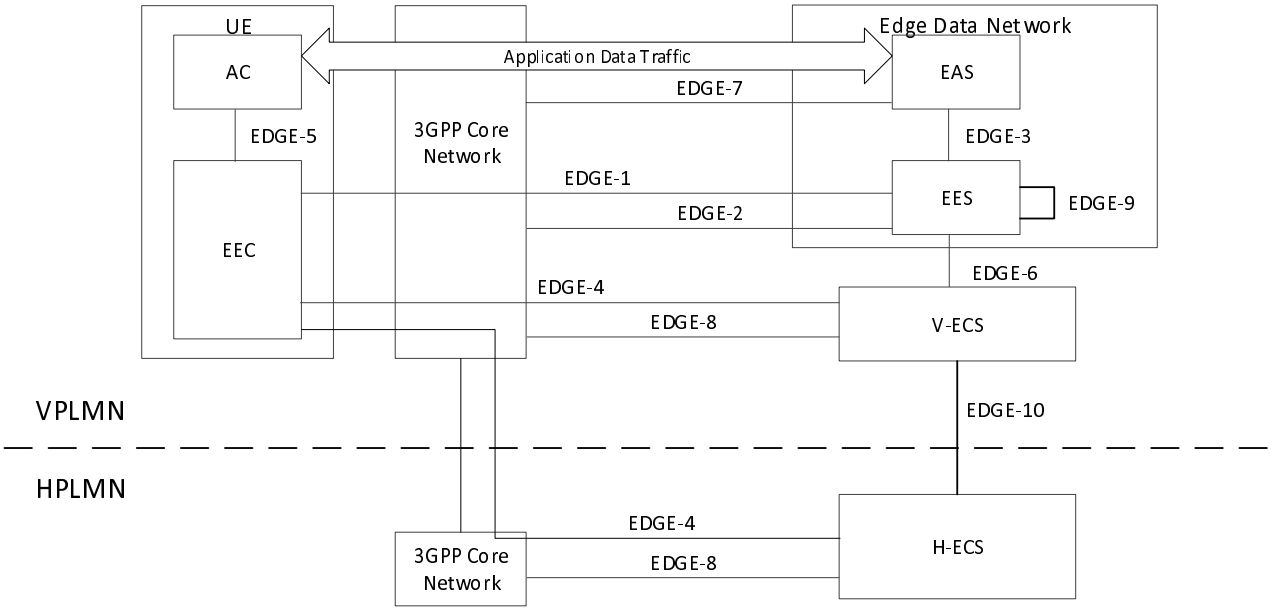

Figure 6.2a.3-1: Architecture for enabling edge applications for home routed roaming scenarios

6.2b Architecture for Federation support

6.2b.1 General

This clause describes the architecture for support of Federation. To support Federation, EDGE-10 reference point is used between the ECSs to exchange ECS profile and EDN configuration information.

NOTE: ECS profile of partner ECSs can be preconfigured in the ECS or can be configured by the OAM system. For cases where the preconfigured and OAM configured information is not sufficient or not available, the ECS may communicate with other ECSs, e.g. ECS with edge repository functionality, to obtain the information.

If the ECSP is required to support service provisioning for a certain EAS whose information is not within the pre-configuration or OAM configuration, the ECS can use Edge repository functions as defined in clause 6.3.4 to support ECS discovery via ECS-ER.

6.2b.2 Architecture

Figure 6.2b.2-1 shows the architecture for support of federation. EDGE-10 reference point is introduced between the ECSs. ECSs interfacing over EDGE-10 reference point can be provided by different or the same ECSP.

EDGE-10 interface is used for exchange of EDN configuration information.

When one of the ECS is enhanced as an edge repository (ECS-ER) as defined in clause 6.3.4, making it the center of information for edge deployments, the ECS-ER receives information about edge deployments from other ECSs and stores it. In such deployments, EDGE-10 interface is used both for exchanging of ECS profile during ECS discovery and for exchanging EDN configuration information during service provisioning information retrieval.

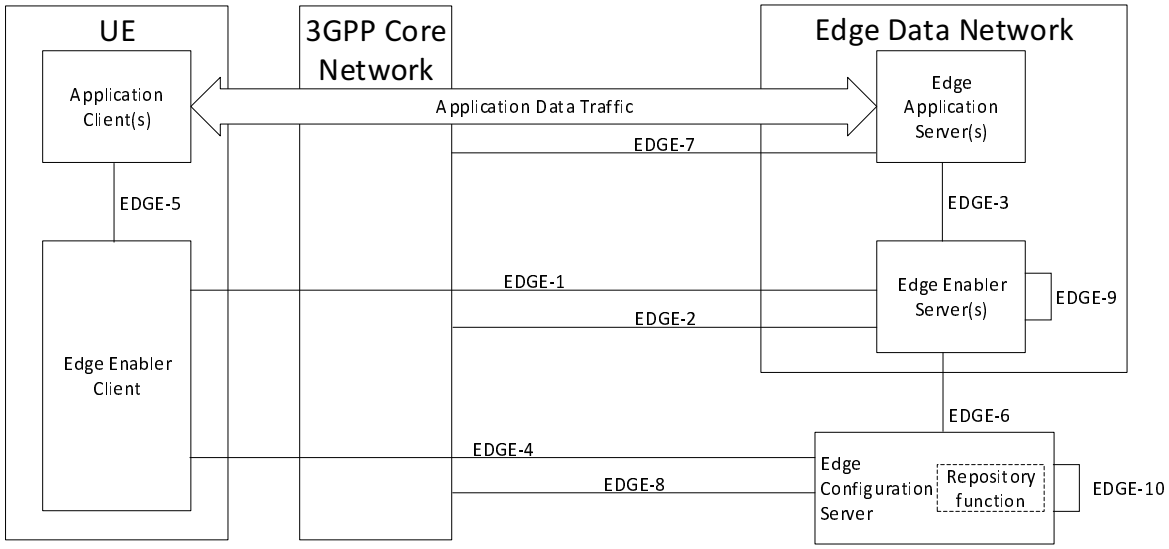

Figure 6.2b.2-1: Architecture for Federation support

6.2c Architecture for enabling cloud applications with edge applications

Figure 6.2c-1 illustrates the architecture for enabling cloud applications along with the edge applications.

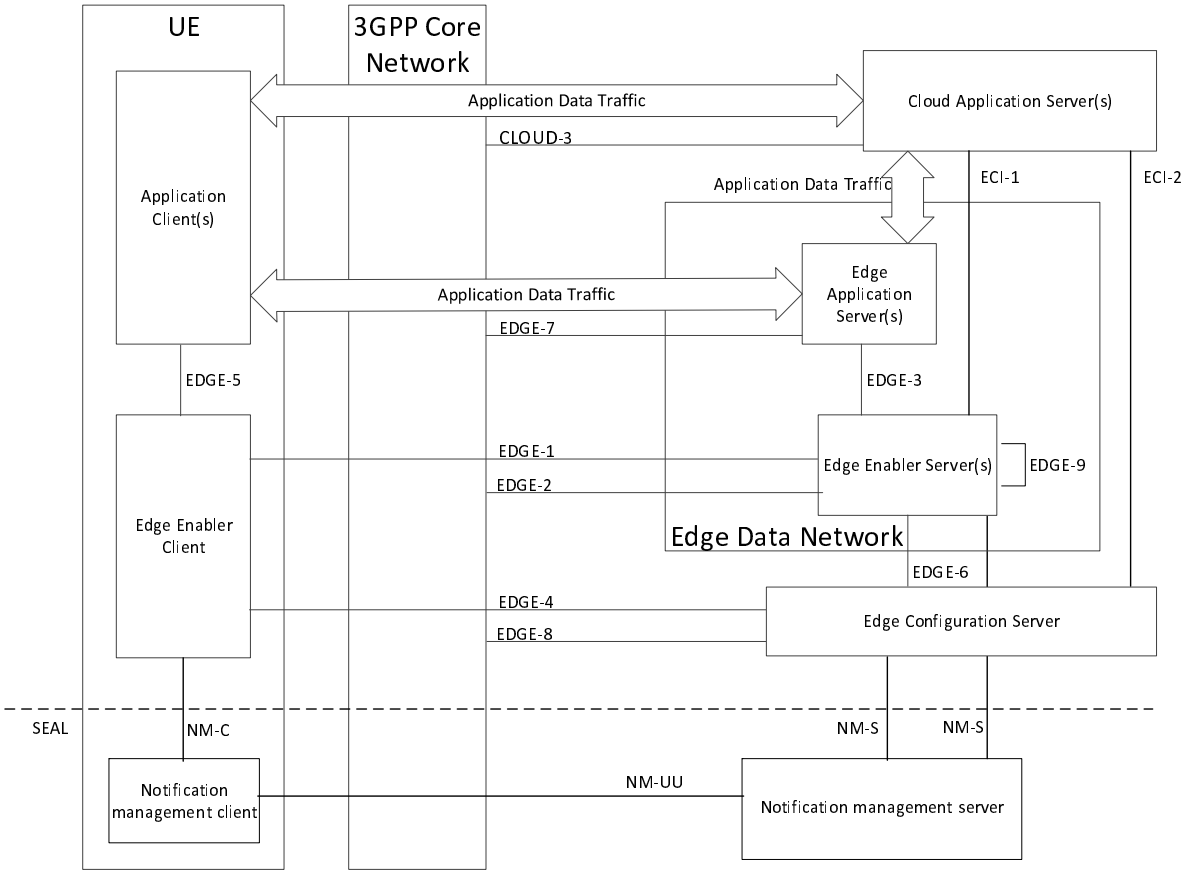

Figure 6.2c-1: Architecture for enabling cloud application with edge applications

Cloud application server (CAS) residing outside the EDN may need to interact with the EEL entities e.g. for service continuity. The CAS and EAS interaction is Application Data Traffic, which is out-of-scope of this specification.

6.2d Architecture for enabling cloud applications with edge applications, with CES support

Figure 6.2d-1 illustrates the architecture for enabling cloud applications along with the edge applications, when CES is used.

NOTE: Edge and cloud servers can utilize SEAL NM service but for simplicity such an interaction is not depicted in the figure.

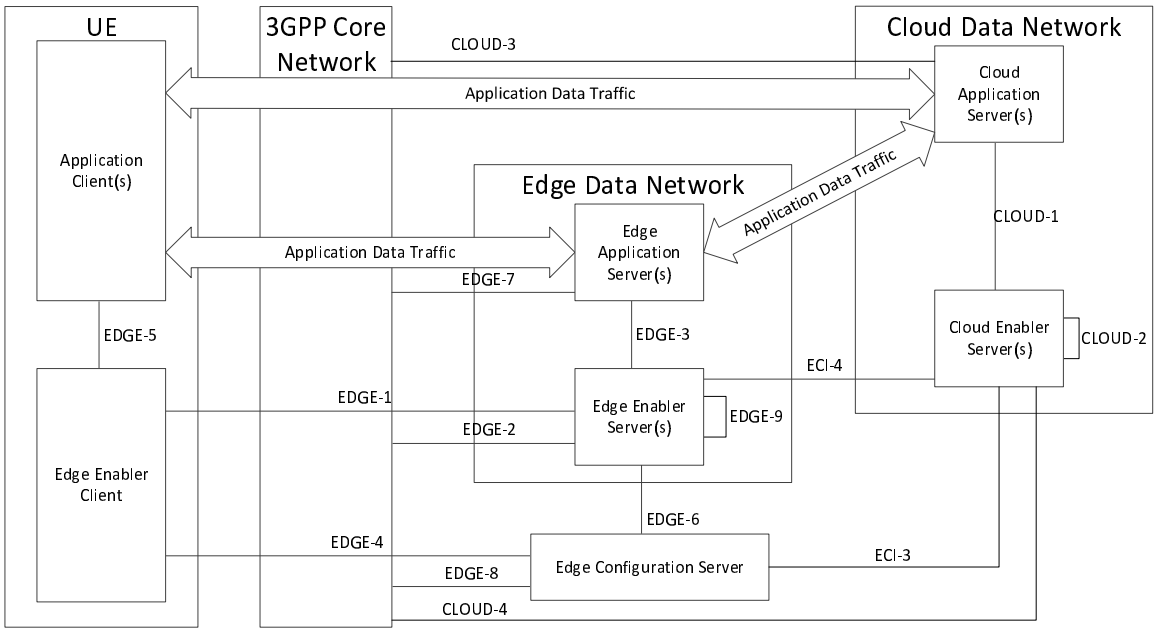

Figure 6.2d-1: Architecture for enabling cloud application with edge applications

Cloud Application Server (CAS) residing in the cloud DN may need to interact with the Cloud Enabler Server (CES) which is part of the EEL for interworking, e.g. for service continuity. The CAS and EAS interaction is Application Data Traffic, which is out-of-scope of this specification.

6.3 Functional entities

6.3.1 General

This clause describes the functional entities of the architecture for enabling edge applications.

6.3.2 Edge Enabler Server (EES)

EES provides supporting functions needed for EASs and EEC.

Functionalities of EES are:

a) provisioning of configuration information to EEC, enabling exchange of application data traffic with the EAS;

b) providing API invoker and API exposing functions as specified in 3GPP TS 23.222 [6]. To support deployments specified in clause A.5, providing CAPIF core functions as specified in 3GPP TS 23.222 [6];

c) interacting with 3GPP Core Network for accessing the capabilities of network functions either directly (e.g. via PCF) or indirectly (i.e. SCEF/NEF/SCEF+NEF);

d) exposing events related to ACT;

e) EEC context transfer between EESs;

f) supporting external exposure of 3GPP network and service capabilities to the EAS(s) over EDGE-3;

g) registration functions (i.e., registration, update, and de-registration) for the EEC(s) and the EAS(s);

h) triggering the EAS instantiation on demand;

i) supporting ACR related operations (e.g. ACR launching, ACR information notification, EELManagedACR); and

j) supporting the security related functions (e.g. authentication, authorization, acting as consent enforcing entity) as specified in 3GPP TS 33.558 [23] and 3GPP TS 33.501 [31].

6.3.3 Edge Enabler Client (EEC)

EEC provides supporting functions needed for AC(s).

Functionalities of EEC are:

a) retrieval of configuration information to enable the exchange of Application Data Traffic with the EAS;

b) discovery of EASs available in the EDN;

c) detecting UE mobility events;

d) exposure of events of interest to AC; and

e) retrieval of UE ID and/or Edge UE ID.

6.3.4 Edge Configuration Server (ECS)

ECS provides supporting functions needed for the EEC to connect with an EES.

Functionalities of ECS are:

a) provisioning of Edge configuration information to the EEC. The Edge configuration information includes the following:

   1) the information for the EEC to distinguish amongst the EESs (e.g. EDN service area); and

   2) the information for establishing a connection with EESs (such as URI);

b) providing the T-EES information to the S-EES;

NOTE: The ECS can be deployed in the MNO domain or can be deployed in 3rd party domain by service provider.

c) supporting the functionalities of registration (i.e., registration, update, and de-registration) for the EES(s);

d) supporting the functionalities of API invoker and API exposing function as specified in 3GPP TS 23.222 [6];

e) interacting with 3GPP Core Network for accessing the capabilities of network functions either directly (e.g. via PCF) or indirectly (i.e. SCEF/NEF/SCEF+NEF).

f) providing service provisioning information to a partner ECS; and

g) retrieving service provisioning information from a partner ECS.

If the ECSP is required to support service provisioning for a certain EAS whose information is not within the pre-configuration or OAM configuration, the ECS can use Edge repository functions to support ECS discovery via ECS-ER. To support functions of the edge repository the ECS supports the following functionality(ies):

a) registering and providing edge deployment information to ECS-ER.

To support the federation and discovery of a common EAS for a set of UEs the functionalities of the enhanced ECS i.e. ECS-ER, in addition to ECS functionalities, are:

1. Federation

   a) supporting the functionalities of registration (i.e., registration, update, and de-registration) for the ECS(s);

   b) receiving and storing information about edge computing resources from the ECS(s);

   c) receiving and storing information about edge computing resources from other ECS-ER(s); and

   d) providing information about Edge computing resources to other ECS-ER(s) of the federation.

2. Common EAS discovery

    a) storing and providing common EES and common EAS information.

NOTE: ECS can support repository function as ECS-ER.

6.3.5 Application Client (AC)

AC is the application resident in the UE performing the client function. Depending on how ACR is implemented, the AC might be required to decide whether to initiate ACR. Other details of the AC are out of scope of this specification.

6.3.6 Edge Application Server (EAS)

EAS is the application server resident in the EDN, performing the server functions. The AC connects to the EAS in order to avail the services of the application with the benefits of Edge Computing.

It is possible that the server functions of an application are available only as an EAS.

However, it is also possible that certain server functions are available both at the edge and in the cloud, as an EAS and an Application Server resident in the cloud respectively. The server functions offered by an EAS and its cloud Application Server counterpart may be the same or may differ; if they differ, the Application Data Traffic exchanged with the AC may also be different.

The EAS can consume the 3GPP Core Network capabilities in the following ways, all of which are optional to support:

a) invoking 3GPP Core Network capabilities via the edge enabler layer through the EES

b) invoking 3GPP Core Network function (e.g. PCF) APIs directly, if it is an entity trusted by the 3GPP Core Network; and

c) invoking the 3GPP Core Network capabilities through the capability exposure functions i.e. SCEF/NEF/SCEF+NEF.

The EAS can support processing ACR related operations (e.g. ACR status update, selected target EAS declaration).

The EAS can expose its Service API(s) (i.e., EAS Service API(s)) towards the other EASs by supporting API provider domain functions as specified in TS 23.222 [6]; and the EAS can consume the EAS Service API(s) exposed by the other EAS(s) by supporting API invoker functionalities as specified in TS 23.222 [6].

6.3.7 Notification management client

Notification management client is as specified in 3GPP TS 23.434 [13].

6.3.8 Notification management server

Notification management server is as specified in 3GPP TS 23.434 [13].

6.3.9 Cloud Enabler Server (CES)

CES provides supporting functions needed for CASs. The CES is part of the EEL and it does not have service area restriction. CES facilitates service continuity between EAS and CAS. The CES re-uses most of the EES services.

Functionalities of the CES are:

a) providing access to network capability information (e.g. location information) to the CAS;

b) facilitating setup of a data session between AC and CAS with a specific QoS; and

c) supporting ACR related operations.

6.3.10 Cloud application server (CAS)

CAS is the application server resident in the cloud, performing the server functions. The AC connects to the CAS in order to avail the services of the application.

6.4 Service-based interfaces

The architecture for enabling edge applications contains the following service-based interfaces:

Eecs: Service-based interface exhibited by ECS.

Eees: Service-based interface exhibited by EES.

6.5 Reference Points

6.5.1 General

This clause describes the reference points of the architecture for enabling edge applications.

6.5.2 EDGE-1

EDGE-1 reference point enables interactions between the EES and the EEC. It supports:

a) registration and de-registration of the EEC to the EES;

b) retrieval and provisioning of EAS configuration information;

c) discovery of EASs available in the EDN; and

d) service continuity procedures (e.g. ACR initiation).

6.5.3 EDGE-2

EDGE-2 reference point enables interactions between the EES and the 3GPP Core Network functions and APIs for retrieval of network capability information. It supports:

- access via SCEF and NEF APIs as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 29.522 [4], 3GPP TS 23.682 [17], 3GPP TS 29.122 [5]; or
- direct access to core network functions with the EES deployed within the MNO trust domain (see 3GPP TS 23.501 [2] clause 5.13, 3GPP TS 23.503 [12], 3GPP TS 23.682 [17]).

NOTE: EDGE-2 reference point reuses 3GPP reference points or interfaces of EPS or 5GS considering different deployment models.

6.5.4 EDGE-3

EDGE-3 reference point enables interactions between the EES and the EASs. It supports:

a) registration of EASs with availability information (e.g. time constraints, location constraints);

b) de-registration of EASs from the EES;

c) discovery of T-EAS information to support ACT;

d) providing access to network capability information (e.g. location information);

e) requesting the setup of a data session between AC and EAS with a specific QoS and receiving QoS related information; and

f) service continuity procedures (e.g. ACR status).

NOTE: Optimized distribution of events across the EDGE-3 interface is out of scope of this specification.

6.5.5 EDGE-4

EDGE-4 reference point enables interactions between the ECS and the EEC. It supports:

a) provisioning of Edge configuration information to the EEC.

6.5.6 EDGE-5

EDGE-5 reference point enables interactions between AC(s) and the EEC. It supports:

a) registration, registration update and de-registration of AC to the EEC;

b) EAS discovery by the AC;

c) ACR triggering by the AC;

d) EEC services subscription; and

e) UE ID request.

6.5.7 EDGE-6

EDGE-6 reference point enables interactions between the ECS and the EES. It supports:

a) registration of EES information to the ECS;

b) de-registration of EES information from the ECS; and

c) retrieval of the T-EES information from the ECS.

6.5.8 EDGE-7

EDGE-7 reference point enables interactions between the EAS and the 3GPP Core Network functions and APIs for retrieval of network capability information. It supports:

- access via SCEF and NEF APIs as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 29.522 [4], 3GPP TS 23.682 [17], 3GPP TS 29.122 [5]; or

- direct access to core network functions with the EAS deployed within the MNO trust domain (see 3GPP TS 23.501 [2] clause 5.13, 3GPP TS 23.682 [17]).

NOTE: EDGE-7 reference point reuses 3GPP reference points or interfaces of EPS or 5GS considering different deployment models.

6.5.9 EDGE-8

EDGE-8 reference point enables interactions between the ECS and the 3GPP Core Network functions and APIs for retrieval of network capability information. It supports:

- access via SCEF and NEF APIs as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 29.522 [4], 3GPP TS 23.682 [17], 3GPP TS 29.122 [5]; or

- direct access to core network functions with the ECS deployed within the MNO trust domain (see 3GPP TS 23.501 [2] clause 5.13, 3GPP TS 23.682 [17]).

NOTE: EDGE-8 reference point reuses 3GPP reference points or interfaces of EPS or 5GS considering different deployment models.

6.5.10 EDGE-9

EDGE-9 reference point enables interactions between two EESs. EDGE-9 reference point may be provided between EES within different EDN (Figure 6.5.10-1) and within the same EDN (Figure 6.5.10-2).

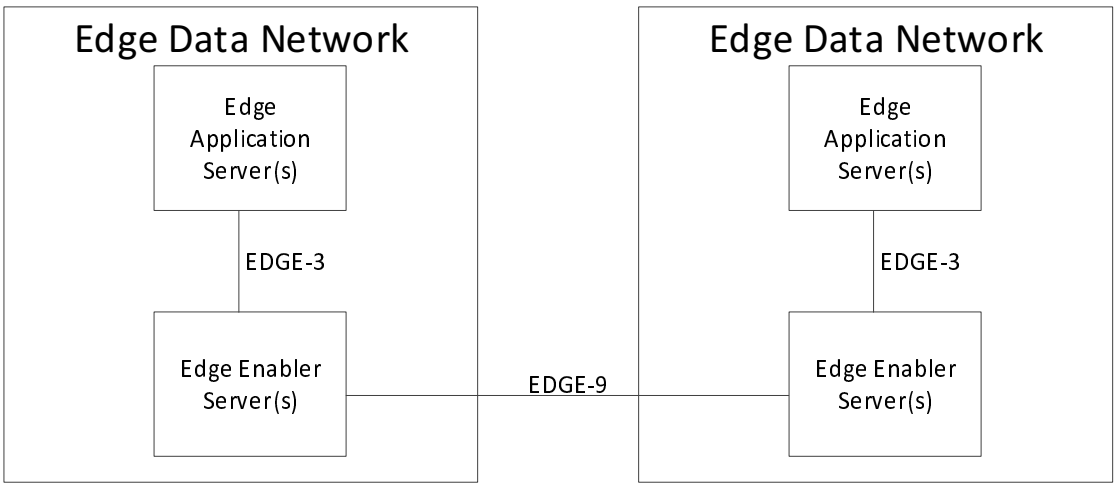

Figure 6.5.10-1: Inter-EDN EDGE-9

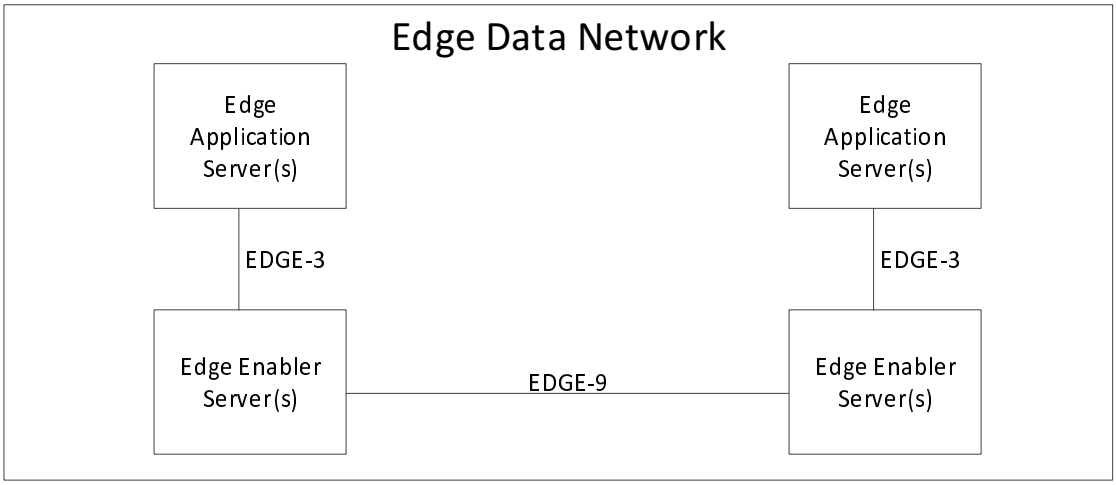

Figure 6.5.10-2: Intra-EDN EDGE-9

EDGE-9 supports:

a) discovery of T-EAS information to support ACR;

b) EEC context relocation procedures; and

c) transparent transfer of the application context during EELManagedACR.

6.5.11 NM-UU

NM-UU reference point is as specified in 3GPP TS 23.434 [13].

6.5.12 NM-S

NM-S reference point is as specified in 3GPP TS 23.434 [13], where EES or ECS acts VAL server.

6.5.13 NM-C

NM-C reference point is as specified in 3GPP TS 23.434 [13], where EEC acts as VAL client.

6.5.14 ECI-1

ECI-1 enables interaction between CAS and EES. ECI-1 supports:

a) notifying the CAS about selection of an EES to provide edge enabler services;

b) discovery of T-EAS to support ACT from CAS to T-EAS; and

c) selected T-EAS declaration where CAS acts as S-EAS.

ECI-1 supports:

a) ACR status update between EES and CAS as specified in clause 8.8.2A.6; and

b) T-EAS discovery procedure initiated by CAS as specified in clause 8.8.2A.6.

6.5.15 ECI-2

ECI-2 enables interaction between CAS and ECS.

NOTE: ECI-2 functionalities are not specified in the current release.

6.5.16 ECI-3

ECI-3 enables interaction between CES and ECS.

ECI-3 supports:

a) T-EES retrieval procedure.

6.5.17 ECI-4

ECI-4 enables interaction between CES and EES.

ECI-4 supports:

a) EEC context relocation procedure; and

b) ACR parameter information procedure.

6.5.18 CLOUD-1

CLOUD-1 enables interaction between CAS and CES.

CLOUD-1 supports:

a) providing access to network capability information (e.g. location information);

b) requesting the setup of a data session between AC and CAS with a specific QoS and receiving QoS related information; and

c) service continuity procedures (e.g. ACR status).

6.5.19 CLOUD-2

CLOUD-2 enables interaction between CES and CES.

NOTE: CLOUD-2 functionalities are not specified in the current release.

6.5.20 CLOUD-3

CLOUD-3 enables interaction between CAS and the 3GPP core network.

6.5.21 CLOUD-4

CLOUD-4 enables interaction between CES and the 3GPP core network.

6.5.22 EDGE-10

EDGE-10 reference point enables interactions between the ECS and another ECS. It supports:

a) service provisioning information retrieval.

b) registration and de-registration of the ECS to the ECS acting as edge repository; and

c) retrieval or discovery of information about other ECS(s) of the federation.

6.6 Cardinality rules

6.6.1 General

The cardinality rules are applied to the architecture specified in clause 6.2. The cardinality rules are classified as functional entity cardinality and reference point cardinality. The functional entity cardinality specifies the multiplicity of the functional entity that can exist as per the architecture. The reference point cardinality specifies the multiplicity of source and target functional entities that can exist in a relationship defined by the reference point in the architecture.

NOTE: The cardinality rules for the functional entities involved in EDGE-2, EDGE-7 and EDGE-8 interactions with 3GPP core network is based on the interactions between the AF and 3GPP Core Network entities as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.682 [17].

6.6.2 Functional Entity Cardinality

6.6.2.1 General

6.6.2.2 AC

The following cardinality rules apply for ACs:

a) one or more ACs may be located in a UE.

6.6.2.3 EEC

The following cardinality rules apply for EECs:

a) One or more EEC(s) may be located in a UE.

6.6.2.4 ECS

The following cardinality rules apply for ECSs:

a) One or more ECS(s) may be deployed to support one EDN;

b) One ECS may be deployed to support one or more EDN(s);

c) One or more ECS(s) may be deployed by a PLMN operator; and

d) One or more ECS(s) may be deployed by an ECSP.

Following cardinality rule apply to the ECS that supports edge repository functionality and acts as an ECS-ER:

a) One ECS-ER may be deployed by a PLMN operator; and

b) One ECS-ER may be deployed by an ECSP.

6.6.2.5 EES

The following cardinality rules apply for EES:

a) One or more EES(s) may be located in an EDN; and

b) One or more EES(s) may be located in an EDN per ECSP.

6.6.2.6 EAS

The following cardinality rules apply for EASs:

a) One or more EAS(s) may be located in an EDN.

NOTE: EAS(s) belonging to the same EASID can be deployed with EES(s) of multiple ECSP(s) in an EDN.

6.6.2.7 CES

The following cardinality rules apply for CES:

a) One CES may be located in a cloud DN per ECSP.

6.6.2.8 CAS

The following cardinality rules apply for CASs:

a) One or more CAS(s) may be located in a cloud DN.

6.6.3 Reference Point Cardinality

6.6.3.1 General

6.6.3.2 EDGE-1 (Between EEC and EES)

The following cardinality rules apply for EDGE-1:

a) One EEC may communicate with one or more EES(s) for one or more AC concurrently; and

b) One EES may communicate with one or more EEC(s) concurrently.

6.6.3.3 EDGE-3 (Between EAS and EES)

The following cardinality rules apply for EDGE-3:

a) One EAS may communicate with only one EES within the same EDN; and

b) One EES may communicate with one or more EAS(s) concurrently.

6.6.3.4 EDGE-4 (Between EEC and ECS)

The following cardinality rules apply for EDGE-4:

a) One EEC may communicate with one or more ECS(s) concurrently; and

b) One ECS may communicate with one or more EEC(s) concurrently.

6.6.3.5 EDGE-5 (Between AC and EEC)

The following cardinality rules apply for EDGE-5:

a) One AC may communicate with only one EEC; and

b) One EEC may communicate with one or more AC(s) concurrently.

6.6.3.6 EDGE-6 (Between EES and ECS)

The following cardinality rules apply for EDGE-6:

a) One EES may communicate with one or more ECS(s) concurrently; and

b) One ECS may communicate with one or more EES(s) concurrently.

6.6.3.7 EDGE-9 (Between EES and EES)

The following cardinality rules apply for EDGE-9:

a) One EES may communicate with one or more EES(s) concurrently.

6.6.3.8 EDGE-10 (Between ECS and ECS)

Following cardinality rules apply for EDGE-10:

a) One ECS may communicate with one or more ECS(s) concurrently.

6.6.3.9 ECI-1 (Between CAS and EES)

The following cardinality rules apply for ECI-1:

a) One CAS may communicate with one or more EES(s) concurrently; and

b) One EES may communicate with one or more CAS(s) concurrently.

6.6.3.10 ECI-2 (Between CAS and ECS)

The following cardinality rules apply for ECI-2:

a) One CAS may communicate with one or more ECS(s) concurrently; and

b) One ECS may communicate with one or more CAS(s) concurrently.

6.6.3.11 ECI-3 (Between CES and ECS)

The following cardinality rules apply for ECI-3:

a) One CES may communicate with one or more ECS(s) concurrently; and

b) One ECS may communicate with one or more CES(s) concurrently.

6.6.3.12 ECI-4 (Between CES and EES)

The following cardinality rules apply for ECI-4:

a) One CES may communicate with one or more EES(s) concurrently; and

b) One EES may communicate with one or more CES(s) concurrently.

6.6.3.13 CLOUD-1 (Between CAS and CES)

The following cardinality rules apply for CLOUD-1:

a) One CAS may communicate with only one CES within the same cloud DN; and

b) One CES may communicate with one or more CAS(s) concurrently.

6.6.3.14 CLOUD-2 (Between CES and CES)

The following cardinality rules apply for CLOUD-2:

a) One CES may communicate with one or more CES(s) concurrently.

6.7 Capability exposure for enabling edge applications

6.7.1 General

The Figure 6.7.1-1 shows the capability exposure for enabling edge applications.

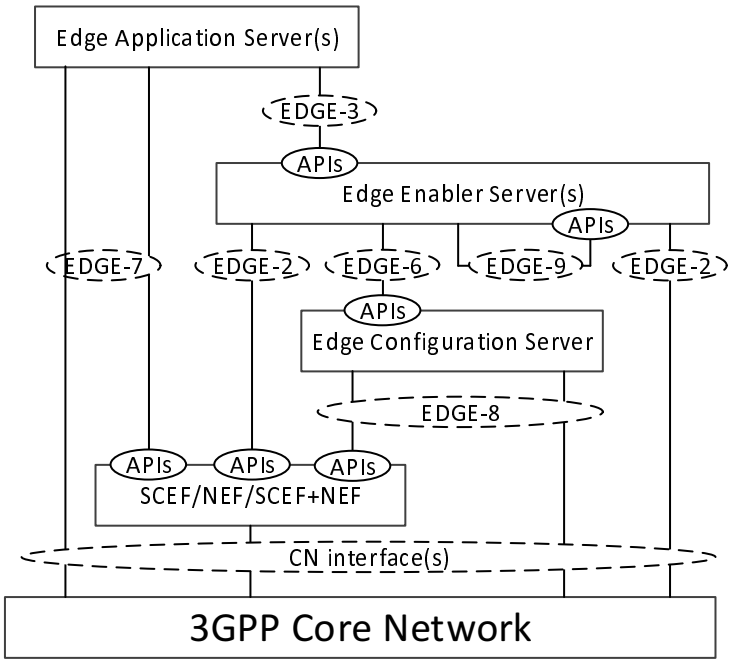

Figure 6.7.1-1: Capability exposure for enabling edge applications

Capability exposure includes the 3GPP core network (i.e. 5GC, EPC), ECS and the EES capability exposure, to fulfil the needs of the edge service operations. The capability exposure functionality is utilized by the functional entities (i.e. EES, EAS and ECS) depicted in the architecture for enabling the edge applications.

NOTE: The edge enabling layer also supports the exposure of EAS Service APIs using CAPIF, which is not explicitly depicted in the Figure 6.7.1-1.

6.7.2 APIs provided by the Edge Enabler Layer

Table 6.7.2-1 summarizes the APIs exposed by the ECS.

Table 6.7.2-1: APIs provided by the ECS

API Name	Known Consumers	References
Eecs_ServiceProvisioning	EEC	8.3
Eecs_EESRegistration	EES	8.4.4
Eecs_TargetEESDiscovery	EES, CES	8.8.3.3
Eecs_ECSRegistration	ECS	8.17.2.2
Eecs_ECSDiscovery	ECS	8.17.2.3
Eecs_ECSServiceProvisioning	ECS	8.17.2.4
Eecs_EASInfoManagement	EES	8.20.2

Table 6.7.2-2 summarizes the APIs exposed by the EES.

Table 6.7.2-2: APIs provided by the EES

API Name	Known Consumers	References
Eees_EECRegistration	EEC	8.4.2
Eees_EASRegistration	EAS	8.4.3
Eees_EASDiscovery	EEC	8.5
Eees_UELocation	EAS	8.6.2
Eees_ACRManagementEvent	EAS, CAS	8.6.3
Eees_AppClientInformation	EAS	8.6.4
Eees_UEIdentifier	EEC, EAS	8.6.5
Eees_SessionWithQoS	EAS	8.6.6
Eees_TrafficInfluenceEAS	EAS	8.6.7
Eees_TargetEASDiscovery	EAS, EES, CAS	8.8.3.2
Eees_AppContextRelocation	EEC, EAS, EES	8.8.3.4
Eees_ACREvents	EEC	8.8.3.5
Eees_EELManagedACR	EAS	8.8.3.6
Eees_SelectedTargetEAS	EAS, CAS	8.8.3.7
Eees_ACRStatusUpdate	EAS, CAS	8.8.3.8
Eees_ACRParameterInformation	EES, CES	8.8.3.9
Eees_EECContextPull	EES	8.9.4.2
Eees_EECContextPush	EES, CES	8.9.4.3
Eees_EASInformationProvisioning	EEC	8.15
Eees_CommonEasAnnouncement	EES	8.19

NOTE: The event exposure related APIs (e.g. Eees_EASDiscovery and Eees_ACREvents) can be realized as single event subscription API.

Table 6.7.2-3 summarizes the APIs exposed by the CAS.

Table 6.7.2-3: APIs provided by the CAS

API Name	Known Consumers	References
Ecas_SelectedEES	EES	8.8.3.10

Table 6.7.5-4 summarizes the APIs exposed the EEC.

Table 6.7.2-4: APIs provided by the EEC

API Name	Known Consumers	References
Eeec_ACRegistration	AC	8.14.4.2
Eeec_EASDiscovery	AC	8.14.4.3
Eeec_ACRTrigger	AC	8.14.4.4
Eeec_Services	AC	8.14.4.5
Eeec_UEId	AC	8.14.4.6

Table 6.7.2-2 summarizes the EES APIs re-used by the CES.

Table 6.7.2-5: APIs re-used by the CES

API Name	Known Consumers	References
Eees_EASRegistration	CAS	8.4.3
Eees_UELocation	CAS	8.6.2
Eees_ACRManagementEvent	CAS	8.6.3
Eees_AppClientInformation	CAS	8.6.4
Eees_UEIdentifier	CAS	8.6.5
Eees_SessionWithQoS	CAS	8.6.6
Eees_TrafficInfluenceEAS	CAS	8.6.7
Eees_TargetEASDiscovery	EES	8.8.3.2
Eees_AppContextRelocation	CAS	8.8.3.4
Eees_ACREvents	EEC	8.8.3.5
Eees_SelectedTargetEAS	CAS	8.8.3.7
Eees_ACRStatusUpdate	CAS	8.8.3.8
Eees_ACRParameterInformation	EES	8.8.3.9
Eees_EECContextPush	EES	8.9.4.3

7 Identities and commonly used values

7.1 General

The following clauses list identities and commonly used values that are used in this technical specification.

7.2 Identities

7.2.1 General

The following clauses specify a collection of identities that are associated with entities defined and being used in this specification.

7.2.2 Edge Enabler Client ID (EECID)

The EECID is a globally unique value that identifies an EEC.

NOTE: Security and privacy aspects related to EECID are specified in 3GPP TS 33.558 [23].

7.2.3 Edge Enabler Server ID (EESID)

The EESID identifies an EES and each EES connected with the PLMN has a unique EESID within PLMN domain.

7.2.4 Edge Application Server ID (EASID)

The EASID is a globally unique identifier which identifies a particular application for e.g. SA6Video, SA6Game etc. All EAS instances (e.g. of SA6Video application) will share the same EASID.

NOTE: The definition of the EASID is in 3GPP TS 24.558 [29] and 3GPP TS 29.558 [30].

7.2.5 Application Client ID (ACID)

The ACID identifies the client side of a particular application, for e.g. SA6Video viewer, SA6MsgClient etc. For example, all SA6MsgClient clients will share the same ACID.

In case that the UE is running mobile OS, the ACID is a pair of OSId and OSAppId.

7.2.6 UE ID

The UE Identifier (UE ID) uniquely identifies a particular UE within a PLMN domain. UE ID can be:

a) a GPSI, as defined in 3GPP TS 23.501 [2].

NOTE 1: For user's privacy reasons, GPSI in the form of MSISDN can be used only after obtaining user's consent.

NOTE 2: To protect user's privacy, if MSISDN cannot be used then AF-specific UE ID which is a GPSI in the form of an External ID may either be acquired through the NEF's Nnef_UEId_Get service operation (see TS 23.502 clause 4.15.10) or other out of scope means (e.g. pre-configuration).

b) an EEL-generated Edge UE ID, as defined in clause 7.2.9.

7.2.7 UE Group ID

The UE Group ID uniquely identifies a group of UE within a PLMN domain. Following identities are examples that can be used:

a) internal group ID, as defined in 3GPP TS 23.501 [2]; and

b) external group ID, as defined in 3GPP TS 23.501 [2].

7.2.8 EEC Context ID

The EEC Context ID is a globally unique value which identifies a set of parameters associated with the EEC (e.g., due to registration) and maintained in the Edge Enabler Layer by EESs.

If the EEC registration request does not include a previously assigned EEC Context ID value, the receiver EES assigns a new EEC Context ID and creates an EEC Context as described in the Table 8.2.8-1.

Providing a previously assigned EEC Context ID at registration allows maintaining the EEC Context in the Edge Enabler Layer beyond the lifetime of a registration, subject to policies. If the EEC registration request does include a previously assigned EEC Context ID value, after EEC Context relocation, the receiver EES may assign a new EEC Context ID, subject to implementation and local policies.

NOTE: The EEC Context ID may be implemented as combination of other IDs (e.g., EES ID and registration ID). How the EEC Context ID is specified or assigned is out of scope of this specification.

7.2.9 Edge UE ID

The Edge UE ID is an identifier that is associated with the UE ID (GPSI as per clause 7.2.6) and managed by EES. The EES can generate Edge UE ID as needed (e.g. as per ECSP policy). Edge UE ID can be shared with the EAS directly (using UE Identifier API as per clause 8.6.5) and/or indirectly via AC (using UE ID request as per clause 8.14.2.6) in order for it to be used by the EAS over EDGE-3 interactions when it is not desired to share the UE ID (GPSI as per clause 7.2.6) with the EAS. The Edge UE ID can be temporary to limit the access of the EAS when needed.

NOTE: The Edge UE ID is not applicable for EDGE-7 interactions.

7.2.10 EAS bundle information

The EAS bundle information includes EAS bundle type, a list of EASIDs or a EAS bundle ID. The EAS bundle information may also include main EASID and EAS bundle requirements. EAS bundle ID establishes an association between the EASs. When included in the EAS profile, EAS bundle ID denotes the bundle to which the EAS belongs. When included in the AC profile EAS bundle ID is used to perform different Edge Enabler Layer operations, such as EAS discovery. Edge Enabler Layer handles the EASs belonging to the same bundle as required by related EAS bundle requirements as described in clause 8.2.10.

NOTE 1: Both EAS bundle ID and EAS bundle requirements are provided by the ASP.

NOTE 2: Bundle ID is necessary when the affinity between bundled EASs is strong (e.g., co-deployment and co-migration is essential) and the related ASPs, which provide the AC and bundled EASs, established the bundle. List of EASIDs is required when the affinity between the bundled EASs is weak (e.g., co-deployment and co-migration is only "nice to have").

NOTE 3: Following types of EAS bundles are considered in this release:

- Direct bundle, where AC interacts with multiple EASs of the EAS bundle directly with no coordination between the EASs; and
- Proxy bundle, where the AC interacts with one EAS of the EAS bundle which in turn coordinates with other EASs of the EAS bundle to provide services to the AC by exchanging Application Data Traffic with the other EASs, which is out-of-scope of this specification.

NOTE 4: Discovery of EAS Service APIs via CAPIF for the proxy bundle type is not considered in this release.

7.2.11 Application Group ID

Application Group ID uniquely identifies a group of UEs using the same application. It is allocated (either dynamically or pre-configured in the AC) by the ASP and is unique within the application. ACs supporting the same application on different OS (e.g., iOS, Android), and therefore differing ACIDs (as specified in clause 7.2.5), can have the same Application Group ID.

NOTE 1: In this version of specification, Application Group ID is assumed to be unique per EAS ID. Ensuring the uniqueness of the Application Group ID per EAS ID is out of scope of this specification.

NOTE 2: In this version of specification, an Application Group is assumed to correspond to a single application.

7.3 Commonly used values

7.3.1 General

7.3.2 UE location

The UE location identifies where the UE is connected to the network or the position of the UE. It provides consistent definition of the UE's location across the UE and network entities. Following values are examples of UE locations that can be used:

a) Cell Identity, Tracking Area Identity, GPS Coordinates or civic addresses as defined in 3GPP TS 23.502 [3] clause 4.15.3.

7.3.3 Service areas

7.3.3.1 General

ECSPs and ASPs may allow access to Edge Computing service from specific areas i.e. allowing only the UEs within that area to access functional entities resident in the EDN. This area is called service area.

Some functional elements make decisions based on the topological location of the UE, (e.g. the cell it is connected to) while others make decisions based on the UE's geographical location (e.g. its geographical coordinates).

Functional elements that are aware of both topological and geographical information can translate one value to the other.

7.3.3.2 Topological Service Area

A Topological Service Area is defined in relationship with a UE's point of connection to the network, such as: a collection of Cell IDs, Tracking Area Identities or the PLMN ID. Any UE that is attached to the Core Network from a cell whose ID is in this list, can be served by the functional entity in the EDN that is configured to serve that Topological Service Area.

NOTE: Topological Service Area information is not applicable for untrusted functional elements (EESs and/or EASs deployed outside the MNO trust domain).

7.3.3.3 Geographical Service Area

A Geographical Service Area is an area that is specified by geographical units as defined in 3GPP TS 23.032 [21], such as: Geographical coordinates, an area that is defined as a circle whose centre is denoted by geographical coordinates, an area that is defined by a polygon whose corners are denoted by geographical coordinates. A Geographical Service Area can also be expressed in other ways such as: a well-known buildings, parks, arenas, civic addresses or ZIP code etc.

Applications can be configured to serve UEs that are in a specified geographical area and deny service from UEs that are not located in that area.

NOTE: Whether and how geographical information is used by applications to provide or deny service is out of scope.

7.3.3.4 EDN service area

A service area from which the access to the EDN is allowed. ECSPs can use LADNs, as described in Annex A.2.4 of this document, to deploy EDNs with access restricted from specific areas. When an EDN is deployed using LADN, the EDN service area is same as the LADN service area and rules specified for LADN apply to the UE, as specified in 3GPP TS 23.501 [2].

In a deployment using DNs other than LADNs, the EDN service area is the whole PLMN for non-roaming scenario.

NOTE 1: The EDN service area for roaming scenario is out of scope in this release of the specification.

NOTE 2: For the purpose of restricting the access to the EES from specific areas, ECSP can use the EES service area, which is specified in clause 7.3.3.5, even if the EDN service area is the whole PLMN.

The EDN service area may be expressed as a Topological Service Area.

7.3.3.5 EES Service Area

A service area from which the access to the EES is allowed. This service area is equal to or a subset of the service area of the EDN in which the EES resides.

The EES service area may be expressed as a Topological Service Area, a Geographical Service Area or both.

7.3.3.6 EAS service area

A service area from which the access to the EAS is allowed. This service area is equal to or a subset of the service area of the EES which serves the EAS.

The EAS service area may be expressed as a Topological Service Area, a Geographical Service Area or both.

8 Procedures and information flows

8.1 General

This clause provides procedures and information flows necessary for enabling edge application including information elements used in the procedures.

8.2 Common Information Elements

8.2.1 General

This clause provides descriptions for Information Elements which are commonly used in several procedures.

8.2.2 AC Profile

An AC Profile includes information about AC used to determine services and service characteristics required.

NOTE: Information elements in the AC Profile are provided by the ASP.

Table 8.2.2-1: AC Profile

Information element	Status	Description
ACID	M	Identity of the AC.
AC Type	O	The category or type of AC (e.g. V2X). This is an implementation specific value.
Preferred ECSP list	O	When used in a service provisioning request, this IE indicates to the ECS which ECSPs are preferred for the AC. The ECS may use this information in the selection of EESs.
AC Schedule	O	The expected operation schedule of the AC (e.g. time windows)
Expected AC Geographical Service Area	O	The expected location(s) (e.g. route) of the hosting UE during the AC's operation schedule. This geographic information can express a geographic point, polygon, route, signalling map, or waypoint set.
AC Service Continuity Support (NOTE 1)	O	Indicates if service continuity support is required or not for the application. The IE indicates which ACR scenarios are supported by the AC and which of these are preferred by the AC, also indicates the AC ability (e.g. EAS bundle information) of handling bundled EAS coordinate ACR.
Simultaneous EAS connectivity information in service continuity	O	Indicates if simultaneous EAS connectivity is needed and the inactive time guidance for keeping connectivity towards the S-EAS.
List of EASs	O	List of EAS that serve the AC along with the service KPIs required by the AC
> EASID	M	Identifier of the EAS
> Expected AC Service KPIs	O	KPIs expected in order for ACs to receive currently required services from the EAS, as described in Table 8.2.3-1
> Minimum required AC Service KPIs	O	Minimum KPIs required in order for ACs to receive meaningful services from the EAS, as described in Table 8.2.3-1
List of required EAS bundle information	O	Information related to the EAS bundles which the AC requires.
> Bundle ID (NOTE 2)	O	Bundle ID as described in clause 7.2.10.
> List of EASIDs (NOTE 2)	O	List of EASIDs associated with the EAS bundle.
> Bundle type	M	Type of the EAS bundle as described in clause 7.2.10
> Main EASID	O	Indicate which EAS in a bundle takes the main EAS service role.
> EAS bundle requirements	O	Requirements associated with the EAS bundle as described in clause 8.2.10.
NOTE 1: The EAS bundle information is not applicable for proxy type of EAS bundle. NOTE 2: At least one of the IEs shall be present if EAS bundle information is provided.		

8.2.3 AC Service KPIs

AC Service KPIs provide information about service characteristics required by the ACs.

Table 8.2.3-1: AC Service KPIs

Information element	Status	Description
Connection bandwidth	O	The required connection bandwidth in Kbit/s for the application.
Request rate	O	The request rate to be generated by the AC.
Response time	O	Response time (NOTE) required for the server servicing the requests.
Availability	O	Percentage of time the server is required to be available for the AC's use.
Compute	O	The compute resources required by the AC.
Graphical Compute	O	The graphical compute resources required by the AC.
Memory	O	The memory resources required by the AC.
Storage	O	The storage resources required by the AC.
NOTE: The response time includes the round-trip time of the request and response packet, the processing time at the server and the time required by the server to consume 3GPP Core Network capabilities, if any.		

8.2.4 EAS Profile

An EAS Profile includes information about an EAS used to describe services and service characteristics offered.

NOTE: Information elements in the EAS Profile are provided by the ASP.

Table 8.2.4-1: EAS Profile

Information element	Status	Description
EASID	M	The identifier of the EAS
EAS Endpoint	M	Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EAS. This information maybe discovered by EEC and exposed to ACs so that ACs can establish contact with the EAS.
List of EAS bundle information	O	List of EAS bundles to which the EAS belongs and related bundling requirements.
> Bundle ID (NOTE 3)	O	Bundle ID as described in clause 7.2.10.
> List of EAS IDs (NOTE 2, NOTE 3)	O	List of the EAS IDs of the EASs to be invoked by the EAS for an EAS driven association of EASs.

> Bundle type	M	Type of the EAS bundle as described in clause 7.2.10
> Main EASID	O	Indicate which EAS in a bundle takes the main EAS service role.
> EAS bundle requirements	O	Requirements associated with the EAS bundle as described in clause 8.2.10.
ACID(s)	O	Identifies the AC(s) that can be served by the EAS
EAS Provider Identifier	O	The identifier of the ASP that provides the EAS.
Allowed MNO information (NOTE 4)	O	Information of the allowed operator (e.g. MNO name, PLMN ID) from which its subscriber can consume the EAS services
EAS Type	O	The category or type of EAS (e.g. V2X)
EAS description	O	Human-readable description of the EAS
EAS Schedule	O	The availability schedule of the EAS (e.g. time windows)
EAS Geographical Service Area	O	The geographical service area that the EAS serves. ACs in UEs that are located outside that area shall not be served.
EAS Topological Service Area	O	The EAS serves UEs that are connected to the Core Network from one of the cells included in this service area. ACs in UEs that are located outside this area shall not be served. See possible formats in Table 8.2.7-1.
EAS Service KPIs	O	Service characteristics provided by EAS, detailed in Table 8.2.5-1
EAS service permission level	O	Level of service permissions e.g. trial, gold-class supported by the EAS
EAS Feature(s)	O	Service features e.g. single vs. multi-player gaming service supported by the EAS
EAS synchronization support	O	Indicates if the EAS supports content synchronization between EASs.
EAS Service continuity support	O	Indicates if the EAS supports service continuity or not. This IE indicates which ACR scenarios are supported by the EAS, also indicates the EAS ability (e.g. EAS bundle information) of handling bundled EAS coordinate ACR.
EAS Transport layer service continuity support	O	This IE indicates the EAS service continuity support for seamless transport layer (e.g. TCP/TLS/QUIC) relocation
General context holding time duration (NOTE 1)	O	The time duration that the EAS holds the context before the AC connects to the EAS in case of ACR for service continuity planning. It is an indication of the time the EAS holds the application context for a UE to move to its service area after receiving an ACR notification from the EES following an ACR request from the EEC.
List of EAS DNAI(s)	O	DNAI(s) associated with the EAS. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [2]. It is a subset of the DNAI(s) associated with the EDN where the EAS resides.
List of N6 Traffic Routing requirements	O	The N6 traffic routing information and/or routing profile ID corresponding to each EAS DNAI.
EAS Availability Reporting Period	O	The availability reporting period (i.e. heartbeat period) that indicates to the EES how often it needs to check the EAS's availability after a successful registration.
EAS Status	O	The status of the EAS (e.g. enabled, disabled, etc.)
NOTE 1: Since the EASID of the EAS identifies the type of the application (e.g. SA6Video, SA6Game etc) as described in clause 7.2.4, "General context holding time duration" determined by EAS can depend on the EASID (type of the application). NOTE 2: This IE may be provided when only bundle ID is provided, and the bundle type indicates the proxy bundle. NOTE 3: At least one of the IEs shall be present if EAS bundle information is provided. NOTE 4: For edge node sharing scenario, in order to restrict the access to the subscriber of the partner operator, this IE should only include MNO information of the leading operator.		

NOTE: The EAS Transport layer service continuity support can be used in EAS discovery, e.g. as described in 3GPP TS 23.433 [26] for SEALDD server acting as EAS, which can further support the EAS IP replacement function.

8.2.5 EAS Service KPIs

EAS Service KPIs provide information about service characteristics provided by the EAS

Table 8.2.5-1: EAS Service KPIs

Information element	Status	Description
Maximum Request rate	O	Maximum request rate from the AC supported by the server.
Maximum Response time (NOTE)	O	The maximum response time advertised for the AC's service requests.
Availability	O	Advertised percentage of time the server is available for the AC's use.
Available Compute	O	The maximum compute resource available for the AC.
Available Graphical Compute	O	The maximum graphical compute resource available for the AC.
Available Memory	O	The maximum memory resource available for the AC.
Available Storage	O	The maximum storage resource available for the AC.
Connection Bandwidth	O	The connection bandwidth in Kbit/s advertised for the AC's use.
NOTE: The maximum response time includes the round-trip time of the request and response packet, the processing time at the server and the time required by the server to consume 3GPP Core Network capabilities, if any.		

8.2.6 EES Profile

The EES profile includes information about the EES and the services it provides.

NOTE: Information elements in the EES Profile are provided by the ECSP.

Table 8.2.6-1: EES Profile

Information element	Status	Description
EESID	M	The identifier of the EES
EES Endpoint	M	Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EES. This information is provided to the EEC to connect to the EES.
EDN information	O	EDN information where the EES resides.
> DNN	M	Data network name to identify the EDN.
> DNAI(s)	O	DNAI(s) associated with the EDN.
EASIDs	M	List of EASIDs registered or expected to be registered with the EES.
List of EAS bundle information	O	List of EAS bundles per EASID to which the EAS belongs and related bundling requirements.
> Bundle ID (NOTE 2)	O	A bundle ID as described in clause 7.2.10.
> List of EASIDs (NOTE 2)	O	List of EASIDs associated with the EAS bundle.
> Bundle type	M	Type of the EAS bundle as described in clause 7.2.10
> EAS bundle requirements	O	Requirements associated with the EAS bundle as described in clause 8.2.10.
Instantiable EAS information	O	The EAS instantiation status per EASID (e.g. instantiated, instantiable but not be instantiated yet).
> Instantiation criteria (NOTE 1)	O	The criteria upon which EAS can be instantiated (e.g. based on specific date and time).
EEC registration configuration	M	Indicates whether the EEC is required to register on the EES to use edge services or not.
ECSP ID	O	The identifier of the ECSP that provides the EES.
EES Topological Service Area	O	The EES serves UEs that are connected to the Core Network from one of the cells included in this service area. EECs in UEs that are located outside this area shall not be served. See possible formats in Table 8.2.7-1.
EES Geographical Service Area	O	The area being served by the EES in Geographical values (as specified in clause 7.3.3.3)
List of EES DNAI(s)	O	DNAI(s) associated with the EES. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [2]. It is a subset of the DNAI(s) associated with the EDN, where the EES resides.
EES Service continuity support	O	Indicates if the EES supports service continuity or not. This IE indicates which ACR scenarios are supported by the EES, also indicates the EES ability (e.g. EAS bundle information) of handling bundled EAS coordinate ACR.
NOTE 1: "Instantiation criteria" IE shall be present only when the value of "Instantiable EAS information" IE is "instantiable but not be instantiated yet". NOTE 2: At least one of the IEs shall be present if EAS bundle information is provided.		

NOTE: The list of EES DNAI(s) can include the DNAI(s) of the EAS(s) registered with the EES.

8.2.7 Topological Service Area

The following formats may be used for expressing a Topological Service Area:

Table 8.2.7-1: Topological Service Area

Information element	Status	Description
Cell IDs (NOTE)	O	The list of cell IDs defining the Topological Service Area
TAIs (NOTE)	O	The list of Tracking Area IDs defining the Topological Service Area
PLMN IDs (NOTE)	O	The list of PLMN IDs defining the Topological Service Area
NOTE: A combination of these information elements can be used to define the Topological Service Area. Combinations should not have duplicate or overlapping information for the same Topological Service Area.		

8.2.8 EEC Context

The EEC Context includes information about an EEC for receiving edge enabler services.

Table 8.2.8-1: EEC Context

Information element	Status	Description
EEC ID	M	Unique identifier of the EEC.
EEC Context ID	M	Identifier assigned to the EEC Context
Source EES Endpoint	M	The endpoint address (e.g., URI, IP address) of the EES that provided EEC context ID.
UE Identifier	O	The identifier of the hosting UE (i.e., GPSI)
List of EDGE-1 subscriptions	O	List of subscriptions IDs for capability exposure to the EEC ID (NOTE).
UE location	O	Latest UE location of the UE hosting the EEC which was available at the EES.
List of AC Profiles	O	Information about the ACs as described in Table 8.2.2-1.
UE Mobility Support Requirement	O	Indicates UE requires mobility support or not. For the request over EDGE-1 interface, the EES as per ECSP policy and EAS requirements, may decide whether to subscribe to NEF or NWDAF for UE location information based on this information.
List of Service Session Contexts	O	List of associated Service Session Context IEs. Each Service Session Context includes information maintained by the EES for the services (involving UE related resources) received from an EAS registered to the EES.
> Service Session Context	M	Service Session Context is described in Table 8.2.8-2
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
NOTE: The corresponding EDGE-1 subscription information may include 3GPP CN subscription information such as subscription correlation ID		

Table 8.2.8-2: Service Session Context

Information element	Status	Description
EAS ID	M	Identifier of the EAS providing the application services
EAS Endpoint	M	Endpoint information of the EAS.
AC ID	O	Identifier of the AC ID for which the service session is provided, if determined.
Selected ACR scenario list	O	List of selected ACR scenarios.

8.2.9 Geographical Service Area

The following formats may be used for expressing a Geographical Service Area:

Table 8.2.9-1: Geographical Service Area

Information element	Status	Description
Geographical Area Description	O	A shape defined in 3GPP TS 23.032 [21]
Civic Location	O	An area identified by a civic location element, e.g. building, park, arena, civic address or ZIP code.

8.2.10 EAS bundle requirements

The following IEs describe the EAS bundle requirements:

NOTE: Information elements in the EAS Bundle Requirements are provided by the ASP.

Table 8.2.10-1: EAS bundle requirements

Information element	Status	Description
Coordinated EAS discovery	O	Indicates if coordinated EAS discovery is required i.e., if EAS discovery request for one of the bundled EAS is processed, then EAS discovery response should include information of all the EASs belonging to the bundle.
Coordinated ACR	O	Indicates if coordinated ACR is required i.e., if EAS ACR is initiated for one of the bundled EAS, then ACR should be initiated for all the EASs belonging to the bundle. The IE may further indicate what actions must be taken if ACR for one or more bundled EAS fails e.g. ACR for all other EAS that are part of the bundle must be cancelled or not.
Affinity	O	Indicates the affinity requirement of the EAS bundle. The IE can be set to "strong" indicating that the EASs must be in the same EDN, "preferred" indicating that it is nice to have EASs in the same EDN but not essential or "weak" indicating that it's not essential for EASs to be in the same EDN.

8.2.11 Application Group profile

An Application Group profile includes information about the Application Group used to determine common EAS.

Table 8.2.11-1: Application Group profile

Information element	Status	Description
Application Group ID	M	Application group identifier as defined in 7.2.11.
EAS ID	M	Identifier of EAS
Expected Group Geographical Service Area.	O	The expected location(s) (e.g. route) of the group of UEs during the AC's operation schedule. This geographic information can express a geographic point, polygon, route, signalling map, or waypoint set.

8.2.12 ECS Profile

The ECS profile includes information about the ECS and EDN configuration information it provides.

Table 8.2.12-1: ECS Profile

Information element	Status	Description
ECS address	M	Endpoint information of ECS (e.g. URI, FQDN, IP address)
ECSP Identifier	O	The identifier of the ECSP (e.g., the MNO or a 3rd party service provider) that provides the ECS.
Spatial Validity Conditions	O	Spatial validity condition, as described in 3GPP TS 23.548 [20]
Federation information	O	List of information for different federation agreements related to the ECS
> List of partner ECSPs	O	List of ECSPs that are authorized to receive the information of this ECS.
List of supported PLMN(s)	O	The List of PLMNs and associated ECSPs for which EDN configuration information can be provided by the ECS.
> PLMN ID	O	The identifier of a PLMN for which EDN configuration information can be provided by the ECS.
> List of supported ECSP(s)	O	The identifier of the ECSP(s) associated with the PLMN and whose information is available at the ECS
>> ECSP ID	M	Identifier of an ECSP
>>> EASIDs	M	List of EASIDs available or expected to be available through the ECSP.
> PDU configuration	O	DNN and S-NSSAI information for roaming UEs to establish an PDU session with the ECS.

8.3 ECS Discovery and Service provisioning

8.3.1 General

Service provisioning allows configuring the EEC with information about available Edge Computing services, based on the hosting UEs location, service requirements, service preferences and connectivity. This configuration includes the necessary address information for the EEC to establish connection with the EES(s).

If the ECS deployed by MNO is contracted with one or more ECSP(s), the ECS provides EES configuration information of MNO owned and ECSP owned EESs via MNO ECS as described in clause 8.3.3.3.3.

If the ECS is deployed by a non-MNO ECSP, the ECS endpoint address may be configured with the EEC. An EEC that is aware of multiple ECSP's ECS endpoint addresses may perform the service provisioning procedure per ECS of each ECSP multiple times.

Figure 8.3.1-1 illustrates an overview of service provisioning. Service provisioning procedures support the following models:

- Request/Response model; and
- Subscribe/Notify model.

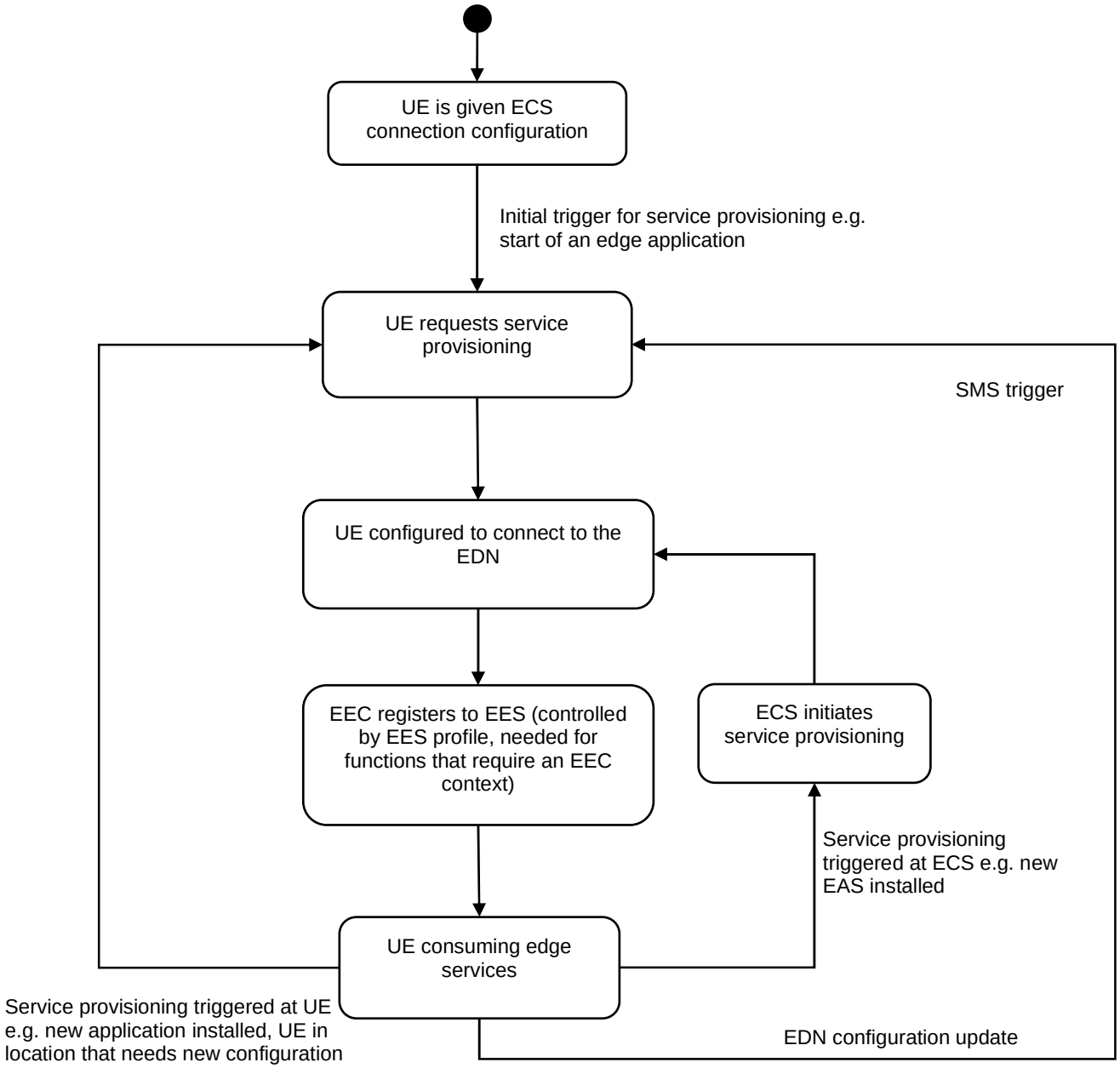

Figure 8.3.1-1: Overview of Service provisioning

The UE is given configuration information enabling it to connect to the ECS. The UE can then request initial provisioning from the ECS to obtain configuration required to connect to the EDN. Once provisioned, the EEC of the UE registers with the selected EES(s) from the list of provisioned EES(s) it received from the ECS(s), if the EEC registration configuration in EES profile indicates that EEC registration is required. The UE further consumes the edge computing services and performs various operations such as EAS discovery, Edge application communications, ACR, etc. While the UE is consuming the edge computing services, the UE or ECS may be triggered to re-request service provisioning.

The triggers for service provisioning are classified as:

a. Triggers at UE - Some examples are:

- AC related updates available at the EEC due to AC installation/re-installation, AC requesting application server access (e.g. via internet browser);

- EEC supporting one or more ACs may be updated due to EEC re-installation; and

- Lifetime of EDN Configuration Information is expired or the EEC detects that the UE moves out of EDN Service Area in the EDN Configuration Information.

b. Triggers at ECS – Some examples are:

- EES updates received due to EAS installation/re-installation/re-location; and
- ECS receives the EDN/DNAI change notification of the UE from 5GC when the ECS subscribes to the user plane path management events as specified in clause 8.10.2.

8.3.2 ECS Discovery

8.3.2.1 General

ECS configuration information consists of one or more endpoint information (e.g. URI(s), FQDN(s), IP address(es)) of ECS(s), and optionally the corresponding ECS Provider Identifier. ECS configuration information can be

- pre-configured with the EEC;
- configured by an edge-aware AC;
- configured by the user;
- provisioned by MNO through 5GC procedure if the UE has the capability to deliver the ECS configuration information to the EEC on the UE (see 3GPP TS 23.548 [20], clause 6.5.2);
- derived from HPLMN identifier for non-roaming scenario or from VPLMN identifier for roaming scenario; or
- derived from serving SNPN identifier.

NOTE 1: How the ECS configuration information is configured to the EEC user, or pre-configuration is out of scope of the present specification.

It may be possible to provide the ECS configuration information to the EEC from the 5GC if the UE has the capability to deliver the ECS configuration information to the EEC on the UE.

NOTE 2: When the AF provides the ECS configuration information to 5GC, the list of supported PLMN(s) of this ECS configuration information can be provided together. As described in 3GPP TS 23.548 [20], NFs do not need to be aware of internal structure of ECS configuration information.

It may be possible to provide the ECS configuration information to the EEC from an edge-ware AC via EDGE-5 reference point within the UE if the AC is configured with the ECS configuration information and can communicate with the EEC. When the ECS configuration information is provided from an AC, the EEC uses the ECS configuration information for the initial service provisioning for the AC if there is no ECS configuration information is provided from the 5GC.

If the ECS configuration information is provided by 5GC and available at the EEC, the EEC shall use the information for the initial provisioning request. Otherwise, the EEC shall use pre-configured ECS address for the initial provisioning if ECS configuration information is preconfigured with the EEC.

NOTE 3: The ECS configuration information configured by an edge-aware AC is considered to be part of pre-configured ECS configuration information with the EEC for the AC.

Table 8.3.2.1-1 describes the information elements of ECS configuration information for an ECS.

Table 8.3.2.1-1: ECS configuration information per ECS

Information element	Status	Description
ECS address	M	Endpoint information of ECS (e.g. URI, FQDN, IP address)
ECSP Identifier (NOTE 1)	O	The identifier of the ECSP (e.g., the MNO or a 3rd party service provider) that provides the ECS.
Spatial Validity Conditions	O	Spatial validity condition, as described in 3GPP TS 23.548 [20]
Security Parameters	O	The security parameters (as specified in 3GPP TS 33.558 [23], clause 6.2) are used by EEC to communicate with the ECS.
List of supported PLMN(s)	O	The List of PLMNs and associated ECSPs for which EDN configuration information can be provided by the ECS.
> PLMN ID	O	The identifier of a PLMN for which EDN configuration information can be provided by the ECS.
> List of supported ECSP(s) (NOTE 2)	O	The identifier of the ECSP(s) associated with the PLMN and whose information is available at the ECS
>> ECSP ID	M	Identifier of an ECSP
NOTE 1: This IE shall be included when the ECS configuration information is provisioned by the MNO through the 5GC procedure. NOTE 2: This IE may not be included if the ECSP does not want to expose its EES deployment information or business relationship-related information.		

8.3.2.2 Procedures

8.3.2.2.1 General

There is no additional information about procedures for ECS Discovery.

8.3.2.3 Information flows

8.3.2.3.1 General

There is no additional information about information flows for ECS Discovery

8.3.2.4 APIs

8.3.2.4.1 General

There is no additional information about APIs for ECS Discovery

8.3.3 Service provisioning

8.3.3.1 General

The following clauses specify procedures, information flows and APIs for service provisioning.

8.3.3.2 Procedures

8.3.3.2.1 General

Following procedures are supported for service provisioning:

- Request-response procedure;
- Subscribe-notify procedures, including:
  - Subscription procedure;
  - Notification procedure;

- Subscription update procedure; and
- Unsubscribe procedure.

8.3.3.2.2 Request-response model

Figure 8.3.3.2.2-1 illustrates service provisioning procedure based on request/response model.

Pre-conditions:

1. The EEC has been pre-configured or has discovered the address (e.g. URI) of the ECS;
2. The EEC has been authorized to communicate with the ECS;
3. The UE Identifier is either preconfigured or resulted from a successful authorization; and
4. The ECS is configured with ECSP's policy for service provisioning.

NOTE 1: Details of ECSP's policy are out of scope.

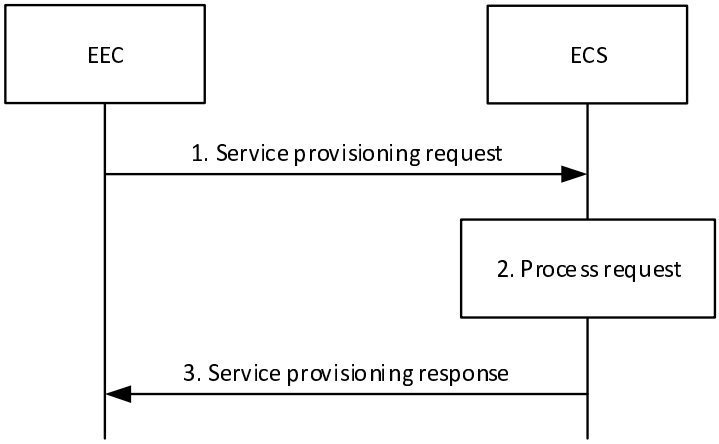

Figure 8.3.3.2.2-1: Service provisioning – Request/Response

1. The EEC sends a service provisioning request to the ECS. The service provisioning request includes the security credentials of the EEC received during EEC authorization procedure and may include the UE identifier such as GPSI, connectivity information, UE location, EEC service continuity support and AC profile(s) information. EEC may provide its desired ECSP identifier(s) in the service provisioning request based on EEC preference.
2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. The ECS may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.2. If the UE serving PLMN identifier is not provided by the EEC in the connectivity information of the service provisioning request, the ECS may invoke the NEF monitoring event API as described in 3GPP TS 23.502 [43] and 3GPP TS 23.682 [17] to obtain the UE roaming status and serving PLMN identifier. If the UE is roaming, the ECS may use the serving PLMN identifier to determine the roaming partner ECS (i.e. V-ECS) information to be provided to the EEC in the service provisioning response. If AC profile(s) are provided by the EEC, and the Application group profile is not provided, the ECS identifies the EES(s) based on the provided AC profile(s) and the UE location.

   When Application group profile is provided in the request,

   - if the ECS-ER is not available, then
     - the ECS identifies EES(s) based on the information contained in the request (e.g.AC profile, Application group profile, UE location);
   - if the ECS-ER is available, and:

- EES information is not available corresponding to the Application Group ID, then the ECS identifies EES(s) and stores the identified EES(s)'s information and related Application group ID into the ECS-ER; or

- EES information is available corresponding to the Application Group ID, then the ECS retrieves the EES (s) information corresponding to the Application Group ID from the ECS-ER.

NOTE 2: It is up to the ASP or the EES to determine validity of the application group.

The ECS may take Group Geographical Service Area information and KPI requirements of the AC to determine the EES(s) corresponding to the Application group ID.

When neither Application group profile nor AC profiles(s) are provided, then:

- if available, the ECS identifies the EES(s) based on the UE-specific service information at the ECS and the UE location;

- ECS identifies the EES(s) by applying the ECSP policy (e.g. based only on the UE location);

Furthermore, the ECS may identify the EES based on the EEC service continuity support information and EES service continuity support information.

NOTE 3: Details of the UE-specific service information and how it is available at the ECS is out of scope.

NOTE 4: Both steps are evaluated prior to sending a response.

If desired ECSP identifier(s) is provided by the EEC, the ECS identifies the EES(s) to be sent in step 3 based on registered ECSP identifier in EES profile and the desired ECSP identifier(s).

NOTE 5: For EEC desired ECSP identifier usage, it is assumed that the ECSP providing the EES and PLMN operator are the same organization and an ECSP providing the EES (desired by the EEC) registers its EES in ECS provided by another ECSP based on service agreement to provide services to EEC.

The ECS also determines other information that needs to be provisioned, e.g. identification of the EDN, EDN service area, EES endpoints.

If ECS does not identify any suitable EES(s) based on EDN configuration available at the ECS and UE's location, the ECS determines a partner ECS that may satisfy the requirements. Based on ECSP policy, the ECS may use preconfigured or OAM configured information about the partner ECSs or ECS discovery via ECS-ER as specified in clause 8.17.2.3 or both.

If required by the ECSP policies, the ECS may use service provisioning information retrieval procedure as specified in clause 8.17.2.4 to obtain service provisioning information from the partner ECS.

NOTE 6: ECSP policies can restrict sharing partner ECSP's information with the EEC.

When the bundle EAS information is provided, then;

- If bundle EAS information includes EAS bundle identifier, the ECS identifies all the EES(s) providing the same EAS bundle identifier.

- If bundle EAS information includes a list of EASIDs, the ECS identifies the one or more EES which support all of the EASs within the same EDN based on the EDN information obtained in the EES profile.

3. If the processing of the request was successful, the ECS responds to the EEC's request with a service provisioning response. If the ECS has identified the relevant EES(s) information, the service provisioning response includes a list of EDN configuration information, e.g. identification of the EDN, EDN service area, and the required information (e.g. URI, IP address) for establishing a connection to the EES.

   The ECS may provide associated EES(s) information (one or more EES information) in the service provisioning response along with the bundle EAS information.

   If the alternative ECS(s) has been identified in step 2, the ECS sends a successful response including the Redirect information element containing the list of ECS(s) configuration information indicating that alternative ECS(s) is available for service provisioning request. The response may include information such as DNN and S-NSSAI for roaming UEs to establish a PDU session with the ECS as specified in 3GPP TS 23.548 [20].

If the ECS is not provisioned with any EDN configuration information or is unable to determine either the EES information or the partner ECS information using the inputs in service provisioning request, UE-specific service information at the ECS or the ECSP's policy, the ECS shall reject the service provisioning request and respond with an appropriate failure cause.

If the service provisioning response contains a list of ECS configuration information, the EEC may initiate service provisioning procedure with one or more ECS(s) provided in the response. If the UE is roaming to a V-PLMN and the ECS configuration information includes V-PLMN ID in the list of Supported PLMN ID(s), the EEC establishes a connection with the V-ECS as specified in 3GPP TS 23.548 [20]. The connection with the V-ECS can be a HR-SBO PDU session or an LBO PDU session based on the information received from the ECS.

If the EDN configuration information includes an LADN DNN as an identifier for the EDN, the EEC considers the LADN as the EDN. Therefore, the service area of EDN is the LADN Service Area which can be discovered using the UE Registration Procedure.

The EEC may cache the service provisioning information (e.g. EES endpoint) for subsequent use and avoid the need to repeat step 1. If the Lifetime IE is included in the Service provisioning response, then the EEC may cache and reuse the Service provisioning information only for the duration specified by the Lifetime IE, without the need to repeat step 1.

If the ECS provided information regarding the service continuity support of individual EESs, the EEC may take this information into account when selecting an EES for EEC registration, EAS discovery or T-EAS discovery, respectively.

If for multiple EES(s), the instantiable EAS information IE for an EAS is not available or the instantiable EAS information IE is set to instantiated or instantiable, the EEC can select one or more such EES to perform EAS discovery. For EAS discovery to mitigate the waste of EDN resources EEC considers the instantiable EAS information and the associated instantiation criteria, the EEC selects one EES, if the EAS instantiation status corresponding to the EASID requested by AC/EEC is instantiable but not yet instantiated (i.e. no instantiated EAS).

NOTE 7: If the service provisioning request fails, the EEC can resend the service provisioning request again, taking into account the received failure cause.

After the EEC establishes a connection to an EES using information received in step 3, the EES can issue an AF request to influence traffic routing as specified in 3GPP TS 23.501 [2] clause 5.6.7 in order to influence the user plane path to this connected EES.

NOTE 8: For example, using a particular DNAI to reach the data network containing the EES might be necessary to meet AC service KPIs.

NOTE 9: If the EAS instantiation fails based on the selected EES, the EEC may retry the EAS discovery request to another EES (e.g. selecting another one EES based on the instantiable EAS information).

8.3.3.2.3 Subscribe-notify model

8.3.3.2.3.1 General

Clause 8.3.3.2.3.2 and clause 8.3.3.2.3.3 together illustrate the service provisioning procedure based on Subscribe/Notify model.

Clause 8.3.3.2.3.4 illustrates the service provisioning update procedure.

Clause 8.3.3.2.3.5 illustrates the service provisioning unsubscribe procedure.

8.3.3.2.3.2 Subscribe

Figure 8.3.3.2.3.2-1 illustrates the service provisioning subscription procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has been pre-configured or has discovered the address (e.g. URI) of the ECS;
2. The EEC has been authorized to communicate with the ECS as specified in clause 8.11;
3. The UE Identifier is either preconfigured or resulted from a successful authorization;
4. The ECS is configured with ECSP's policy for service provisioning; and

5. The EEC has optionally acquired a Notification Target Address to be used in its subscriptions to notifications.

NOTE 1: Details of ECSP's policy are out of scope.

NOTE 2: How the EEC acquires the notification target address or a notification channel URI to receive the notifications is out of scope of this release. The notification target address can terminate at the EEC (e.g. in an IoT device) if the deployment supports EEC reachability, or it can terminate at a push notification service. Details of the push notification service are out of scope of this release.

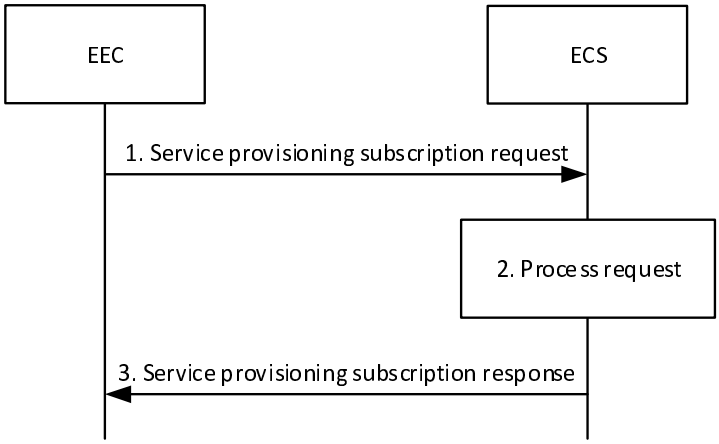

Figure 8.3.3.2.3.2-1: Service provisioning subscription

1. The EEC sends a service provisioning subscription request to the ECS. The service provisioning subscription request includes the security credentials of the EEC received during EEC authorization procedure and Notification Target Address (e.g. URL) and may include the UE identifier such as GPSI, connectivity information, proposed expiration time and AC Profile information. EEC may provide its desired ECSP identifier(s) in the service provisioning request based on EEC preference.

   If the application triggering is supported and required by the EEC, the EEC may include the EEC Triggering Request information element instead of the Notification Target Address in the request message.

2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. If required, the ECS may utilize the capabilities (e.g. UE location or user plane management event notification service if available) of the 3GPP core network as specified in clause 8.10.2. If the request is authorized, the ECS creates and stores the subscription for provisioning.

NOTE 3: The ECS can monitor the user plane path change for EDGE-1 traffic toward EES(s) by utilizing the user plane management event notification service specified in 3GPP TS 23.501 [2]. Based on target DNAI reported from 5GC the ECS can notify more suitable EES(s) to the EEC.

3. If the processing of the request was successful, the ECS responds with a service provisioning subscription response, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EEC shall send a Service provisioning subscription update request prior to the expiration time. If a Service provisioning subscription update request is not received prior to the expiration time, the ECS shall treat the EEC as implicitly unsubscribed.

   If the ECS is unable to determine the EES information using the inputs in service provisioning subscription request, UE-specific service information at the ECS or the ECSP policy, the ECS shall reject the service provisioning subscription request and respond with an appropriate failure cause.

NOTE 4: If the service provisioning subscription request fails, the EEC can resend the service provisioning subscription request again, taking into account the received failure cause.

8.3.3.2.3.3 Notify

Figure 8.3.3.2.3.3-1 illustrates the service provisioning notification procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has subscribed with the ECS for the provisioning information as specified in clause 8.3.3.2.3.2.

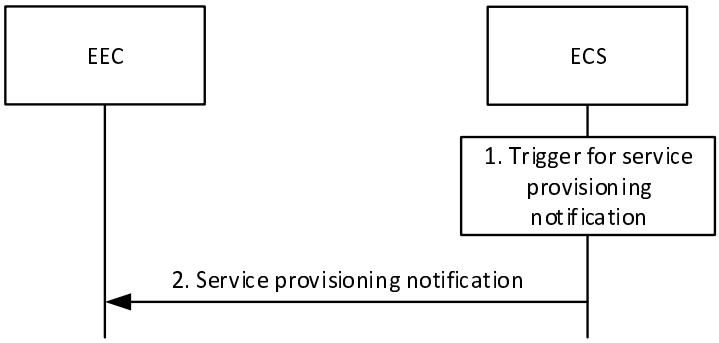

Figure 8.3.3.2.3.3-1: Service provisioning notification

1. An event occurs at the ECS that satisfies trigger conditions for updating service provisioning of a subscribed EEC. If UE's location information is not available, the ECS may obtain the UE location by utilizing the capabilities of the 3GPP core network as specified in clause 8.10.2. If the UE serving PLMN identifier is not provided by the EEC in the connectivity information of the service provisioning request, the ECS may invoke the NEF monitoring event API as described in 3GPP TS 29.522 [4] and 3GPP TS 29.122 [5] to obtain the UE roaming status and serving PLMN identifier. If the UE is roaming, the ECS may use the serving PLMN identifier to determine the partner ECS information to be provided to the EEC in the service provisioning notification. If AC profile(s) were provided by the EEC during subscription creation, the ECS identifies the EES(s) based on the provided AC profile(s) and the UE location. If AC profiles(s) were not provided, then:

   - if available, the ECS identifies the EES(s) based on the UE-specific service information at the ECS and the UE location;

   - ECS identifies the EES(s) by applying the ECSP policy (e.g. based only on the UE location);

NOTE 1: Details of the UE-specific service information and how it is available at the ECS is out of scope.

NOTE 2: Both steps are evaluated prior to sending a response.

If desired ECSP identifier(s) provided by the EEC, the ECS identifies the EES(s) to be sent in step 2 based on registered ECSP identifier in EES profile and the desired ECSP identifier(s).

NOTE 3: For EEC desired ECSP identifier usage, it is assumed that the ECSP providing the EES and PLMN operator are the same organization and an ECSP providing the EES (desired by the EEC) registers its EES in ECS provided by another ECSP based on service agreement to provide services to EEC.

The ECS also determines other information that needs to be provisioned, e.g. identification of the EDN, EDN service area, EES endpoints.

If ECS does not identify any suitable EES(s) based on EDN configuration available at the ECS and UE’s location, the ECS determines a partner ECS that may satisfy the requirements. Based on ECSP policy, the ECS may use preconfigured or OAM configured information about the partner ECSs or ECS discovery via ECS-ER as specified in clause 8.17.2.3 or both. If required by the ECSP policies, the ECS may use service provisioning information retrieval procedure as specified in clause 8.17.2.4 to obtain service provisioning information from the partner ECS.

NOTE 4: ECSP policies can restrict sharing partner ECSP's information with the EEC.

When the bundle EAS information is provided, then;

- If bundle EAS information included EAS bundle identifier, the ECS identifies all the EES(s) providing the same EAS bundle identifier.

- If bundle EAS information includes a list of EASIDs, the ECS identifies the one or more EES which support all of the EASs within the same EDN based on the EDN information obtained in the EES profile.

If the application triggering is supported and required by the EEC as indicated in EEC Triggering Request IE of the Service Provisioning Subscription Request, then the ECS performs the EEC triggering service as described in the clause 8.16.1 and skips the step 2.

2. The ECS sends a provisioning notification to the EEC. If the ECS has identified the relevant EES(s) information, the service provisioning notification includes the list of EDN configuration information determined in step 1. If the ECS has determined suitable partner ECS(s), the service provisioning notification includes a list of ECS configuration information and may include information for roaming UEs to establish PDU session with the ECS as specified in 3GPP TS 23.548 [20]. The ECS may provide associated EES(s) information (one or more EES information) in the service provisioning response along with the bundle EAS information.

If the service provisioning notification contains a list of ECS configuration information, the EEC may initiate service provisioning procedure with one or more ECS(s) provided in the notification. If the UE is roaming to a V-PLMN and the ECS configuration information includes V-PLMN ID in the list of Supported PLMN ID(s), the EEC establishes a PDU session with the V-PLMN to access the ECS in the visited network as specified in 3GPP TS 23.548 [20].

If the EDN configuration information in the service provisioning notification includes an LADN DNN as an identifier for the EDN, the EEC considers the LADN as the EDN. Therefore, the service area of EDN is the LADN Service Area, which can be discovered using the UE Registration Procedure.

If the ECS provided information regarding the service continuity support of individual EESs, the EEC may take this information into account when selecting an EES for EEC registration, EAS discovery or T-EAS discovery, respectively.

After the EEC establishes a connection to an EES using information received in step 2, the EES can issue an AF request to influence traffic routing as specified in 3GPP TS 23.501 [2] clause 5.6.7 in order to influence the user plane path to this connected EES.

NOTE 5: For example, using a particular DNAI to reach the data network containing the EES might be necessary to meet AC service KPIs.

8.3.3.2.3.4 Subscription update

Figure 8.3.3.2.3.4-1 illustrates the service provisioning subscription update procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has subscribed with the ECS for the provisioning information as specified in clause 8.3.3.2.3.2.

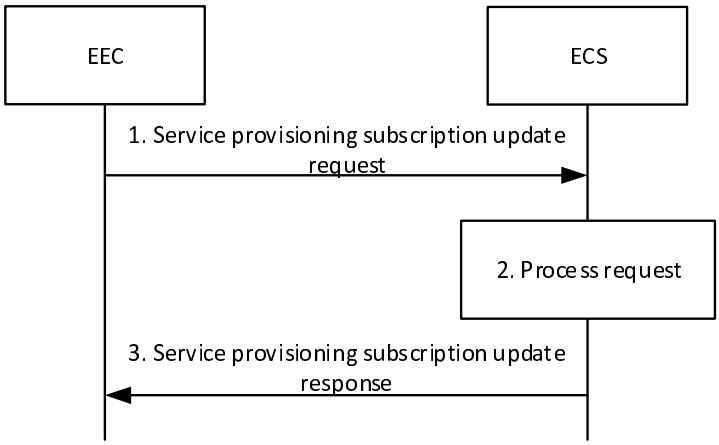

Figure 8.3.3.2.3.4-1: Service provisioning subscription update

1. The EEC sends a service provisioning subscription update request to the ECS. The service provisioning subscription update request includes the security credentials of the EEC received during EEC authorization procedure along with the subscription identifier and may include the UE identifier such as GPSI, connectivity information, proposed expiration time for the updated subscription and AC profile(s).

2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. If required, the ECS may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.2. If authorized, the ECS updates the stored subscription for provisioning as requested in step 1.

3. The ECS responds with a service provisioning subscription update response, which may include the expiration time, indicating when the updated subscription will automatically expire. To maintain the subscription, the EEC shall send a Service provisioning subscription update request prior to the expiration time. If a Service provisioning subscription update request is not received prior to the expiration time, the ECS shall treat the EEC as implicitly unsubscribed.

8.3.3.2.3.5 Unsubscribe

Figure 8.3.3.2.3.5-1 illustrates the service provisioning unsubscribe procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has subscribed with the ECS for the provisioning information as specified in clause 8.3.3.2.3.2.

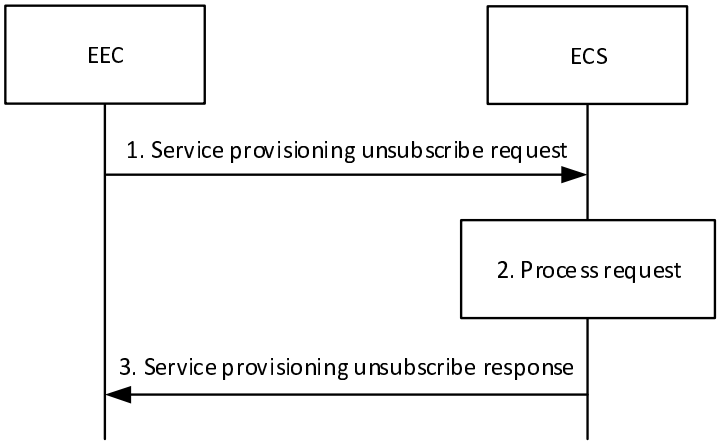

Figure 8.3.3.2.3.5-1: Service provisioning unsubscribe

1. The EEC sends a service provisioning unsubscribe request to the ECS. The service provisioning unsubscribe request includes the security credentials of the EEC received during EEC authorization procedure along with the subscription identifier.

2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. If authorized, the ECS cancels the subscription for provisioning as requested in step 1.

3. The ECS responds with a service provisioning unsubscribe response.

8.3.3.3 Information flows

8.3.3.3.1 General

The following information flows are specified for service provisioning:

- Service provisioning request and response;

- Service provisioning subscription request and response;
- Service provisioning notification;
- Service provisioning update request and response; and
- Service provisioning unsubscribe request and response.

8.3.3.3.2 Service provisioning request

Table 8.3.3.3.2-1 describes the information elements for service provisioning request from the EEC to the ECS.

Table 8.3.3.3.2-1: Service provisioning request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
AC Profile(s) (NOTE)	O	Information about services the EEC wants to connect to, as described in Table 8.2.2-1.
Application information (NOTE)	O	List of information about services the EEC wants to connect to, including the option to provide application group profile information.
> AC Profile	M	Application Profile as described in Table 8.2.2-1.
> Application Group profile	O	Application Group profile associated with the AC Profile, as defined in Table 8.2.11-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC. When requesting service provisioning for T-EES discovery, if the EEC requires that T-EES must support "EEC executed ACR via T-EES" scenario, then EEC includes only "EEC executed ACR via T-EES" in this IE
UE Identifier	O	The identifier of the UE (i.e. GPSI)
Connectivity information	O	List of connectivity information for the UE, e.g. PLMN ID, SSID.
UE location	O	The location information of the UE. The UE location is described in clause 7.3.2.
ECSP identifiers	O	The list of EEC preferred ECSPs that provide the EES.
NOTE: Only one of AC Profile(s) or Application information shall be provided.		

8.3.3.3.3 Service provisioning response

Table 8.3.3.3.3-1 describes the information elements for service provisioning response from the ECS to the EEC.

Table 8.3.3.3.3-1: Service provisioning response

Information element	Status	Description
Successful response	O	Indicates that the service provisioning request was successful.
> List of EDN configuration information	M	List of EDN configuration information as defined in Table 8.3.3.3.3-2.
Failure response	O	Indicates that the service provisioning request failed.
> Cause	O	Indicates the cause of service provisioning request failure.
Redirect	O	Indicates redirection to (an)other ECS(s).
> ECS(s) information	M	Endpoint address of ECS(s) to which the UE is redirected for service provisioning.
> DNN	O	DNN required for establishing PDU Session to the redirected ECS
> S-NSSAI	O	S-NSSAI required for establishing PDU Session to the redirected ECS

Table 8.3.3.3.3-2: EDN configuration information

Information element	Status	Description
EDN connection information (NOTE 1)	M	Information required by the UE to establish connection with the EDN.
> DNN/APN	M	Data Network Name/Access Point Name
> S-NSSAI	O	Network Slice information
> EDN Topological Service Area	O	The EDN serves UEs that are connected to the Core Network from one of the cells included in this service area. See possible formats in Table 8.2.7-1.
List of EESs	M	List of EESs of the EDN.
> EESID	M	The identifier of the EES
> EES Endpoint	M	The endpoint address (e.g. URI, IP address) of the EES
> EAS information (NOTE 2)	O	EAS registration and associated bundle information.
>> EASID	M	An EASID registered or expected to be registered with the EES.
>> List of EAS bundle information	O	List of EAS bundles to which the EAS belongs.
>>> Bundle ID (NOTE 3)	O	Bundle ID as described in clause 7.2.10.
>>> List of EASIDs (NOTE 3)	O	A list of the EASIDs of the EASs in the bundle.
> Application Group ID list (NOTE 5)	O	List of Application Group IDs associated with EAS
> Instantiable EAS information	O	The EAS instantiation status per EASID (e.g. instantiated, instantiable but not be instantiated yet)
>> Instantiation criteria (NOTE 4)	O	The criteria upon which EAS can be instantiated (e.g. based on specific date and time).
> ECSP ID	O	The identifier of the ECSP that provides the EES.
> EES Topological Service Area	O	The EES serves UEs that are connected to the Core Network from one of the cells included in this service area. EECs in UEs that are located outside this area shall not be served. See possible formats in Table 8.2.7-1.
> EES Geographical Service Area	O	The area being served by the EES in Geographical values (as specified in clause 7.3.3.3)
> List of EES DNAI(s)	O	DNAI(s) associated with the EES/EAS. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [2].
> EES Service continuity support	O	Indicates if the EES supports service continuity or not. This IE also indicates which ACR scenarios are supported by the EES.
> EEC registration configuration	M	Indicates whether the EEC is required to register on the EES to use edge services or not.
> Security Credential	O	Indicates the security credential sent by the ECS. The security credential is used by EEC to communicate with the EES as specified in 3GPP TS 33.558 [23], clause 6.3.
Lifetime	O	Time duration for which the EDN configuration information is valid and supposed to be cached in the EEC.

NOTE 1: If the UE is provisioned or pre-configured with URSP rules by the HPLMN or serving SNPN, the UE handles the precedence between EDN connection info and URSP rules as defined in 3GPP TS 23.503 [12] clause 6.1.2.2.1. EDN connection info is considered to be part of UE Local Configurations.
NOTE 2: EAS information is limited to the EEC requested applications. If no AC profiles were present in the service provisioning request, the EAS information is subject to the ECSP policy (e.g. no EAS information or a subset of EAS information related to the EES).
NOTE 3: At least one of the IEs shall be present if EAS bundle information is provided.
NOTE 4: "Instantiation criteria" IE shall be present only when the value of "Instantiable EAS information" IE is "instantiable but not be instantiated yet".
NOTE 5: "Application Group ID list" IE shall be present when "Application Group profile" is included for "AC profile" in service provisioning request as specified in clause 8.3.3.3.2.

8.3.3.3.4 Service provisioning subscription request

Table 8.3.3.3.4-1 describes the information elements for service provisioning subscription request from the EEC to the ECS.

Table 8.3.3.3.4-1: Service provisioning subscription request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Notification Target Address (NOTE 1, NOTE 2)	O	The Notification Target Address (e.g. URL) where the notifications destined for the EEC should be sent to.
AC profile(s)	O	Information about services the EEC wants to connect to, as described in Table 8.2.2-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
UE Identifier	O	The identifier of the UE (i.e., GPSI)
Connectivity information	O	List of connectivity information for the UE, e.g. PLMN ID, SSID.
Proposed expiration time	O	Proposed expiration time for the subscription
ECSP identifiers	O	The list of EEC preferred ECSPs that provide the EES.
EEC Triggering request (NOTE 2)	O	Indicates that EEC Triggering is requested
NOTE 1: When SEAL NMS is used this IE is same as Callback URL in SEAL notification management service. NOTE 2: One of them may be provided.		

8.3.3.3.5 Service provisioning subscription response

Table 8.3.3.3.5-1 describes the information elements for service provisioning subscription response from the ECS to the EEC.

Table 8.3.3.3.5-1: Service provisioning subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.3.3.3.6 Service provisioning notification

Table 8.3.3.3.6-1 describes the information elements for service provisioning notification from the ECS to the EEC.

Table 8.3.3.3.6-1: Service provisioning notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the ECS for the request
List of EDN configuration information (NOTE)	M	List of EDN configuration information as defined in Table 8.3.3.3.3-2.
Redirect (NOTE)	O	Indicates redirection to (an)other ECS(s).
> ECS(s) information	M	Endpoint address of ECS(s) to which the UE is redirected for service provisioning.
> DNN	O	DNN required for establishing PDU Session to the redirected ECS
> S-NSSAI	O	S-NSSAI required for establishing PDU Session to the redirected ECS
NOTE: One of the IEs shall be present.		

NOTE: When SEAL NMS is used, Service provisioning notification is the Notification data in SEAL Notification message of clause 17.3.2.4 in 3GPP TS 23.434 [13].

8.3.3.3.7 Service provisioning subscription update request

Table 8.3.3.3.7-1 describes the information elements for service provisioning subscription update request from the EEC to the ECS.

Table 8.3.3.3.7-1: Service provisioning subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Connectivity information	O	List of connectivity information for the UE, e.g. PLMN ID, SSID.
Proposed expiration time	O	Proposed expiration time for the subscription
AC profile(s)	O	Information about services the EEC wants to connect to, as described in Table 8.2.2-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.

8.3.3.3.8 Service provisioning subscription update response

Table 8.3.3.3.8-1 describes the information elements for service provisioning subscription update response from the ECS to the EEC.

Table 8.3.3.3.8-1: Service provisioning subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.3.3.3.9 Service provisioning unsubscribe request

Table 8.3.3.3.9-1 describes the information elements for service provisioning unsubscribe request from the EEC to the ECS.

Table 8.3.3.3.9-1: Service provisioning unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the ECS
Security credentials	M	Security credentials of the EEC

8.3.3.3.10 Service provisioning unsubscribe response

Table 8.3.3.3.10-1 describes the information elements for service provisioning unsubscribe response from the ECS to the EEC.

Table 8.3.3.3.10-1: Service provisioning unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.3.3.4 APIs

8.3.3.4.1 General

Table 8.3.3.4.1-1 illustrates the API for service provisioning.

Table 8.3.3.4.1-1: Eecs_ServiceProvisioning API

API Name	API Operations	Operation Semantics	Consumer(s)
Eecs_ServiceProvisioning	Request	Request/Response	EEC
	Subscribe	Subscribe/Notify	EEC
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.3.3.4.2 Eecs_ServiceProvisioning_Request operation

API operation name: Eecs_ServiceProvisioning_Request

Description: The consumer requests for one time service provisioning information.

Inputs: See clause 8.3.3.3.2.

Outputs: See clause 8.3.3.3.3.

See clause 8.3.3.2.2 for details of usage of this operation.

8.3.3.4.3 Eecs_ServiceProvisioning_Subscribe operation

API operation name: Eecs_ServiceProvisioning_Subscribe

Description: The consumer subscribes for service provisioning information.

Inputs: See clause 8.3.3.3.4.

Outputs: See clause 8.3.3.3.5.

See clause 8.3.3.2.3.2 for details of usage of this operation.

8.3.3.4.4 Eecs_ServiceProvisioning_Notify operation

API operation name: Eecs_ServiceProvisioning_Notify

Description: The consumer is notified with service provisioning information.

Inputs: See clause 8.3.3.3.6.

Outputs: None.

See clause 8.3.3.2.3.3 for details of usage of this operation.

8.3.3.4.5 Eecs_ServiceProvisioning_UpdateSubscription operation

API operation name: Eecs_ServiceProvisioning_UpdateSubscription

Description: The consumer updates an existing subscription for service provisioning information.

Inputs: See clause 8.3.3.3.7.

Outputs: See clause 8.3.3.3.8.

See clause 8.3.3.2.3.4 for details of usage of this operation.

8.3.3.4.6 Eecs_ServiceProvisioning_Unsubscribe operation

API operation name: Eecs_ServiceProvisioning_Unsubscribe

Description: The consumer cancels an existing subscription for service provisioning information.

Inputs: See clause 8.3.3.3.9.

Outputs: See clause 8.3.3.3.10.

See clause 8.3.3.2.3.5 for details of usage of this operation.

8.4 Registration

8.4.1 General

Registration procedures allow entities in the edge deployment to deliver information to other entities.

The following registrations are supported:

- EEC registration with EES;
- EAS registration with EES; and
- EES registration with ECS.

8.4.2 EEC Registration

8.4.2.1 General

An EEC performs registration with an EES in order to provide information that can be used by the EES in Edge Computing services. The procedure also enables initialization, update and removal of the EEC context information at the EES. The context may be further used for edge-specific operations or processing, e.g. analytics.

An EEC may be registered with one or more EESs on behalf of one or more ACs simultaneously.

In deployments with bundled EAS(s) registered to different EESs, to perform EEC registration (if needed) the EEC sends the EEC registration message to all the associated EES for the EAS bundle.

8.4.2.2 Procedures

8.4.2.2.1 General

Following are supported for EEC registration:

- EEC registration procedure;
- EEC registration update procedure;
- EEC de-registration procedure; and
- EEC Context relocation procedure.

NOTE: In this version of specification, each registration procedure provides for registering a single EEC per UE.

8.4.2.2.2 EEC registration

Figure 8.4.2.2.2-1 illustrates EEC registration procedure.

Pre-conditions:

1. The EEC is authorized to access the EES for the purpose of performing registration and has received relevant security credentials as specified in clause 8.11; and
2. The EEC has received service provisioning information from the ECS, including information for accessing the EES.

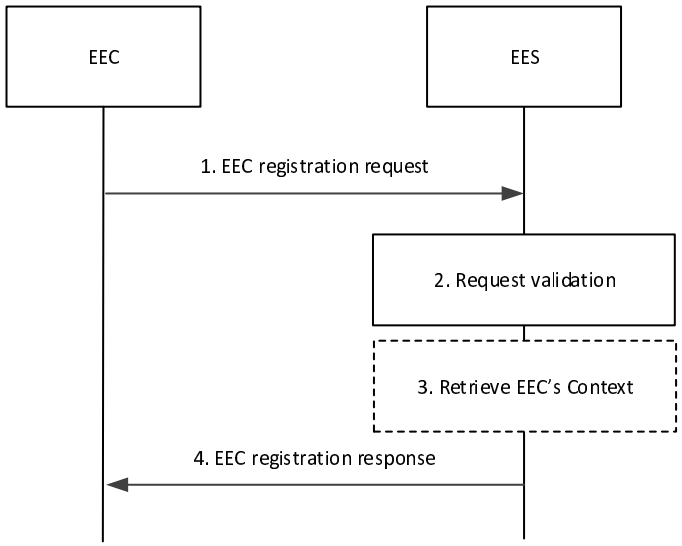

Figure 8.4.2.2.2-1: EEC registration procedure

1. The EEC sends EEC registration request to the EES. The request from the client includes the security credentials received after successful authorization for edge computing services and may include a proposed expiration time. The request also optionally includes information indicating to the EES how the EEC expects to use the services of the EES. The EEC may include indication for UE mobility support requirement to the EES.

   If the EEC is moving to this EES from the purview of another EES, called S-EES, the request from the EEC may include the identity and endpoint of the S-EES and an EEC context ID that was provided by the S-EES to maintain continuity of the EEC context and to authorize EEC context relocation. If the EEC registration is being performed as part of ACR, the EEC shall not include the S-EES endpoint and the EEC context ID.

2. Upon receiving the request from the EEC, the EES validates the registration request and verifies the security credentials. The EES further determines whether the requirements that were indicated in the AC Profile(s) can be fulfilled e.g., without failing to meet the requirements of the already registered EECs, and reserves corresponding resources (e.g., for EASs). If the AC Profile(s) include EAS bundle information the reserved EAS resources are apportioned among the EASs in the bundle, based on the indicated requirements and local policies.

   NOTE 1: Resource reservation at EEC registration ensures that the EES provides services for the duration of the registration.

   If the EEC provides in the registration request the EAS selection request indicator and based on EES local policies, the EES selects EASs providing the capabilities required by the AC Profile(s), reserves the corresponding resources, and provides the information to the EEC in the registration response.

   If bundle EAS information (either as EAS bundle identifier or as a list of EASIDs) is included and the EAS selection request indicator is set, then the EES determines whether all or a subset of the EAS(s) in the bundle are registered and instantiated. If only a subset of bundle EASs is found, the EES may determine whether instantiable but not yet instantiated EASs match the subset of remaining (i.e. not yet found) bundle EASs and performs the dynamic EAS instantiation triggering procedure in clause 8.12 for this subset.

   If the EEC provides in the registration request a UE type, the EES may use this information to apply UE-type-specific local policies.

   NOTE 2: Without any indication from UE (either EAS selection request indication or UE type), the EES handling is as per R17 procedure.

   NOTE 3: The "UE type" IE as present in EEC registration request message can be used by EES to identify "constrained device".

3. Upon successful validation of the request, if the received EEC registration request contains an EEC context ID and a S-EES Endpoint, the EES performs an EEC Context Pull relocation (clause 8.9.2.2) from the S-EES. The source and target EES perform EEC Context handling as detailed in clause 8.9.1.

   NOTE 4: Only a single EEC Context ID may be provided in the EEC registration request.

   NOTE 5: In this version of specification, each registration procedure relocates a single EEC context.

   NOTE 6: Step 3 is executed when EEC determines to change its connection from S-EES to T-EES and ACR is not required.

   If the EEC registration request fails after the EEC Context Pull relocation, e.g., the EES cannot reserve the necessary resources while meeting the capability requirements of the existing registered EECs, the EES shall determine the EEC Context information stale and send a failure response with a corresponding cause.

4. The EES sends a successful EEC registration response, which includes the registration ID and may include a newly assigned EEC context ID. If the EEC registration request contains AC Profile(s), and the EES determines that the requirements indicated in the AC profile(s) cannot be fulfilled for some of the AC profile(s), the EES shall include the list of ACIDs of such AC Profile(s) and may include appropriate reasons. If step 3 was executed, the EEC registration response also includes EEC context retrieval result. The EEC stores the new EEC context ID and uses it if and when it registers with another EES. The EES may also provide an expiration time to indicate to the EEC when the registration will automatically expire. To maintain the registration, the EEC shall send a registration update request prior to the expiration. If a registration update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly de-registered.

   If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC performs the required EDGE-1 subscriptions at the T-EES.

8.4.2.2.3 EEC registration update

Figure 8.4.2.2.3-1 illustrates EEC registration update procedure.

Pre-conditions:

1. EEC has already registered with the EES.

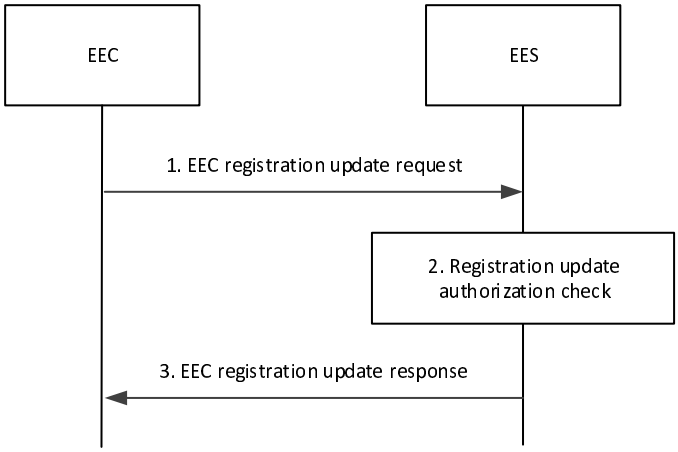

Figure 8.4.2.2.3-1: EEC registration update procedure

1. The EEC sends EEC registration update request to the EES. The request from the client includes the security credentials received after successful authorization for edge computing services and may include a proposed expiration time and AC profile(s) parameters, including new or updated selected EAS information. The EEC may include indication for UE mobility support requirement to the EES.

2. Upon receiving the request from the EEC, the EES validates the registration update request and verifies the security credentials.

3. Upon successful validation of the request, the EES sends a successful registration update response, which may include updated expiration time to indicate to the EEC when the updated registration will automatically expire. If the EEC registration update request contains AC Profile(s), and the EES determines that the requirements indicated in the AC profile(s) cannot be fulfilled for some of the AC profile(s), the EES shall include the list of ACIDs of such AC Profile(s) and may include appropriate reasons. To maintain the registration, the EEC shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly de-registered.

8.4.2.2.4 EEC de-registration

Figure 8.4.2.2.4-1 illustrates EEC de-registration procedure.

Pre-conditions:

1. EEC has already registered with the EES.

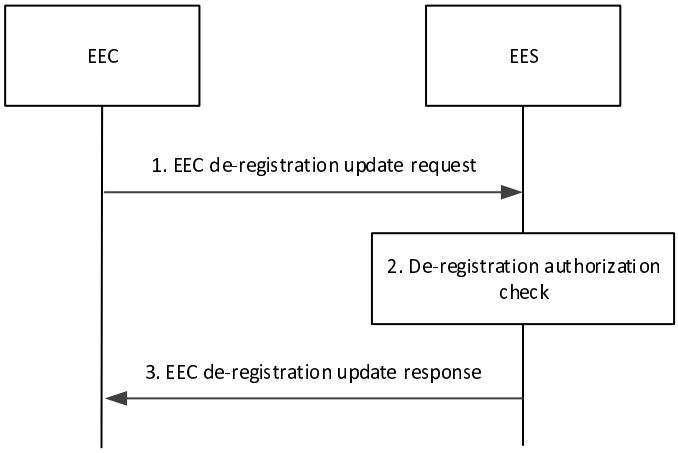

Figure 8.4.2.2.4-1: EEC de-registration procedure

1. The EEC sends EEC de-registration request to the EES. The request from the client includes the security credentials received after successful authorization for edge computing services.

2. Upon receiving the request from the EEC, the EES validates the de-registration request and verifies the security credentials.

3. Upon successful authorization, the EES sends a successful de-registration response.

8.4.2.3 Information flows

8.4.2.3.1 General

The following information flows are specified for EEC registration:

- EEC registration request and response;
- EEC registration update request and response; and
- EEC registration de-registration request and response.

8.4.2.3.2 EEC registration request

Table 8.4.2.3.2-1 describes information elements in the EEC registration request from the EEC to the EES.

Table 8.4.2.3.2-1: EEC registration request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
UE Identifier	O	The identifier of the hosting UE (i.e., GPSI)
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
AC Profile(s)	O	Profiles of ACs for which the EEC provides edge enabling services. AC Profiles are further described in Table 8.2.2-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
EAS selection request indicator	O	Indicates the request for EAS selection support from the EES (e.g., for constrained device).
UE type	O	Indicates UE or device type (e.g. constrained device)
Proposed expiration time	O	Proposed expiration time for the registration.
EEC context ID (NOTE)	O	Identifier of the EEC context obtained from a previous registration.
Source EESID (NOTE)	O	Identifier of the EES that provided EEC context ID.
Source EES Endpoint (NOTE)	O	The endpoint address (e.g. URI, IP address) of the EES that provided EEC context ID.
UE Mobility Support Requirement	O	Indicates UE requires mobility support or not
NOTE: This IE shall not be present when EEC registration is performed as part of ACR.		

8.4.2.3.3 EEC registration response

Table 8.4.2.3.3-1 describes information elements in the EEC registration response from the EES to the EEC.

Table 8.4.2.3.3-1: EEC registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the EEC registration.
> Expiration time (NOTE)	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time.
> EEC context ID	O	Identifier of the EEC Context information available at the EES that performed the registration.
> EEC Context Relocation status	O	Indicates whether the EEC context retrieval from the S-EES was successful or not.
> Discovered EAS list	O	List of EASs discovered to provide the capabilities required by the AC Profiles. If the request includes the EAS selection request indicator, then Discovered EAS list shall contain only one selected EAS. If the EES selects no EASs, the list may be empty.
>> EAS profile	M	Profile of the EAS. Each element is described in clause 8.2.4.
> list of unfulfilled AC information	O	List of ACIDs of the AC Profile(s) for which the requirements indicated in the AC profile(s) cannot be fulfilled
>> ACID	M	Application Identifier
>> reason	O	Reason indicating the cause (e.g. EAS not available, requirements cannot be fulfilled)
Failure response	O	Indicates that the registration request failed.
> Cause	M	Provides the cause for registration request failure.
NOTE: The Expiration time IE shall be included if based on the ECSP policy the EES requires EEC to periodically refresh the EEC registration.		

8.4.2.3.4 EEC registration update request

Table 8.4.2.3.4-1 describes information elements in the EEC registration update request from the EEC to the EES.

Table 8.4.2.3.4-1: EEC registration update request

Information element	Status	Description
Registration ID	M	Identifier of the EEC registration.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
AC profile(s)	O	AC Profile as described in Table 8.2.2-1
Proposed expiration time	O	Proposed expiration time for the updated registration.
UE Mobility Support Requirement	O	Indicates UE requires mobility support or not

8.4.2.3.5 EEC registration update response

Table 8.4.2.3.5-1 describes information elements in the EEC registration update response from the EES to the EEC.

Table 8.4.2.3.5-1: EEC registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration update request was successful.
> Expiration time (NOTE)	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time.
> list of unfulfilled AC information	O	List of ACIDs of the AC Profile(s) for which the requirements indicated in the AC profile(s) cannot be fulfilled
>> ACID	M	Application Identifier
>> reason	O	Reason indicating the cause (e.g. EAS not available, requirements cannot be fulfilled)
Failure response	O	Indicates that the registration update request failed.
NOTE: The Expiration time IE shall be included if based on the ECSP policy the EES requires EEC to periodically refresh the EEC registration.		

8.4.2.3.6 EEC de-registration request

Table 8.4.2.3.6-1 describes information elements in the EEC de-registration request from the EEC to the EES.

Table 8.4.2.3.6-1: EEC de-registration request

Information element	Status	Description
Registration ID	M	Identifier of the EEC registration.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.

8.4.2.3.7 EEC de-registration response

Table 8.4.2.3.7-1 describes information elements in the EEC de-registration response from the EES to the EEC.

Table 8.4.2.3.7-1: EEC registration update response

Information element	Status	Description
Successful response	O	Indicates that the de-registration request was successful.
Failure response	O	Indicates that the de-registration request failed.
> Cause	M	Provide the cause for de-registration request failure.

8.4.2.4 APIs

8.4.2.4.1 General

Table 8.4.2.4.1-1 illustrates the API for EEC registration.

Table 8.4.2.4.1-1: Eees_EECRegistration API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EECRegistration	Request	Request/Response	EEC
	Update		
	Deregister		

8.4.2.4.2 Eees_EECRegistration_Request operation

API operation name: Eees_EECRegistration_Request

Description: The consumer requests to register the EEC on the EES.

Inputs: See clause 8.4.2.3.2.

Outputs: See clause 8.4.2.3.3.

See clause 8.4.2.2.2 for details of usage of this operation.

8.4.2.4.3 Eees_EECRegistration_Update operation

API operation name: Eees_EECRegistration_Update

Description: The consumer requests to update the registered information of the EEC on the EES.

Inputs: See clause 8.4.2.3.4.

Outputs: See clause 8.4.2.3.5.

See clause 8.4.2.2.3 for details of usage of this operation.

8.4.2.4.4 Eees_EECRegistration_Deregister operation

API operation name: Eees_EECRegistration_Deregister

Description: The consumer requests to de-register the EEC from the EES.

Inputs: See clause 8.4.2.3.6.

Outputs: See clause 8.4.2.3.7.

See clause 8.4.2.2.4 for details of usage of this operation.

8.4.3 EAS Registration

8.4.3.1 General

The EAS Registration procedure allows an EAS to provide its information to an EES in order to enable its discovery.

If there is a change in the requirements or the information of an EAS, it uses the EAS registration update procedure to update the EES.

The EAS uses the EAS de-registration procedure to remove its information from the EES.

EAS registration at the EES can be time bound. So, to maintain the registration, the EAS needs to send a registration update request prior to the registration expiration time. If a registration update request is not received prior to the registration expiration time, the EES treats the EAS as implicitly de-registered.

NOTE: For registered EAS(s), the EES can request AF traffic influence for any UE, which is implementation specific.

8.4.3.2 Procedures

8.4.3.2.1 General

Following are supported for EAS registration:

- EAS registration procedure;
- EAS registration update procedure; and

- EAS de-registration procedure.

8.4.3.2.2 EAS registration

Pre-conditions:

1. The EAS has been configured with an EASID;
2. The EAS has been configured with the address (e.g. URI) of the EES; and
3. Both the EAS and EES have the necessary credentials to enable communications.

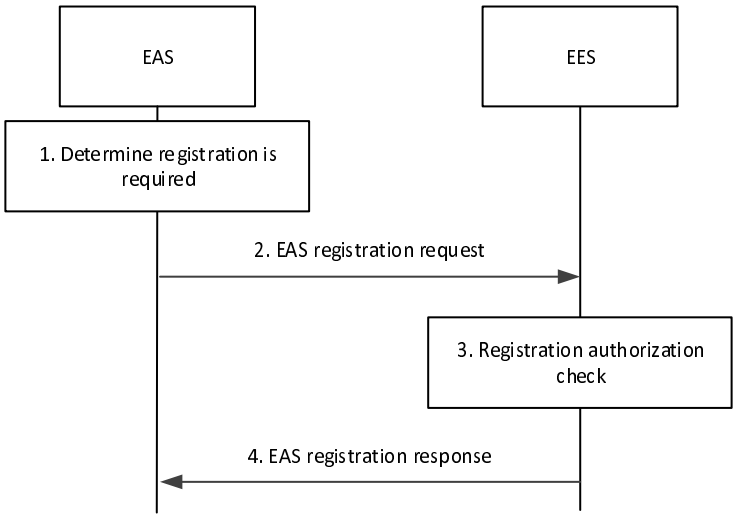

Figure 8.4.3.2.2-1: EAS Registration procedure

1. The EAS determines that registration to the EES is needed (e.g. the EAS is instantiated and started up).
2. The EAS sends an EAS registration request to the EES. The request shall include the EAS profile and may include proposed expiration time for the registration.
3. The EES performs an authorization check to verify whether the EAS has the authorization to register on the EES.
4. Upon successful authorization, the EES stores the EAS Profile for later use (e.g. for serving EAS discovery requests received from EECs, etc.) and replies to the EAS with an EAS registration response. If the request includes bundle ID, the EES stores the received information. The EES may provide an expiration time to indicate to the EAS when the registration will automatically expire. To maintain the registration, the EAS shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the EES shall treat the EAS as implicitly de-registered.

8.4.3.2.3 EAS registration update

Pre-conditions:

1. The EAS has already registered with the EES.

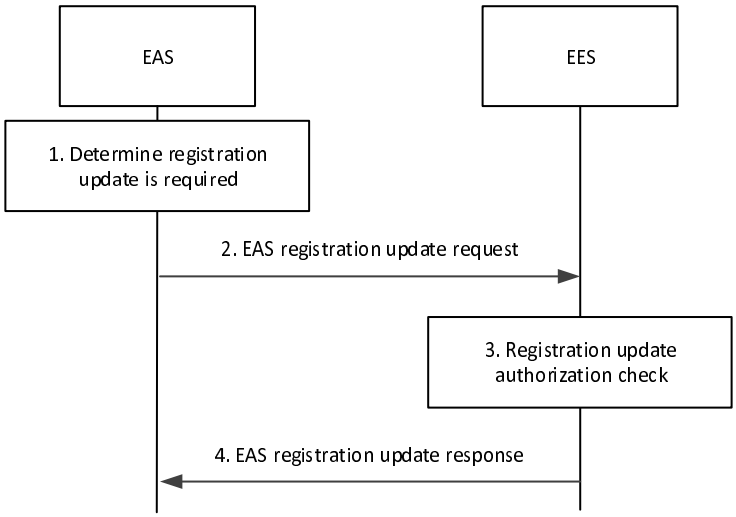

Figure 8.4.3.2.3-1: EAS registration update procedure

1. The EAS determines that its existing registration needs to be updated (e.g. because the EAS's status or availability schedule has changed, or EAS's registration is about to expire).
2. The EAS sends an EAS registration update request to the EES. The request shall include the registration ID and may include the EAS profile and proposed expiration time for the updated registration.
3. The EES performs an authorization check to verify whether the EAS has the authorization to update the registration on the EES.
4. Upon successful authorization, the EES updates the registered EAS Profile and replies to the EAS with an EAS registration update response. If the request includes updated bundle ID, the EES updates the stored information. The EES may provide an updated expiration time to indicate to the EAS when the updated registration will automatically expire. To maintain the registration, the EAS shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the EES shall treat the EAS as implicitly de-registered.

8.4.3.2.4 EAS de-registration

Pre-conditions:

1. The EAS has already registered with the EES.

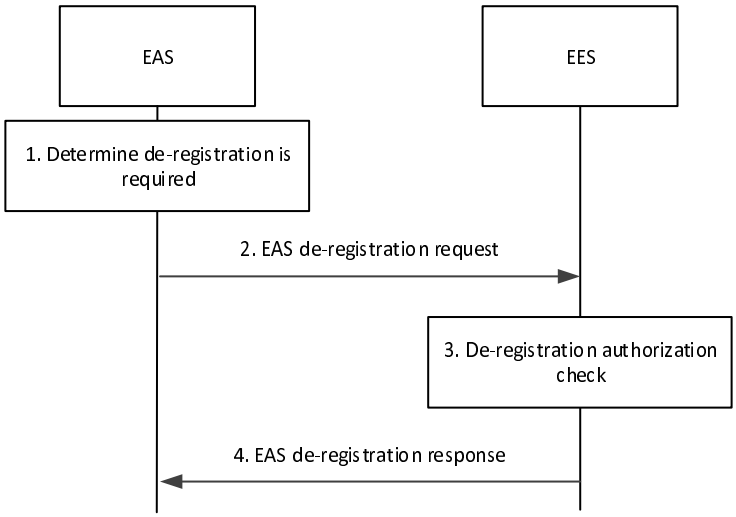

Figure 8.4.3.2.4-1: EAS de-registration procedure

1. The EAS determines that its existing registration needs to be terminated (e.g. because the services of the EAS are not needed anymore).
2. The EAS sends an EAS de-registration request to the EES. The request shall include the registration ID.
3. The EES performs an authorization check to verify whether the EAS has the authorization to de-register explicitly.
4. Upon successful authorization, the EES removes the registered EAS Profile and replies to the EAS with an EAS de-registration response.

8.4.3.3 Information flows

8.4.3.3.1 General

The following information flows are specified for EAS registration:

- EAS registration request and response;
- EAS registration update request and response; and
- EAS registration de-registration request and response.

8.4.3.3.2 EAS registration request

Table 8.4.3.3.1-2 describes information elements in the EAS registration request from the EAS to the EES.

Table 8.4.3.3.2-1: EAS registration request

Information element	Status	Description
EAS Profile	M	EAS Profile as described in Table 8.2.4-1
Security credentials	M	Security credentials of the EAS.
Proposed expiration time	O	Proposed expiration time for the registration

8.4.3.3.3 EAS registration response

Table 8.4.3.3.3-1 describes information elements in the EAS registration response from the EES to the EAS.

Table 8.4.3.3.3-1: EAS registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the registration.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the registration never expires.
Failure response	O	Indicates that the registration request failed.
> Cause	O	Indicates the cause of registration request failure

8.4.3.3.4 EAS registration update request

Table 8.4.3.3.4-1 describes information elements in the EAS registration update request from the EAS to the EES.

Table 8.4.3.3.4-1: EAS registration update request

Information element	Status	Description
Registration ID	M	Identifier of the registration.
Security credentials	M	Security credentials of the EAS
Updated EAS Profile (NOTE)	O	EAS Profile as described in Table 8.2.4-1 with updated information. Included only if there is an update in EAS information.
Proposed expiration time (NOTE)	O	Proposed expiration time for the registration
NOTE: At least one of the IEs is included.		

8.4.3.3.5 EAS registration update response

Table 8.4.3.3.5-1 describes information elements in the EAS registration update response from the EES to the EAS.

Table 8.4.3.3.5-1: EAS registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration update request was successful.
> Expiration time	O	Indicates the expiration time of the updated registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the updated registration never expires.
Failure response	O	Indicates that the registration update request failed.
> Cause	O	Indicates the cause of registration update request failure

8.4.3.3.6 EAS de-registration request

Table 8.4.3.3.6-1 describes information elements in the EAS de-registration request from the EAS to the EES.

Table 8.4.3.3.6-1: EAS de-registration request

Information element	Status	Description
Registration ID	M	Identifier of the registration.
Security credentials	M	Security credentials of the EAS

8.4.3.3.7 EAS de-registration response

Table 8.4.3.3.7-1 describes information elements in the EAS de-registration response from the EES to the EAS.

Table 8.4.3.3.7-1: EAS de-registration response

Information element	Status	Description
Successful response	O	Indicates that the de-registration request was successful.
Failure response	O	Indicates that the de-registration request failed.
> Cause	O	Indicates the cause of de-registration request failure

8.4.3.4 APIs

8.4.3.4.1 General

Table 8.4.3.4.1-1 illustrates the API for EAS registration.

Table 8.4.3.4.1-1: Eees_EASRegistration API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EASRegistration	Request	Request/Response	EAS
	Update		
	Deregister		

8.4.3.4.2 Eees_EASRegistration_Request operation

API operation name: Eees_EASRegistration_Request

Description: The consumer requests to register the EAS on the EES.

Inputs: See clause 8.4.3.3.2.

Outputs: See clause 8.4.3.3.3.

See clause 8.4.3.2.2 for details of usage of this operation.

8.4.3.4.3 Eees_EASRegistration_Update operation

API operation name: Eees_EASRegistration_Update

Description: The consumer requests to update the registered information of the EAS on the EES.

Inputs: See clause 8.4.3.3.4.

Outputs: See clause 8.4.3.3.5.

See clause 8.4.3.2.3 for details of usage of this operation.

8.4.3.4.4 Eees_EASRegistration_Deregister operation

API operation name: Eees_EASRegistration_Deregister

Description: The consumer requests to deregister the EAS from the EES.

Inputs: See clause 8.4.3.3.6.

Outputs: See clause 8.4.3.3.7.

See clause 8.4.3.2.4 for details of usage of this operation.

8.4.4 EES Registration

8.4.4.1 General

The EES Registration procedure allows an EES to provide information to an ECS in order to enable provisioning EES(s) to an EEC.

The EES registration update procedure allows an EES to update the ECS, if there is a change in the information at the EES.

The EES uses the EES de-registration procedure to remove its information from the ECS.

8.4.4.2 Procedures

8.4.4.2.1 General

8.4.4.2.2 EES registration

Pre-conditions:

1. The EES has the address (e.g. URI) of the ECS;
2. Both, the EES and ECS, have the necessary credentials to enable communications.

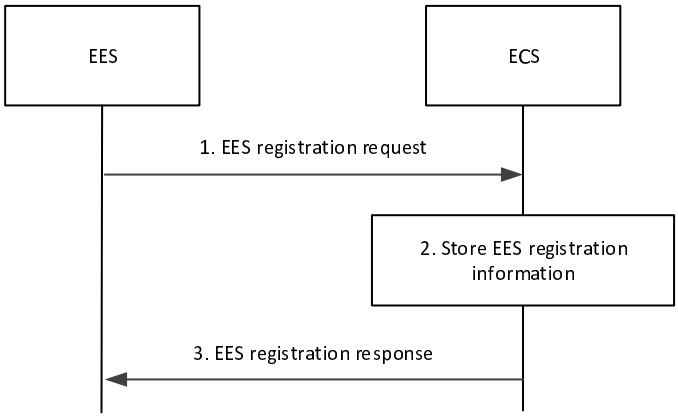

Figure 8.4.4.2.2-1: EES Registration procedure

1. The EES sends the EES registration request to the ECS. The request from the EES includes the EES profile and EES security credentials. The request may include a proposed expiration time for the registration.
2. Upon receiving the request from the EES, the ECS verifies the security credentials of the EES and stores the EES registration information obtained in step 1. If the EES profile includes bundle ID, the ECS stores the information and associates the EES with other EESs providing the same EAS bundle information.
3. The ECS sends an EES registration response indicating success or failure of the registration operation. The ECS may provide an updated expiration time to indicate to the EES when the registration will automatically expire. To maintain the registration, the EES shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the ECS shall treat the EES as implicitly de-registered.

8.4.4.2.3 EES registration update

Pre-conditions:

1. The EES has already registered on the ECS.

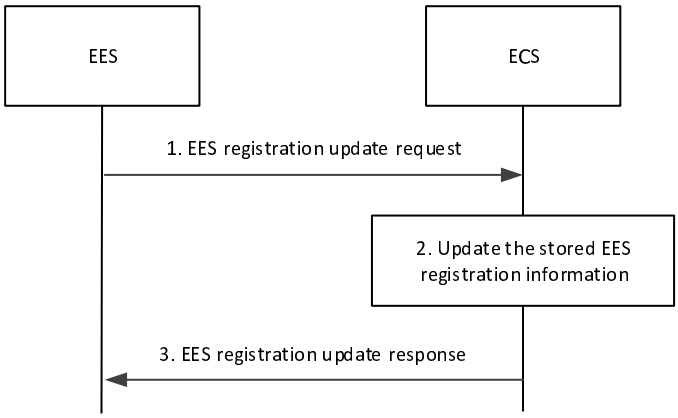

Figure 8.4.4.2.3-1: EES registration update procedure

1. The EES sends the EES registration update request to the ECS. The request from the EES includes the registration identity and EES security credentials, and may include proposed expiration time and updated EES profile.

2. Upon receiving the request from the EES, the ECS verifies the security credentials of the EES and stores the updated EES registration information obtained in step 1. If the request includes updated bundle ID, the ECS updates the stored information and EES associations.

3. The ECS sends an EES registration update response indicating success or failure of the registration update operation. The ECS may provide an updated expiration time to indicate to the EES when the updated registration will automatically expire. To maintain the registration, the EES shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the ECS shall treat the EES as implicitly de-registered.

8.4.4.2.4 EES de-registration

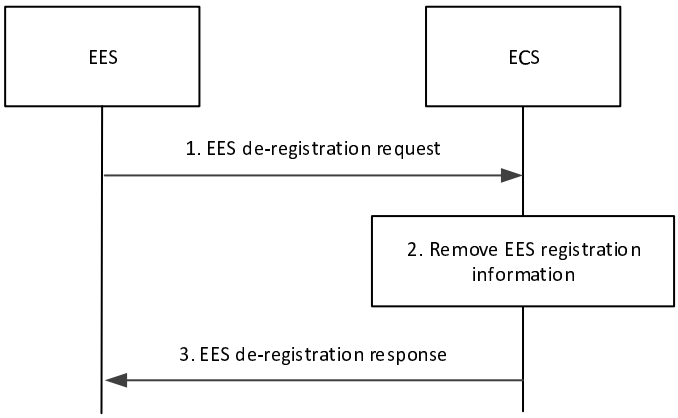

Figure 8.4.4.2.4-1: EES de-registration procedure

1. The EES sends the EES de-registration request to the ECS. The request from the EES includes the registration identity and EES security credentials.

2. Upon receiving the request from the EES, the ECS verifies the security credentials of the EES and removes the corresponding EES registration information.

3. The ECS sends an EES de-registration response indicating success or failure of the de-registration operation.

8.4.4.3 Information elements

8.4.4.3.1 General

The following information flows are specified for EES registration:

- EES registration request and response;
- EES registration update request and response; and
- EES registration de-registration request and response.

8.4.4.3.2 EES registration request

Table 8.4.4.3.2-1 describes information elements for an EES registration request from the EES to the ECS.

Table 8.4.4.3.2-1: EES registration request

Information element	Status	Description
EES Profile	M	Profile information as specified in Table 8.2.6-1
Security credentials	M	Security credentials of the EES.
Proposed expiration time	O	Proposed expiration time for the registration

8.4.4.3.3 EES registration response

Table 8.4.4.3.3-1 describes information elements for an EES registration response from the ECS to the EES.

Table 8.4.4.3.3-1: EES registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the registration.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the registration never expires.
Failure response	O	Indicates that the registration request failed.
> Cause	O	Indicates the cause of registration request failure

8.4.4.3.4 EES registration update request

Table 8.4.4.3.4-1 describes information elements for an EES registration update request from the EES to the ECS.

Table 8.4.4.3.4-1: EES registration update request

Information element	Status	Description
Updated EES Profile (NOTE)	O	Profile information as specified in Table 8.2.6-1
Security credentials	M	Security credentials of the EES.
Registration ID	M	Identifier of the registration.
Proposed expiration time (NOTE)	O	Proposed expiration time for the registration
NOTE: At least one of the IEs is included.		

8.4.4.3.5 EES registration update response

Table 8.4.4.3.5-1 describes information elements for an EES registration update response from the ECS to the EES.

Table 8.4.4.3.5-1: EES registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration update request was successful.
> Expiration time	O	Indicates the expiration time of the updated registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the updated registration never expires.
Failure response	O	Indicates that the registration update request failed.
> Cause	O	Indicates the cause of registration update request failure

8.4.4.3.6 EES de-registration request

Table 8.4.4.3.6-1 describes information elements for an EES de-registration request from the EES to the ECS.

Table 8.4.4.3.6-1: EES de-registration request

Information element	Status	Description
Registration ID	M	Identifier of the registration.
Security credentials	M	Security credentials of the EES

8.4.4.3.7 EES de-registration response

Table 8.4.4.3.7-1 describes information elements for an EES de-registration response from the ECS to the EES.

Table 8.4.4.3.7-1: EES de-registration response

Information element	Status	Description
Successful response	O	Indicates that the de-registration request was successful.
Failure response	O	Indicates that the de-registration request failed.
> Cause	O	Indicates the cause of de-registration request failure

8.4.4.4 APIs

8.4.4.4.1 General

Table 8.4.4.4.1-1 illustrates the API for EES registration.

Table 8.4.4.4.1-1: Eecs_EESRegistration API

API Name	API Operations	Operation Semantics	Consumer(s)
Eecs_EESRegistration	Request	Request/Response	EES
	Update		
	Deregister		

8.4.4.4.2 Eecs_EESRegistration_Request operation

API operation name: Eecs_EESRegistration_Request

Description: The consumer requests to register the EES on the ECS.

Inputs: See clause 8.4.4.3.2.

Outputs: See clause 8.4.4.3.3.

See clause 8.4.4.2.2 for details of usage of this operation.

8.4.4.4.3 Eecs_EESRegistration_Update operation

API operation name: Eecs_EESRegistration_Update

Description: The consumer requests to update the registered information of the EES on the ECS.

Inputs: See clause 8.4.4.3.4.

Outputs: See clause 8.4.4.3.5.

See clause 8.4.4.2.3 for details of usage of this operation.

8.4.4.4.4 Eecs_EESRegistration_Deregister operation

API operation name: Eecs_EESRegistration_Deregister

Description: The consumer requests to deregister the EES from the ECS.

Inputs: See clause 8.4.4.3.6.

Outputs: See clause 8.4.4.3.7.

See clause 8.4.4.2.4 for details of usage of this operation.

8.5 EAS discovery

8.5.1 General

Discovery procedures enable entities in an edge deployment to obtain information about EAS and their available services, based on specified criteria of interest.

EAS discovery enables the EEC to obtain information about available EASs of interest (e.g. instantiated EASs registered with the EES and instantiable EASs that may be created when needed). The discovery of the EASs is based on matching EAS discovery filters provided in the request.

When multiple EASs are discovered for a specific AC, the EEC may select one or more EASs to enable AC communication with one of the selected EASs. The selection algorithm is outside the scope of this specification. Once the EAS is selected, the EEC may subscribe for the ACR event notifications at the EES of the selected EAS, as described in clause 8.8.3.5.2. The EDN configuration information received from ECS may be used for establishing a connection to EAS(s).

EAS discovery may be initiated by the EEC when a certain trigger condition at the UE is met. Some examples are as follows:

- AC related updates available at the EEC (e.g. due to AC installation/re-installation/activation), AC requesting application server access;
- Lifetime received via EAS discovery response specified in clause 8.5.3 is expired; or
- EEC detects the need of application context relocation as in clause 8.8.

NOTE: When the EEC decides to perform EAS discovery is up to EEC implementation.

If the EASs consisting of the EAS bundle register to different EESs and if the Bundle Type of the EAS bundle is set to Direct bundle, then the EEC sends the EAS discovery request message to the associated EES for the bundle EAS information.

8.5.2 Procedures

8.5.2.1 General

Following procedures are supported for EAS discovery:

- Request-response procedure;
- Subscribe-notify procedures for EAS discovery and EAS dynamic information subscription, comprising:
  - Subscription procedure;
  - Subscription update procedure; and
  - Unsubscribe procedure;

8.5.2.2 Request-response model

Pre-conditions:

1. The EEC has received information (e.g. URI, IP address) related to the EES;
2. The EEC has received appropriate security credentials authorizing it to communicate with the EES as specified in clause 8.11; and
3. The EES is configured with ECSP's policy for EAS discovery.

NOTE 1: Details of ECSP's policy are out of scope.

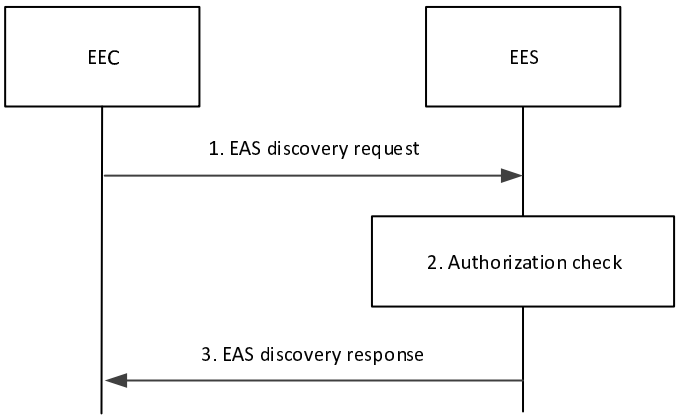

Figure 8.5.2.2-1: EAS Discovery procedure

1. The EEC sends an EAS discovery request to the EES. The EAS discovery request includes the requestor identifier [EECID] along with the security credentials and may include EAS discovery filters, EEC service continuity support, and may also include UE location to retrieve information about particular EAS(s) or a category of EASs, e.g. gaming applications, or Edge Applications Server(s) available in certain service areas, e.g. available on a UE's predicted or expected route. The request may include an EAS selection request indicator.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to discover the requested EAS(s). The authorization check may apply to an individual EAS, a category of EASs or to the EDN, i.e. to all the EASs. If UE's location information is not already available, the EES obtains the UE location by utilizing the capabilities of the 3GPP core network as specified in clause 8.10.3. If EAS discovery filters are provided by the EEC, but it does not contain Application group profile, the EES identifies the EAS(s) based on the provided EAS discovery filters and the UE location.

   When the bundle EAS information is provided, then;

- If bundle EAS information includes EAS bundle identifier, the EES identifies all or part of the EAS(s) associated with the same EAS bundle identifier.

- If bundle EAS information includes a list of EASIDs, the EES identifies the EASs which are all or part of the EAS bundle.

If the EEC indicates that service continuity support is required, when identifying the EAS, the EES shall take the indication which ACR scenarios are supported by the AC, the EEC, the EES and the EAS and which of these are preferred by the AC into consideration. The EES may select one EAS and determine whether to perform application traffic influence for this AC based on AC's service KPI or EAS's service KPI in desired response time, when the EAS does not perform traffic influence in advance.

When EAS discovery filters are not provided, then:

- if available, the EES identifies the EAS(s) based on the UE-specific service information at the EES and the UE location;

- EES identifies the EAS(s) by applying the ECSP policy (e.g. based only on the UE location);

When EAS discovery filters contain Application group profile, the EES checks whether information about common EAS and related Application Group ID is available or not. If the common EAS information related to the Application Group ID is:

- not available, then based on the policy if EES needs to select the common EAS, the EES identifies an EAS for the Application Group ID based on the provided EAS discovery filters such as KPIs, UE-specific service information or the ECSP policy. Furthermore, the EES stores the common EAS information and related Application Group ID.

- available at the EES, then the EES provides information of that EAS as result for EAS discovery.

NOTE 2: The EES may have previously determined and stored the common EAS for Application group ID, or the EES may have received the common EAS selection information for Application group ID during the common EAS announcement procedure.

When the ECS-ER is not available and the EES selects the common EAS, the selected common EAS shall be announced to other EES(s) as per procedure specified in clause 8.19.

When the ECS-ER is available and common EAS information corresponding to the Application Group ID is not available, then the EES identifies one EAS for the group and interacts with the ECS-ER to store the common EAS information as described in clause 8.20.2.3. If common EAS information is already available corresponding to the Application Group ID in the repository, then the ECS-ER returns the common EAS information to the EES as described in clause 8.20.2.3.

NOTE 3: Details of the UE-specific service information and how it is available at the EES is out of scope.

NOTE 4: Both steps are evaluated prior to sending a response.

Upon receiving the request from the EEC, the EES may also collect edge load analytics from ADAES (as specified in clause 8.8.2 of TS 23.436 [28]) or performance data from OAM to find whether the EAS(s) satisfies the Expected AC service KPIs or the Minimum required AC Service KPIs.

Upon receiving the request from the EEC, if the EEC does not indicate EAS Instantiation Triggering Suppress in the EAS Discovery request, the EES may trigger the ECSP management system to instantiate the EAS that matches with EAS discovery filter IEs (e.g. ACID) as in clause 8.12.

Otherwise, upon receiving the request from the EEC, if the EEC indicates EAS Instantiation Triggering Suppress in the EAS Discovery request and the EES supports such capability, the EES determines not triggering the ECSP management system to instantiate the EAS and may determine Instantiable EAS Information for EAS(s) that are instantiable but not yet instantiated and match the EAS discovery filter IEs. Instantiable EAS Information is provided in the EAS Discovery response and includes the EASID(s) and, for each EASID, the status indicating whether the EAS is instantiated or instantiable but not yet instantiated.

If the EEC provides in the EAS discovery request the EAS selection request indicator, the EES selects EAS satisfying the EAS discovery filter or based on other information (e.g. ECSP policy) as described above (if no

EAS discovery filter received), and then provides the selected EAS information to the EEC in the discovered EAS list of EAS discovery response.

NOTE 5: Without EAS selection request indication, the EES handling is as per R17 procedure.

3. If the processing of the request was successful, the EES sends an EAS discovery response to the EEC, which includes information about the discovered EASs and Instantiable EAS Information. For discovered EASs, this includes endpoint information. Depending on the EAS discovery filters received in the EAS discovery request, the response may include additional information regarding matched capabilities, e.g. service permissions levels, KPIs, AC locations(s) that the EASs can support, ACR scenarios supported by the EAS, etc. The EAS discovery response may contain a list of EASs and Instantiable EAS Information. This list may be based on EAS discovery filters containing a Geographical or Topological Service Area, e.g. a route, included in the EAS discovery request by the EEC. When the discovered EAS is for a certain application group, then the Application Group ID is also included in the response message. If the discovered EAS is registered to another EES, then the EES endpoint of the EES where the discovered EAS is registered is also included in the response message.

   When the EES determines to trigger the EAS instantiation, then the response may indicate that the EAS instantiation is in progress so that the detailed EAS profile information will be available later. When EEC receives the EAS instantiation in progress indication, the EEC may send EAS discovery subscription request message or send EAS discovery request message later to the EES for obtaining updated EAS information.

   If the EES is unable to determine the EAS information using the inputs in the EAS discovery request, UE-specific service information at the EES or the ECSP policy, the EES shall reject the EAS discovery request and respond with an appropriate failure cause.

   If the EEC is not registered with the EES, and ECSP policy requires the EEC to perform EEC registration prior to EAS discovery, the EES shall include an appropriate failure cause in the EAS discovery response indicating that EEC registration is required.

   If the UE location and predicted/expected UE locations, provided in the EAS discovery request, are outside the Geographical or Topological Service Area of an EAS, then the EES shall not include that EAS in the discovery response. The discovery response may include EAS(s) that cannot serve the UE at its current location if a predicted/expected UE location was provided in the EAS discovery request.

Upon receiving the EAS discovery response, if the EEC selects an EAS which is instantiated (i.e., an EAS profile was provided), the EEC uses the endpoint information for routing of the outgoing application data traffic to EAS(s), as needed, and may provide necessary notifications to the AC(s). The EEC may use the border or overlap between EAS Geographical Service Areas for service continuity purposes. The EEC may cache the EAS information (e.g. EAS endpoint) for subsequent use and avoid the need to repeat step 1. If the Lifetime IE is included in the response, the EEC may cache the EAS information only for the duration specified by the Lifetime IE.

Upon receiving the EAS discovery response, if the EEC selects an EAS which is instantiable but not yet instantiated (i.e. an EAS profile is not provided), the EEC sends the EAS information provisioning request indicating the selected EASID as in clause 8.15.

NOTE 6: Within the duration specified by the Lifetime IE, the cached EAS Profile can be updated (e.g. according to notifications from the EES for changes of EAS information due to EAS status change) or the cached EAS Profile can be invalidated due to new EAS information discovery (e.g. due to UE mobility). The EEC can update or invalidate the cached EAS information (e.g. on PDU Session Release or Modification Command).

NOTE 7: The AC can cache the EAS information (e.g. EAS endpoint) for subsequent use. In the case of the cached information needing to be updated or invalidated, the mechanisms for the EEC to notify the AC is up to implementation and is not specified in the current release of the present document.

NOTE 8: The EEC can use the EAS information provided by the discovery procedure to perform service continuity planning, for example when ultra-low latency ACR is required.

If the EAS discovery request fails, the EEC may resend the EAS discovery request, taking into account the received failure cause. If the failure cause indicated that EEC registration is required, the EEC shall perform an EEC registration before resending the EAS discovery request.

NOTE 9: As long as a proper EAS (e.g. considering expected AC service KPIs included in EAS discovery request) is discovered and selected by the EES, EEC of a constraint UE can stop sending EAS discovery to rest candidate EES(s), and provide the selected EAS information to AC.

8.5.2.3 Subscribe-notify model

8.5.2.3.1 General

Clause 8.5.2.3.2 and clause 8.5.2.3.3 together illustrate the EAS discovery procedure based on Subscribe/Notify model.

Clause 8.5.2.3.4 illustrates the EAS discovery update procedure.

Clause 8.5.2.3.5 illustrates the EAS discovery unsubscribe procedure.

8.5.2.3.2 Subscribe

Figure 8.5.2.3.2-1 illustrates the EAS discovery subscription procedure between the EEC and the EES. This subscription enables EES to inform EEC of various EAS discovery related events of interest to EEC (e.g. EAS discovery notification and EAS dynamic information).

Pre-conditions:

1. The EEC has received information (e.g. URI, IP address) related to the EES;
2. The EEC has received appropriate security credentials authorizing it to communicate with the EES as specified in clause 8.11;
3. The EES is configured with ECSP's policy for EAS discovery; and
4. The EEC has optionally acquired a Notification Target Address to be used in its subscriptions to notifications.

NOTE 1: Details of ECSP's policy are out of scope.

NOTE 2: How the EEC acquires the notification target address or a notification channel URI to receive the notifications is out of scope of this release. The notification target address can terminate at the EEC (e.g. in an IoT device) if the deployment supports EEC reachability, or it can terminate at a push notification service. Details of the push notification service are out of scope of this release.

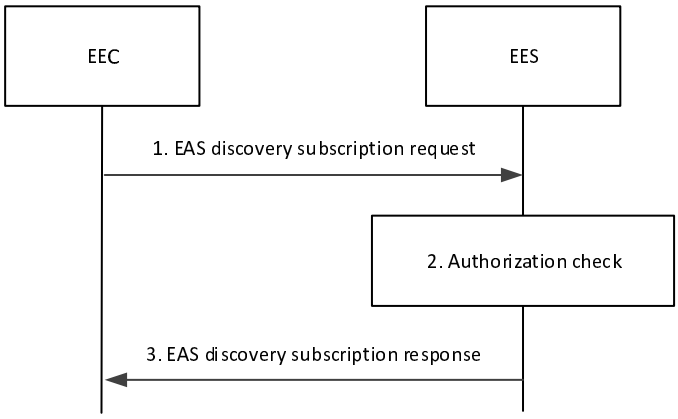

Figure 8.5.2.3.2-1: EAS discovery subscription

1. The EEC sends an EAS discovery subscription request to the EES. The EAS discovery subscription request includes the EECID along with the security credentials, Event ID, and may include EAS discovery filters and EAS dynamic information filters to subscribe to information about particular EAS(s) or a category of EASs (e.g. gaming applications) or dynamic information about EAS(s).

If the application triggering is supported and required by the EEC, the EEC may include the EEC Triggering request information element instead of the Notification Target Address in the request message.

2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to subscribe for information of the requested EAS(s). The authorization check may apply to an individual EAS, a category of EASs or to the EDN, i.e. to all the EASs. The EES may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.3. If the request is authorized, the EES creates and stores the subscription for EAS discovery.

3. If the processing of the request was successful, the EES sends an EAS discovery subscription response to the EEC, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EEC shall send an EAS discovery subscription update request prior to the expiration time. If an EAS discovery subscription update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly unsubscribed.

   In the case of subscription to an EAS availability change event, if there is no instantiated EAS that matches the requested EAS discovery filters and such EAS is instantiable based on the information about instantiable EASs, the request is treated as successful. If the EEC indicates EAS Instantiation Triggering in the EAS discovery subscription request and the EAS instantiation is not in progress for the requested EASID, the EES may trigger dynamic instantiation of the EAS as specified in the clause 8.12; if the EEC indicates EAS Instantiation Triggering Suppress in the EAS discovery subscription request, the EES determines not triggering the ECSP management system to instantiate the EAS and Instantiable EAS Information (e.g. instantiated, instantiable but not be instantiated yet) is provided; otherwise, the EES does not trigger the EAS instantiation nor returns the Instantiable EAS Information.

   In the case of subscription to an EAS dynamic information change event, if the EES is unable to determine the instantiated EAS information using the inputs in the EAS discovery subscription request, UE-specific service information at the EES or the ECSP policy, the EES shall reject the EAS discovery subscription request and respond with an appropriate failure cause.

   If the EEC is not registered with the EES, and ECSP policy requires the EEC to perform EEC registration prior to EAS discovery, the EES shall include an appropriate failure cause in the EAS discovery response indicating that EEC registration is required.

   If the EAS discovery subscription request fails, the EEC may resend the EAS discovery subscription request again, taking into account the received failure cause. If the failure cause indicated that EEC registration is required, the EEC shall perform an EEC registration before resending the EAS discovery subscription request.

8.5.2.3.3 Notify

Figure 8.5.2.3.3-1 illustrates the EAS discovery notification procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the EAS discovery information as specified in clause 8.5.2.3.2.

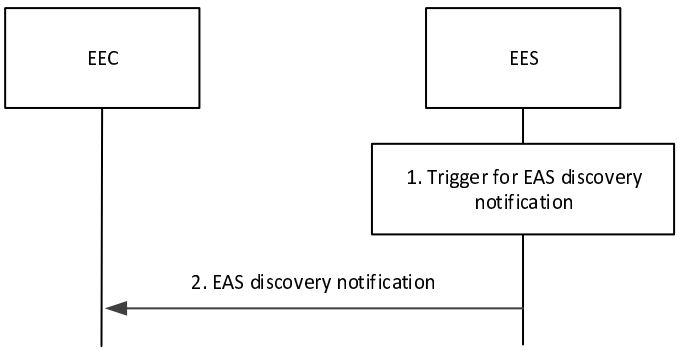

Figure 8.5.2.3.3-1: EAS discovery notification

1. An event occurs at the EES that satisfies trigger conditions for notifying (e.g. to provide EAS discovery information or EAS dynamic information) a subscribed EEC. If UE's location information is not already available, the EES obtains the UE location by utilizing the capabilities of the 3GPP core network as specified in clause 8.10.3. If EAS discovery filters were provided by the EEC during subscription creation, the EES identifies the EAS(s) based on the provided EAS discovery filters and the UE location.

   For EAS dynamic information change event, the EES, based on local policy, may use received EAS endpoints from EEC or all registered EAS endpoints to get edge load analytics information from ADAES services (e.g. as specified in clause 8.8 of TS 23.436 [27]) to monitor EAS service status like EAS status and EAS schedule.

   When the bundle EAS information is provided, then;

- If EAS bundle identifier was provided, the EES identifies all or part of the EAS(s) associated with the same EAS bundle identifier.

- If a list of EASIDs is provided, the EES identifies the EASs which are all or part of the EAS bundle.

   If the EEC indicates that service continuity support is required, the EES shall take the indication which ACR scenarios are supported by the AC and the EEC and which of these are preferred by the AC into consideration.

   If EAS discovery filters were not provided, then:

   - if available, the EES identifies the EAS(s) based on the UE-specific service information at the EES and the UE location;

   - EES identifies the EAS(s) by applying the ECSP policy (e.g. based only on the UE location);

   If EAS discovery filters contain Application group profile, the EES checks whether information about common EAS and related Application Group ID is available or not. If the common EAS information related to the Application Group ID is available at the EES, then the EES provides information of that EAS as result for EAS discovery.

NOTE 1: The EES may have previously determined and stored the common EAS for Application group ID, or the EES may have received the common EAS selection information for Application group ID during the common EAS announcement procedure.

NOTE 2: Details of the UE-specific service information and how it is available at the EES is out of scope.

NOTE 3: Both steps are evaluated prior to sending a response.

   If the UE is located outside the Geographical or Topological Service Area of an EAS, then the EES shall not include this EAS in the EAS discovery notification.

   If the application triggering is supported and required by the EEC as indicated in EEC Triggering Request IE of the EAS Discovery Subscription Request, then the EES performs the EEC triggering service as described in the clause 8.16.1 and skips the step 2.

2. The EES sends an EAS discovery notification to the EEC with the EAS information determined in step 1, which includes information about the discovered EASs and Instantiable EAS Information. For discovered EASs, this includes endpoint information. Depending on the event type and EAS discovery filters received in the EAS discovery subscription request, the notification may include additional information regarding matched capabilities, e.g. service permissions levels, KPIs, AC locations(s) that the EASs can support, ACR scenarios supported by the EAS, etc. The EAS discovery notification may contain a list of EASs and Instantiable EAS Information. This list may be based on EAS discovery filters containing a Geographical or Topological Service Area, e.g. a route, included in the EAS discovery subscription request by the EEC. When the discovered EAS is for a certain application group, then the Application Group ID is also included in the notification message. If the discovered EAS is registered to another EES, then the EES endpoint of the EES where the discovered EAS is registered is also included in the notification message.

Upon receiving the EAS discovery notification, if the EEC selects an EAS which is instantiated (i.e., an EAS profile was provided), the EEC uses the endpoint information for routing of the outgoing application data traffic to EAS(s), as needed, and may provide necessary notifications to the AC(s). The EEC may use the border or overlap between EAS Geographical Service Areas for service continuity purposes. The EEC may cache the EAS information (e.g. EAS endpoint) for subsequent use. If the Lifetime IE is included in the notification, the EEC may cache the EAS information only for the duration specified by the Lifetime IE.

NOTE 4: Within the duration specified by the Lifetime IE, the cached EAS Profile can be updated (e.g. according to notifications from the EES for changes of EAS information due to EAS status change) or the cached EAS Profile can be invalidated due to new EAS information discovery (e.g. due to UE mobility). The EEC can update or invalidate the cached EAS information (e.g. on PDU Session Release or Modification Command).

NOTE 5: The AC can cache the EAS information (e.g. EAS endpoint) for subsequent use. In the case of the cached information needing to be updated or invalidated, the mechanisms for the EEC to notify the AC is up to implementation and is not specified in the current release of the present document.

NOTE 6: The EEC can use the EAS information provided by the discovery procedure to perform service continuity planning, for example when ultra-low latency ACR is required.

Upon receiving the EAS discovery notification, if the EEC selects an EAS which is instantiable but not yet instantiated (i.e. an EAS profile is not provided), the EEC may send the EAS information provisioning request indicating the selected EASID as in clause 8.15.

8.5.2.3.4 Subscription update

Figure 8.5.2.3.4-1 illustrates the EAS discovery subscription update procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the EAS discovery information as specified in clause 8.5.2.3.2

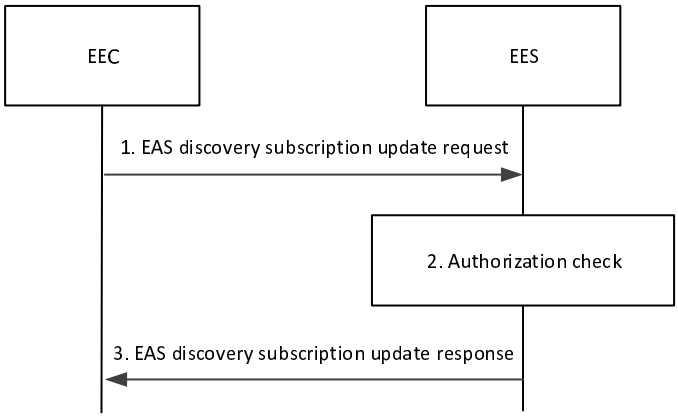

Figure 8.5.2.3.4-1: EAS discovery subscription update

1. The EEC sends an EAS discovery subscription update request to the EES. The EAS discovery subscription update request includes the security credentials and the subscription identifier. It may also include EAS discovery filters, EAS dynamic information filters and/or proposed expiration time for the updated subscription.

2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to update the subscription information. The EES may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.3. If the request is authorized, the EES updates the stored subscription for EAS discovery.

3. The EES sends an EAS discovery subscription update response to the EEC, which may include the expiration time, indicating when the updated subscription will automatically expire. To maintain the subscription, the EEC shall send an EAS discovery subscription update request prior to the expiration time. If an EAS discovery subscription update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly unsubscribed.

8.5.2.3.5 Unsubscribe

Figure 8.5.2.3.5-1 illustrates the EAS discovery unsubscribe procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for notification (e.g. EAS discovery information and EAS dynamic information) as specified in clause 8.5.2.3.2

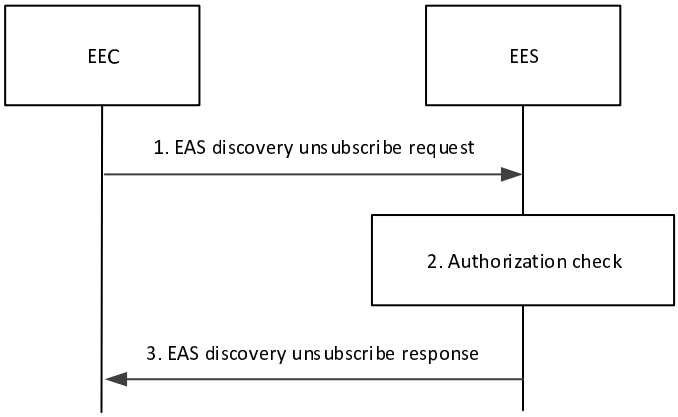

Figure 8.5.2.3.5-1: EAS discovery unsubscribe

1. The EEC sends an EAS discovery unsubscribe request to the EES. The EAS discovery unsubscribe request includes the security credentials of the EEC along with the subscription identifier.
2. Upon receiving the request, the EES performs an authorization check to verify whether the EEC has authorization to perform the operation. If authorized, the EES cancels the subscription for provisioning as requested in step 1.
3. The EES responds with an EAS discovery unsubscribe response.

8.5.3 Information flows

8.5.3.1 General

The following information flows are specified for EAS discovery:

- EAS discovery request and response;
- EAS discovery subscription, notification, subscription update and unsubscribe; and
- EAS dynamic information subscription, notification, subscription update and unsubscribe.

8.5.3.2 EAS discovery request

Table 8.5.3.2-1 describes information elements for the EAS discovery request. Table 8.5.3.2-2 provides further detail about the EAS Discovery Filter information element.

Table 8.5.3.2-1: EAS discovery request

Information element	Status	Description
Requestor identifier	M	The ID of the requestor (e.g. EECID)
UE Identifier	O	The identifier of the UE (i.e., GPSI)
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EAS discovery filters	O	Set of characteristics to determine required EASs, as detailed in Table 8.5.3.2-2.
UE location	O	The location information of the UE. The UE location is described in clause 7.3.2.
Serving MNO information (NOTE 2)	O	The serving MNO information (e.g. MNO name, PLMN ID) which is serving the subscriber.
Target DNAI (NOTE 1)	O	Target DNAI information which can be associated with potential T-EAS(s)
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC or, if this message is sent by the EEC to discover a T-EAS, which ACR scenario(s) are intended to be used for the ACR.
EES Service Continuity Support (NOTE 1)	O	The IE indicates if the S-EES supports service continuity or not. The IE also indicates which ACR scenarios are supported by the S-EES or, if the EAS discovery is used for an S-EES executed ACR according to clause 8.8.2.5, which ACR scenario is to be used for the ACR.
EAS Service Continuity Support (NOTE 1)	O	The IE indicates if the S-EAS supports service continuity or not. The IE also indicates which ACR scenarios are supported by the S-EAS or, if the EAS discovery is used for an S-EAS decided ACR according to clause 8.8.2.4, which ACR scenario is to be used for the ACR.
EAS Instantiation Triggering Suppress	O	Indicates to the EES that EAS instantiation triggering should not be performed for the current request, and Instantiable EAS Information (e.g. instantiated, instantiable but not be instantiated yet) is to be provided in response.
EAS selection request indicator	O	Indicates the request for EAS selection support from the EES (e.g., for constrained device).
Indication of service continuity planning	O	Indicates that this EAS discovery request is triggered for service continuity planning.
Prediction expiration time	O	The estimated time the UE may reach the Predicted/Expected UE location or EAS service area at the latest. This IE is used by EES as analytics input to get edge load analytics information from ADAES service as described in clause 8.8 of TS 23.436 [27].
NOTE 1: This IE shall not be included when the request originates from the EEC. NOTE 2: This IE shall be included if edge node sharing is used.		

Table 8.5.3.2-2: EAS discovery filters

Information element	Status	Description
List of AC characteristics (NOTE 1)	O	Describes the ACs for which a matching EAS is needed.
> AC profile (NOTE 2)	M	AC profile containing parameters used to determine matching EAS. AC profiles are further described in Table 8.2.2-1.
> Application group profile	O	Application group profile associated with the AC Profile, as defined in Table 8.2.11-1.
List of EAS characteristics (NOTE 1, NOTE 3)	O	Describes the characteristic of required EASs.
> EASID	O	Identifier of the required EAS.
> Application Group ID	O	Application group identifier as defined in 7.2.11.
> EAS synchronization support	O	Indicates if the EAS synchronization support is required or not.
> Bundle ID (NOTE 5)	O	A list of EASIDs or a bundle ID as described in clause 7.2.10.
> List of EASIDs (NOTE 5)	O	A list of EASIDs specific to a particular EAS bundle.
> Bundle type (NOTE 4)	O	Type of the EAS bundle as described in clause 7.2.10
> EAS bundle requirements (NOTE 4)	O	Requirements associated with the EAS bundle as described in clause 8.2.10.
> EAS provider identifier	O	Identifier of the required EAS provider
> EAS type	O	The category or type of required EAS (e.g. V2X)
> EAS schedule	O	Required availability schedule of the EAS (e.g. time windows)
> EAS Geographical Service Area	O	Location(s) (e.g. geographical area, route) where the EAS service should be available.
> EAS Topological Service Area	O	Topological area (e.g. cell ID, TAI) for which the EAS service should be available. See possible formats in Table 8.2.7-1.
> Service continuity support	O	Indicates if the service continuity support is required or not.
> Service permission level	O	Required level of service permissions e.g. trial, gold-class
> Service feature(s)	O	Required service features e.g. single vs. multi-player gaming service
NOTE 1: Either "List of AC characteristics" or "List of EAS characteristics" shall be present. NOTE 2: "Preferred ECSP list" IE shall not be present. NOTE 3: The "List of EAS characteristics" IE must include at least one optional IE, if used as an EAS discovery filter. NOTE 4: When EAS discovery request is sent by the EEC, this IE shall not be included. NOTE 5: “Bundle ID" and "List of EASIDs" shall not both be present.		

8.5.3.3 EAS discovery response

Table 8.5.3.3-1 describes information elements for the EAS discovery response from the EES to the EEC.

Table 8.5.3.3-1: EAS discovery response

Information element	Status	Description
Successful response	O	Indicates that the EAS discovery request was successful.
> Discovered EAS list (NOTE 1, NOTE 3)	O	List of discovered EAS(s). Each element includes the information described below.
>> EAS profile	M	Profile of the EAS. Each element is described in clause 8.2.4
>> Application Group ID list (NOTE 4)	O	List of Application Group IDs associated with EAS
>> EES Endpoint	O	The endpoint address (e.g. URI, IP address) of the EES.
>> Lifetime	O	Time interval or duration during which the information elements in the EAS profile is valid and supposed to be cached in the EEC (e.g. time-to-live value for an EAS Endpoint)
> Analytics information	O	Analytics data for each discovered application server.
>> Statistical data	O	Indicates the statistical analytics data (e.g. number of times the client received expected performance from the EAS).
>> Predictive data	O	Indicates predictive analytics data for EAS service status (e.g. EAS schedule, EAS status) change.
> Instantiable EAS Information (NOTE 1)	O	The EAS instantiation status per EASID (e.g. instantiated, instantiable but not instantiated yet, instantiation in progress).
>> Instantiation criteria (NOTE 2)	O	The criteria upon which EAS can be instantiated (e.g. based on specific date and time).
Failure response	O	Indicates that the EAS discovery request failed.
> Cause	O	Indicates the cause of EAS discovery request failure.
NOTE 1: At least one of the IEs must be included in the Successful response. NOTE 2: "Instantiation criteria" IE shall be present only when the value of "Instantiable EAS information" IE is "instantiable but not be instantiated yet". NOTE 3: If EAS discovery is used for ENS scenario, discovered EAS list contains only those EASs which are allowed to be used by the subscribers of the serving MNO. NOTE 4: "Application Group ID list" IE shall be present when "Application Group profile" is included for "AC profile" in EAS discovery request as specified in clause 8.5.3.2		

8.5.3.4 EAS discovery subscription request

Table 8.5.3.4-1 describes the information elements for EAS discovery subscription request from the EEC to the EES.

Table 8.5.3.4-1: EAS discovery subscription request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
UE Identifier	O	The identifier of the UE (i.e., GPSI)
Event ID	M	Event ID: - EAS availability change - EAS dynamic information change
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Notification Target Address (NOTE 1)	O	The Notification target address (e.g. URL) where the notifications destined for the EEC should be sent to.
EAS discovery filters	O	Set of characteristics to determine matching EASs (as detailed in Table 8.5.3.2-2). Applicable for "EAS availability change" event
EAS dynamic information filters	O	List of dynamic information changes (as detailed in Table 8.5.3.4-2) about EAS, the EEC is interested in. Applicable for "EAS dynamic information change" event
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
Proposed expiration time	O	Proposed expiration time for the subscription
EAS Instantiation Triggering Indication (NOTE 2)	O	Indicates to the EES that EAS instantiation triggering may be performed for the current request if needed.
EAS Instantiation Triggering Suppress (NOTE 2)	O	Indicates to the EES that EAS instantiation triggering should not be performed for the current request, and Instantiable EAS Information (e.g. instantiated, instantiable but not be instantiated yet) is to be provided in the notification.
EEC Triggering request (NOTE 1)	O	Indicates that EEC Triggering is requested
NOTE 1: One of them may be included in the request message. NOTE 2: One of them may be included in the request message.		

Table 8.5.3.4-2: EAS dynamic information filters

Information element	Status	Description
List of dynamic information filters	M	List of EAS dynamic information required by the EEC per EAS.
> EASID	M	Identifier of the EAS
> ACIDs	O	Flag to notify change in list of ACIDs served by the EAS
> EAS Description	O	Flag to notify change in description of the. EAS.
> EAS Endpoint	O	Flag to notify change in EAS endpoint It may also include one or more EAS endpoints to be monitored by the EES. If no EAS endpoint is provided, all EASs registered in the EES will be monitored.
> EAS Features	O	Flag to notify any change in features provided by the EAS
> EAS Schedule	O	Flag to notify change in availability schedule of the EAS (e.g. time windows)
> EAS Service Area	O	Flag to notify change in geographical service area that the EAS serves
> EAS Service KPIs	O	Flag to notify change in characteristics of the EAS.
> EAS Status	O	Flag to notify change in the status of the EAS (e.g. enabled, disabled, etc.)
> Service continuity support	O	Flag to notify change in EAS support for service continuity.

8.5.3.5 EAS discovery subscription response

Table 8.5.3.5-1 describes the information elements for EAS discovery subscription response from the EES to the EEC.

Table 8.5.3.5-1: EAS discovery subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.5.3.6 EAS discovery notification

Table 8.5.3.6-1 describes the information elements for EAS discovery notification from the EES to the EEC.

Table 8.5.3.6-1: EAS discovery notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
Event ID	M	Either EAS availability change or EAS dynamic information change
EAS list	O	List of discovered EAS profiles. Each element includes the information described below.
> EAS profile	M	Profile of the EAS. Each element is described in clause 8.2.4
> Application Group ID list (NOTE 3)	O	List of Application Group IDs associated with EAS
> EES Endpoint	O	The endpoint address (e.g. URI, IP address) of the common EES.
> Lifetime	O	Time interval or duration during which the information elements in the EAS profile is valid and supposed to be cached in the EEC (e.g. time-to-live value for an EAS Endpoint)
> Analytics information	O	Analytics information for EAS.
>> Statistical data	O	Indicates the statistical analytics data (e.g. number of times the client received expected performance from the EAS). Applicable for "EAS availability change" event.
>> Predictive data	O	Indicates predictive analytics data for EAS service status (e.g. EAS schedule, EAS status) change. Applicable for "EAS dynamic information change" event.
Instantiable EAS information (NOTE 1)	O	The EAS instantiation status per EASID (e.g. instantiated, instantiable but not be instantiated yet)
> Instantiation criteria (NOTE 2)	O	The criteria upon which EAS can be instantiated (e.g. based on specific date and time).
NOTE 1: "Instantiable EAS information" can be provided to EEC, if the "EAS Instantiation Triggering Suppress" is provided in EAS discovery subscription request. NOTE 2: "Instantiation criteria" IE shall be present only when the value of "Instantiable EAS information" IE is "instantiable but not be instantiated yet". NOTE 3: "Application Group ID list" IE shall be present when "Application Group profile" is included for "AC profile" in EAS discovery subscription request as specified in clause 8.5.3.4		

8.5.3.7 EAS discovery subscription update request

Table 8.5.3.7-1 describes the information elements for EAS discovery subscription update request from the EEC to the EES.

Table 8.5.3.7-1: EAS discovery subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Proposed expiration time	O	Proposed expiration time for the subscription
EAS discovery filters	O	Set of characteristics to determine required EASs, as detailed in Table 8.5.3.2-2.
EAS dynamic information filters	O	List of dynamic information about EAS, the EEC is interested in, as detailed in Table 8.5.3.4-2.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.

8.5.3.8 EAS discovery subscription update response

Table 8.5.3.8-1 describes the information elements for EAS discovery subscription update response from the EES to the EEC.

Table 8.5.3.8-1: EAS discovery subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.5.3.9 EAS discovery unsubscribe request

Table 8.5.3.9-1 describes the information elements for EAS discovery unsubscribe request from the EEC to the EES.

Table 8.5.3.9-1: EAS discovery unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be unsubscribed
Security credentials	M	Security credentials of the EEC

8.5.3.10 EAS discovery unsubscribe response

Table 8.5.3.10-1 describes the information elements for EAS discovery unsubscribe response from the EES to the EEC.

Table 8.5.3.10-1: EAS discovery unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.5.4 APIs

8.5.4.1 General

Table 8.5.4.1-1 illustrates the API for EAS discovery.

Table 8.5.4.1-1: Eees_EASDiscovery API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EASDiscovery	Request	Request/Response	EEC
	Subscribe	Subscribe/Notify	EEC
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.5.4.2 Eees_EASDiscovery_Request operation

API operation name: Eees_EASDiscovery_Request

Description: The consumer requests for one time EAS discovery information.

Inputs: See clause 8.5.3.2.

Outputs: See clause 8.5.3.3.

See clause 8.5.2.2 for details of usage of this operation.

8.5.4.3 Eees_EASDiscovery_Subscribe operation

API operation name: Eees_EASDiscovery_Subscribe

Description: The consumer subscribes for EAS discovery information.

Inputs: See clause 8.5.3.4.

Outputs: See clause 8.5.3.5.

See clause 8.5.2.3.2 for details of usage of this operation.

8.5.4.4 Eees_EASDiscovery_Notify operation

API operation name: Eees_EASDiscovery_Notify

Description: The consumer is notified with EAS discovery and/or EAS dynamic information.

Inputs: See clause 8.5.3.6.

Outputs: None.

See clause 8.5.2.3.3 for details of usage of this operation.

8.5.4.5 Eees_EASDiscovery_UpdateSubscription operation

API operation name: Eees_EASDiscovery_UpdateSubscription

Description: The consumer updates an existing subscription for EAS discovery information.

Inputs: See clause 8.5.3.7.

Outputs: See clause 8.5.3.8.

See clause 8.5.2.3.4 for details of usage of this operation.

8.5.4.6 Eees_EASDiscovery_Unsubscribe operation

API operation name: Eees_EASDiscovery_Unsubscribe

Description: The consumer cancels an existing subscription for EAS discovery information.

Inputs: See clause 8.5.3.9.

Outputs: See clause 8.5.3.10.

See clause 8.5.2.3.5 for details of usage of this operation.

8.6 EES capability exposure to EAS and EEC

8.6.1 General

This clause describes service capability APIs exposed by the EES to the EAS(s) and EEC(s). The service capability APIs exposed include EES capabilities and exposed 3GPP Core Network capabilities. The 3GPP Core Network capabilities may be exposed from EES to the EAS(s) and also to the EEC(s).

The 3GPP Core Network capabilities APIs which are enhanced for exposure are also specified in this clause.

NOTE: When the ACR occurs, the new EAS can re-subscribe the EES capability exposure services on the T-EES.

8.6.2 UE location API

8.6.2.1 General

The EES exposes the UE location API to the EAS in order to support tracking or checking the valid location of the UE. The UE location API exposed by the EES relies on the 3GPP core network capabilities as specified in clause 8.10.3.

The EAS can request UE location API for one-time reporting to check current UE location and for continuous reporting to track UE's location.

The UE location API supports both request-response for one-time queries (in order to check UE's current location) as well as subscribe-notify models for providing UE's location to EAS on a continuous basis and enabling the EAS to track UE's location (as UE location changes).

8.6.2.2 Procedures

8.6.2.2.1 General

8.6.2.2.2 Request-response model

Figure 8.6.2.2.2-1 illustrates the interactions between the EES and the EAS for one-time location report.

Pre-conditions:

1. The EAS is authorized to discover and to use UE location API provided by the EES.
2. The EES is authorized to use Nnef Event Exposure API for UE location, based on service level agreement with MNO.
3. UE Identifier between EAS and the EES is authorized for the UE location API.

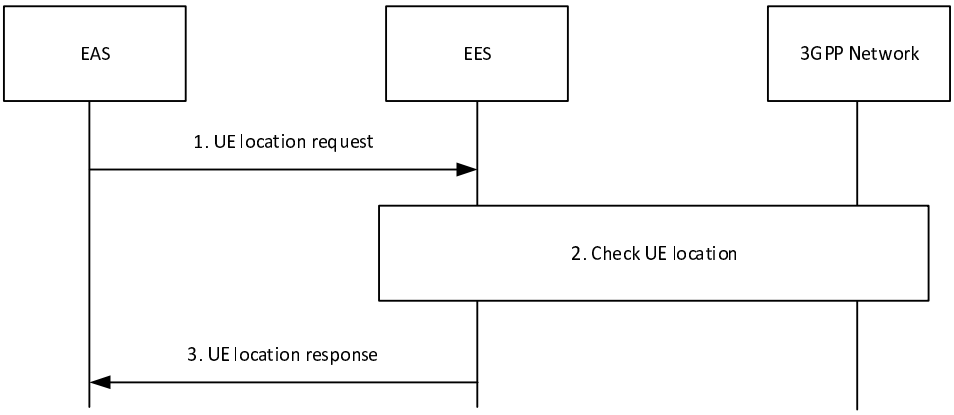

Figure 8.6.2.2.2-1: UE location API request-response model

1. The EAS sends UE location request to the EES. The UE location request shall include the UE Identifier. It may also include location granularity to indicate requested format of the location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.), which can be understood by the EAS and location QoS.

NOTE 1: The trigger condition of the UE location API is up to application service logic, which is out of scope of this specification.

2. The EES checks the UE location:
   a. If the UE location request from the EAS includes the location granularity, the EES considers the location granularity parameter for checking the location of the UE.
   b. If the EES has a valid locally cached location of the UE, the EES may use this cached UE location to respond to the EAS. Otherwise, the EES utilizes the capabilities of the 3GPP core network as specified in clause 8.10.3.
   c. The EES may modify the format of the UE location to fit to the location granularity requested from the EAS in the step 1, if supported. For example, if the EES receives the UE location in a format of tracking area ID or cell ID, the EES can modify the representation of the location information to the GPS Coordinates, or civic addresses (e.g. streets, districts, etc.) as requested by the EAS.

NOTE 2: Format modification mechanism of the UE location to fit the location granularity is outside the scope of this specification. Step 2.c. can be performed if the EES is deployed by the PLMN operator.

3. If successful, the EES responds to the EAS with the location of the UE, and optionally the timestamp of the location.

8.6.2.2.3 Subscribe-notify model

8.6.2.2.3.1 General

8.6.2.2.3.2 Subscribe

Figure 8.6.2.2.3.2-1 illustrates the subscribe operation between the EAS and the EES for continuous UE location reporting.

Pre-conditions:

1. The EAS is authorized to discover and to use UE location API provided by the EES;
2. The EES is authorized to use 3GPP network exposure capability (e.g. Nnef Event Exposure API) for UE location, based on service level agreement with MNO; and
3. UE Identifier or UE Group ID between EAS and the EES is authorized for the UE location API.

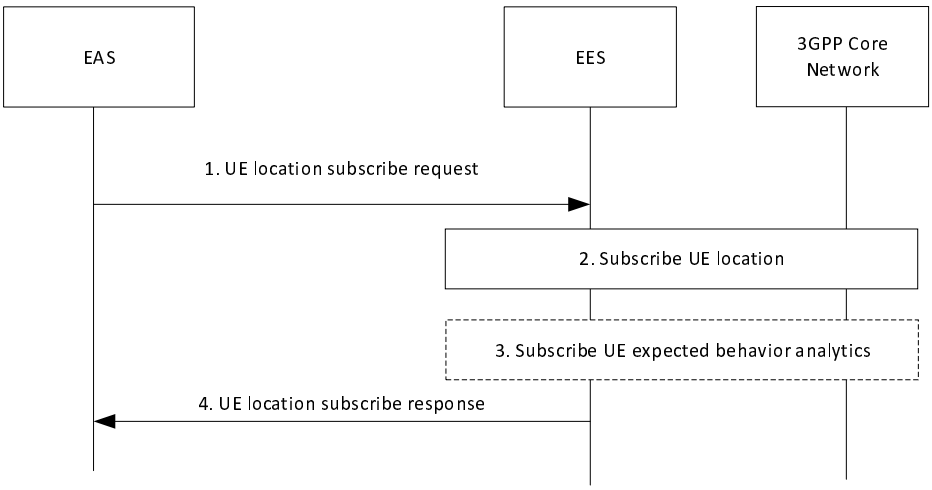

Figure 8.6.2.2.3.2-1: UE location API: Subscribe operation

1. The EAS sends UE location subscribe request to the EES for tracking a UE's location continuously. The UE location subscribe request shall include the UE Identifier or UE Group ID and may include proposed expiration time. It may also include location granularity to indicate requested format of the location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.), which can be understood by the EAS and location QoS.
2. The EES checks if the request from the EAS is authorized. If authorized, the EES sends success response to the EAS and utilizes the UE location exposure capability of the 3GPP core network as specified in clause 8.10.3. The EES requests continuous location reporting from the 3GPP system to have up to date location information of the UE(s).
3. The EES may subscribe to UE expected behaviour analytics (UE mobility) as described in 3GPP TS 23.288 [18].
4. The response includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EAS shall send a UE location subscription update request prior to the expiration time. If a UE location subscription update request is not received prior to the expiration time, the EES shall treat the EAS as implicitly unsubscribed. If it is not authorized, the EES sends failure response with rejection cause.

8.6.2.2.3.3 Notify

Figure 8.6.2.2.3.3-1 illustrates the notify operation between the EES and the EAS for continuous location.

Pre-conditions:

1. The EAS has subscribed to UE location API provided by the EES.

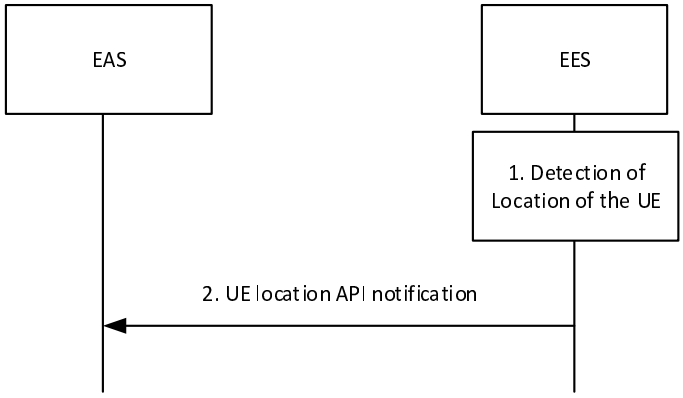

Figure 8.6.2.2.3.3-1: UE location API: Notify operation

1. The EES detects the location of a UE e.g., receiving location of a UE from the 3GPP system. The EES may cache the detected location information locally with timestamp as the latest location information of the UE(s) and start the notification aggregation for a group of UEs. The EES decides whether to aggregate and the aggregation period based on the analytics result received from the 3GPP Core Network, local policy and UE location subscription information received from the EAS. The EES determines to notify the location information of the UE(s) to the EAS which has subscribed for UE(s)'s location.

2. The EES sends UE location notification to the EAS. The EES includes the location of the UE(s). Each UE location includes UE ID and location type and may include the location accuracy and the timestamp of the location.

   The EES may modify the format of location information to fit to the location granularity requested from the EAS during the subscribe operation, if supported. For example, if the EES receives the UE location in a format of tracking area ID or cell ID, the EES can modify the representation of the location information to the GPS Coordinates, or civic addresses (e.g. streets, districts, etc.) as requested from the EAS.

8.6.2.2.3.4 Subscription update

Figure 8.6.2.2.3.4-1 illustrates the subscription update operation between the EAS and the EES.

Pre-conditions:

1. The EAS has subscribed to UE location API provided by the EES.

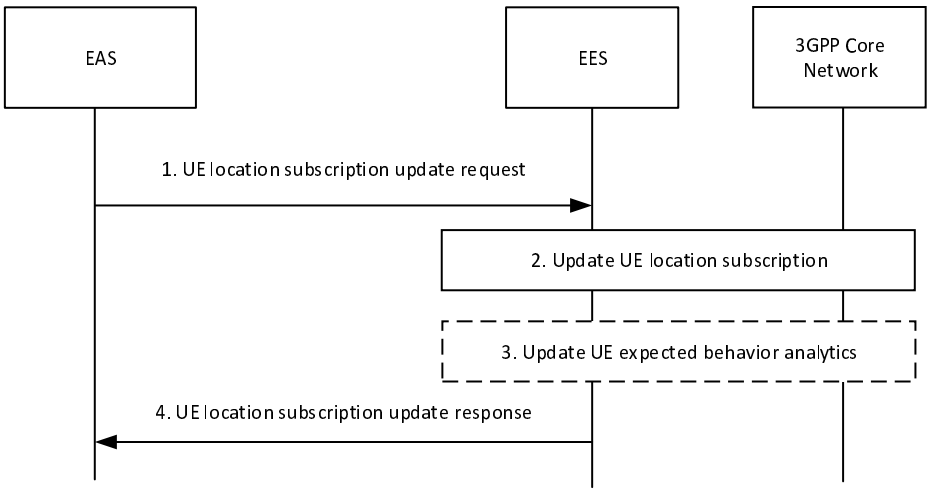

Figure 8.6.2.2.3.4-1: UE location API: Subscription update operation

1. The EAS sends UE location subscription update request to the EES. The request includes the subscription identifier of the subscription to be updated. The UE location subscription update request may also include proposed expiration time for the updated subscription, updated Location granularity and Location QoS.
2. The EES checks if the request from the EAS is authorized. If authorized, the EES updates the subscription request and may update the UE location subscription in the 3GPP Core Network.
3. The EES may update the subscription to the UE expected behaviour analytics.
4. The EES sends the UE location subscription update response to the EAS.

8.6.2.2.3.5 Unsubscribe

Figure 8.6.2.2.3.5-1 illustrates the unsubscribe operation between the EAS and the EES to stop the UE location notifications.

Pre-conditions:

1. The EAS has subscribed to UE location API provided by the EES.

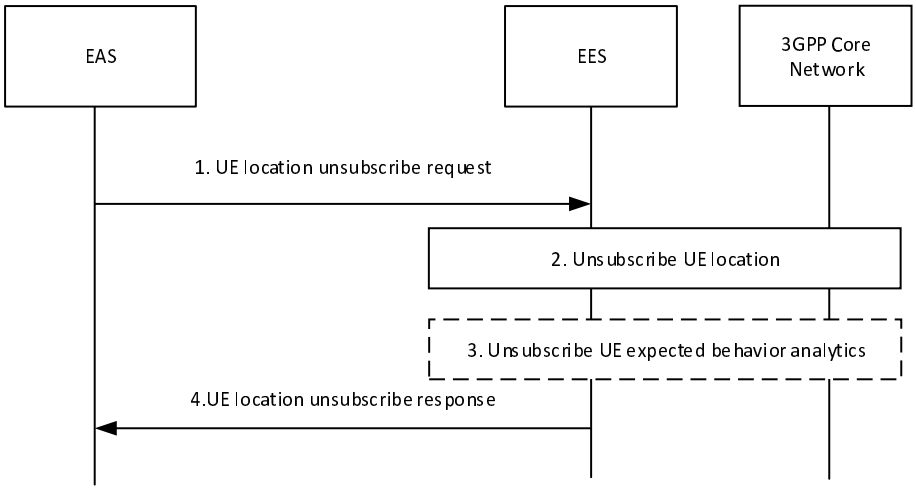

Figure 8.6.2.2.3.5-1: UE location API: unsubscribe operation

1. The EAS sends the UE location unsubscribe request to the EES.
2. The EES checks if the EAS is authorized or not. If authorized, the EES terminates the subscription of the EAS and unsubscribes the UE location from the 3GPP Core Network.
3. The EES unsubscribes from the UE expected behaviour analytics, if applicable.
4. The EES responds to the EAS.

8.6.2.3 Information flows

8.6.2.3.1 General

The following information flows are specified for UE location API:

- UE location request and response; and
- UE location subscription, notification, subscription update and unsubscribe.

8.6.2.3.2 UE location request

Table 8.6.2.3.2-1: UE location request

Information element	Status	Description
UE ID	M	Identifies the UE for which location will be reported (i.e., GPSI)
Security credentials	M	Security credentials of the EAS
Location granularity	O	Indicates format of location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.) that can be understood by the EAS
Location QoS	O	Indicates the location quality of service as described in clause 4.1b of 3GPP TS 23.273 [9].

8.6.2.3.3 UE location response

Table 8.6.2.3.3-1: UE location response

Information element	Status	Description
Successful response	O	Indicates that the UE location request was successful
> UE location	M	Location of the UE
> Timestamp	O	Indicates the age of the UE's location information
> Location accuracy	O	Indicates accuracy of the location information
Failure response	O	Indicates that the subscription request failed
> Cause	O	Indicates the cause of request failure

8.6.2.3.4 UE location subscribe request

Table 8.6.2.3.4-1: UE location subscribe request

Information element	Status	Description
EASID	M	The identifier of the EAS
UE ID (NOTE)	O	Identifies the UE for which location will be reported (i.e., GPSI)
UE Group ID (NOTE)	O	Identifies a group of UEs as defined in clause 7.2.7
Security credentials	M	Security credentials of the EAS
Notification Target Address	M	Notification Target Address of the EAS where the notification is to be sent by the EES
Event reporting information	O	Event Reporting Information as specified in Table 4.15.1-1 of 3GPP TS 23.502 [3], e.g. event reporting mode.
Proposed expiration time	O	Proposed expiration time for the subscription
Location Granularity	O	indicates format of location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.) that can be understood by the EAS
Location QoS	O	Indicate the location quality of service as described in clause 4.1b of 3GPP TS 23.273 [9].
NOTE: Either UE ID or UE Group ID shall be provided.		

8.6.2.3.5 UE location subscribe response

Table 8.6.2.3.5-1: UE location subscribe response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.6.2.3.6 UE location notification

Table 8.6.2.3.6-1: UE location notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
List of event notifications	M	A list of event notifications for one or more UEs.
> UE ID	M	The identifier of each UE (i.e., GPSI)
> UE location	M	Location of the UE
> Timestamp	O	Indicates the age of the location information
> Location accuracy	O	Indicates accuracy of the location information
> Location type	M	Indicates whether it is a predictive or actual UE location change.

8.6.2.3.7 UE location subscription update request

Table 8.6.2.3.7-1: UE location subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials of the EAS
Event reporting information (NOTE)	O	Event Reporting Information as specified in Table 4.15.1-1 of 3GPP TS 23.502 [3], e.g. event reporting mode.
Proposed expiration time (NOTE)	O	Proposed expiration time for the subscription
Notification Target Address (NOTE)	O	Notification Target Address of the EAS where the notification is to be sent by the EES
Location Granularity (NOTE)	O	indicates format of location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.) that can be understood by the EAS
Location QoS (NOTE)	O	Indicate the location quality of service as described in clause 4.1b of 3GPP TS 23.273 [9].
NOTE: At least one of these IEs is present.		

8.6.2.3.8 UE location subscription update response

Table 8.6.2.3.8-1: UE location subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.6.2.3.9 UE location unsubscribe request

Table 8.6.2.3.9-1: UE location unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
Security credentials	M	Security credentials of the EAS

8.6.2.3.10 UE location unsubscribe response

Table 8.6.2.3.10-1: UE location unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.6.2.4 APIs

8.6.2.4.1 General

Table 8.6.2.4.1-1 illustrates the API for UE location.

Table 8.6.2.4.1-1: Eees_UELocation API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_UELocation	Get	Request/Response	EAS
	Subscribe	Subscribe/Notify	EAS
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.6.2.4.2 Eees_UELocation_Get operation

API operation name: Eees_UELocation_Get

Description: The consumer requests one time report of a UE's location.

Inputs: See clause 8.6.2.3.2.

Outputs: See clause 8.6.2.3.3.

See clause 8.6.2.2.2 for details of usage of this operation.

8.6.2.4.3 Eees_UELocation_Subscribe operation

API operation name: Eees_UELocation_Subscribe

Description: The consumer subscribes for continuous reporting of a UE's location.

Inputs: See clause 8.6.2.3.4.

Outputs: See clause 8.6.2.3.5.

See clause 8.6.2.2.3.2 for details of usage of this operation.

8.6.2.4.4 Eees_UELocation_Notify operation

API operation name: Eees_UELocation_Notify

Description: The consumer is notified with report of the UE's location.

Inputs: See clause 8.6.2.3.6.

Outputs: None.

See clause 8.6.2.2.3.3 for details of usage of this operation.

8.6.2.4.5 Eees_UELocation_UpdateSubscription operation

API operation name: Eees_UELocation_UpdateSubscription

Description: The consumer updates an existing subscription for continuous reporting of a UE's location.

Inputs: See clause 8.6.2.3.7.

Outputs: See clause 8.6.2.3.8.

See clause 8.6.2.2.3.4 for details of usage of this operation.

8.6.2.4.6 Eees_UELocation_Unsubscribe operation

API operation name: Eees_UELocation_Unsubscribe

Description: The consumer cancels an existing subscription for continuous reporting of a UE's location.

Inputs: See clause 8.6.2.3.9.

Outputs: See clause 8.6.2.3.10.

See clause 8.6.2.2.3.5 for details of usage of this operation.

8.6.3 ACR management events

8.6.3.1 General

The EES exposes ACR management event notifications of one or more UEs to an EAS. EES also uses ACR management event notifications to inform the EAS of the need to start an ACT or cancel a previously started ACT. ACR management event notifications exposed by the EES may rely on the NEF northbound API for monitoring event of user plane path management event.

This capability exposed by the EES supports:

- "User plane path change". This event supports to detect user plane path change for the application traffic and report the corresponding notification with user plane path change to the EAS.
- "ACR monitoring". This event supports to detect user plane path change for the application traffic, discover the T-EAS(s), and report the corresponding notification with the discovered T-EAS(s).
- "ACR facilitation". This event supports to detect user plane path change for the application traffic, make the decision for ACR, discover the T-EAS(s), influence the traffic for the selected T-EAS and report the corresponding notification with the selected T-EAS.
- "ACT start/stop". This event informs the EAS the need to start or stop an ACT towards or from another EAS for a particular UE. The "ACT start" can also inform the EAS of the ACR parameters.
- "ACR Selection". This event informs the EAS about the selected ACR scenario list for each AC using the EAS.

The availability of the ACR management event notifications relying on the user plane path management event notification service exposed by 5GC may change due to UE mobility between 5GC and EPC. If an EES exposes ACR event notifications to EAS(s) for a UE by relying on the 3GPP Core Network northbound API for user plane path management notifications, the EES monitors the availability of the northbound API for UE(s) served by the EAS (e.g. by utilizing Nnef_APISupportCapability as described in 3GPP TS 23.502 [3]) and provides the availability information to the EAS accordingly. If CAPIF is supported, the EES determines if the ACR management event API is available and able to be exposed to the EAS for a UE via the Availability of service APIs event notifications provided by the CAPIF core function as defined in 3GPP TS 23.222 [6].

8.6.3.2 Procedures

8.6.3.2.1 General

8.6.3.2.2 Subscribe

Figure 8.6.3.2.2-1 illustrates the subscribe operation between the EAS and the EES for ACR management event notifications.

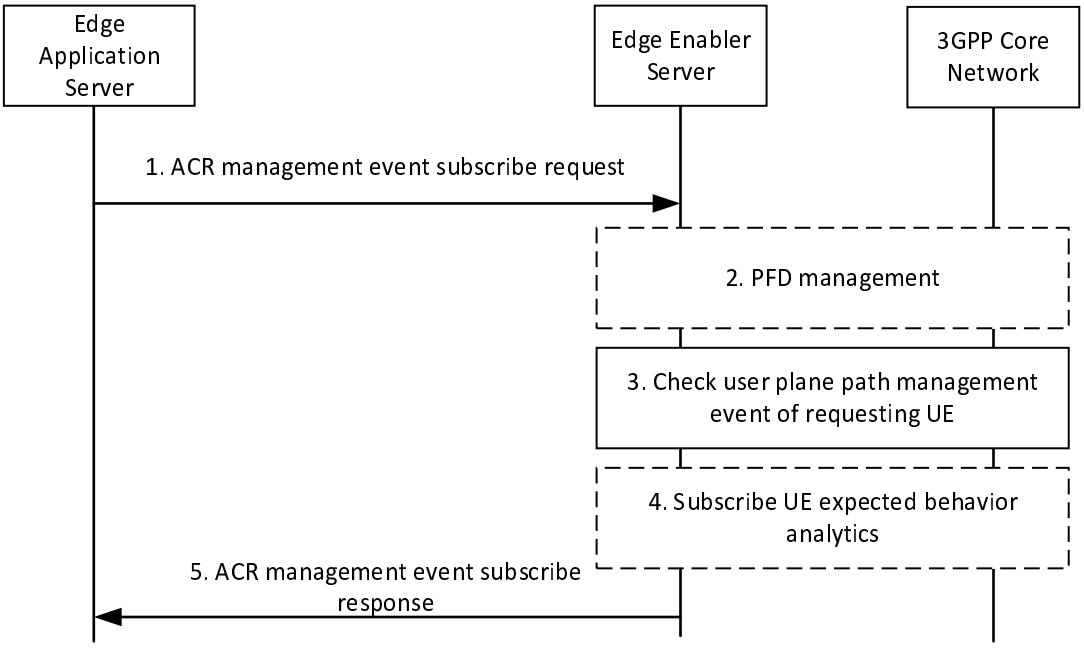

Figure 8.6.3.2.2-1: ACR management event API: Subscribe operation

1. The EAS sends ACR management event subscribe request (e.g. tracking the UE's user plane path change continuously). The EAS shall include UE Identifier or UE Group ID for "user plane path change", "ACR monitoring" and "ACR facilitation" events.

   a. The EAS may include the "user plane path change" event to indicate the EES to notify the EAS when the EES detects there is a user plane path change for the application traffic and the EAS may include Subscription Type (Early and/or Late notification defined in clause 5.6.7 of 3GPP TS 23.501 [2]) and/or Indication of EAS Acknowledgement in the event subscription.

   b. The EAS may include the "ACR monitoring" event to indicate the EES to notify the EAS when the EES detects there is a need for the ACR (e.g. when T-EAS is available at the target DNAI). The EAS may also include the Event Filters to specify the conditions to match for notifying the event, e.g., inter-EDN mobility, intra-EDN mobility.

   c. The EAS may include the "ACR facilitation" event to request the EES to make the decision for ACR, discover the T-EAS(s), influence the traffic for the selected T-EAS and notify the S-EAS of the selected T-EAS. If required, the EAS can add an indication to request service continuity planning.

   d. The EAS may include the "ACT start/stop" event to indicate the EES to notify the EAS of the need for start or stop ACT to or from another EAS for a particular UE. The EES may also use "ACT start" event to notify the EAS of the ACR parameters.

   e. The EAS may include the “ACR Selection” event to indicate the EES to notify the EAS of the selected ACR scenario list applicable to ACs using the EAS.

2. The EES checks if the EAS is authorized for this operation.

If authorized, and if the subscription in step 1 includes at least one of the "user plane path change", "ACR monitoring" and "ACR facilitation" events, the EES may invoke the PFD management procedure with the 3GPP Core Network as described in 3GPP TS 23.682 [10] and 3GPP TS 23.502 [8] with an application id. The traffic filter information sent by the EAS is used in requesting PFD management service. Further the EES provides the same application id for requesting user plane path management event service.

NOTE 1: PFD management can be optionally supported in MNO. If EES cannot invoke step 2a, it responds EAS with appropriate error.

NOTE 2: The EES can map the EASID into the application id that is used to invoke the PFD management procedure.

3. If the subscription in step 1 includes at least one of the "user plane path change", "ACR monitoring" and "ACR facilitation" events, the EES checks if there exists a subscription with the 3GPP core network for the user plane path management event notifications corresponding to the UE information obtained in step 1 as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], which may be triggered by other EAS for the same UE. The EES checks the availability of the user plane path management event service for the UE(s).

   a. if a subscription with 3GPP core network does not exist, then the EES subscribes with the 3GPP core network (PCF, NEF or SCEF+NEF) for the user plane path management event notifications of the UE(s) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3] If the EAS provides Subscription Type and/or Indication of EAS Acknowledgement, the EES include the type of subscription and/or the indication of "AF acknowledgement to be expected" as information on AF subscription to corresponding SMF events within the AF Request;

   b. if a subscription with 3GPP core network exists, then the EES uses the locally cached user plane path management event notification information of the UE(s) to respond to the EAS.

      The EES stores the subscription related to the EAS.

4. If the event is "user plane path change", the EES may subscribe to UE expected behaviour analytics (UE mobility and UE communication) for the group of UEs as described in 3GPP TS 23.288 [18].

5. If EAS is authorized, the EES responds with ACR management event subscribe response. If EAS is not authorized, the EES provides a rejection response with cause information.

   If the target UE(s) and the 3GPP network support mobility between 5GC and EPC, the EES monitors the availability of the user plane path management event notification from the 3GPP network by utilizing Nnef_APISupportCapability or Availability of service APIs event notifications provided by the CAPIF core function.

8.6.3.2.3 Notify

Figure 8.6.3.2.3-1 illustrates the notify operation between the EES and the EAS for continuous ACR management event notifications.

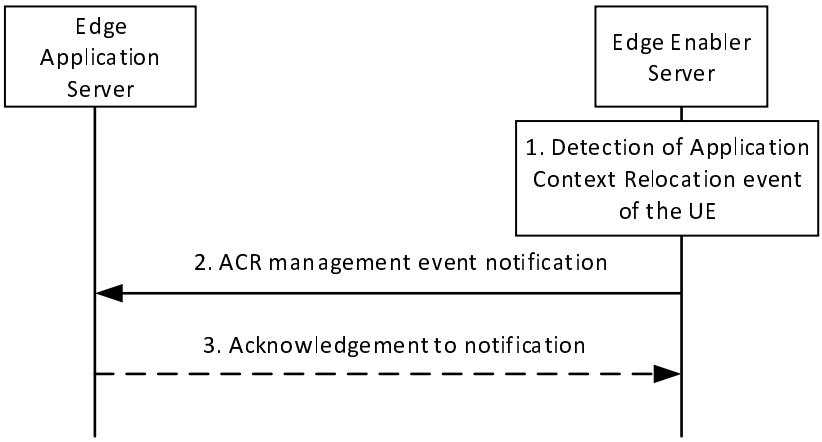

Figure 8.6.3.2.3-1: ACR management event API: Notify operation

1. The EES detects the ACR management event of a UE (e.g. receiving User plane path management event notification for a UE from the 3GPP core network) , or receiving ACR request from the EEC, or when the selected ACR scenario list for a particular AC changes.

   a. If "user plane path change" Event is subscribed, the EES may cache the detected User plane path management event notification locally with timestamp as the latest information of the UE(s) and start the notification aggregation for a group of UEs. The EES decides whether to aggregate and the aggregation period based on the analytics result received from the 3GPP Core Network, local policy and User Plane path management subscription information received from the EAS. The EES determines to notify the user plane path management event notification information (e.g., DNAI) to the EASs which has subscribed for the "user plane path management" event.

   b. If "ACR monitoring" Event is subscribed, based on the detected user plane path change report sent from the 3GPP core network, the EES checks whether the target DNAI is in the EAS profile of the subscribing EAS, if not it further checks whether a T-EAS is available at the target DNAI as described in steps 2-4 of clause 8.8.3.2. If a T-EAS is available, the EES notifies the EAS with T-EAS endpoint; otherwise this event notification will not be sent. Also, when the EES receives the ACR request from the EEC, the EES decides to send the notification to the EAS.

   c. If "ACR facilitation" Event is subscribed, based on the detected user plane path change report sent from the 3GPP core network, the EES checks whether the target DNAI is in the EAS profile of the subscribing EAS, if not it further checks whether a T-EAS is available at the target DNAI as described in steps 2-4 of clause 8.8.3.2. If a T-EAS is available, the EES selects the T-EAS from the discovered EAS list and applies the AF traffic influence with the N6 routing information of the selected T-EAS in the 3GPP Core Network. The EES also notifies the S-EAS with the selected T-EAS endpoint.

   d. If "ACT start/stop" event is subscribed, during the ACR launch if the EEC indicates the need to notify the EAS in the ACR request as described in clause 8.8.3.4, the EES shall send notification to the EAS to inform it about the need to start or stop the ACT to or from another EAS. The EES may include a service continuity planning indication so that the EES will monitor UE location. The notification message includes ACR identity (ACID, UE ID, S-EAS endpoint and T-EAS endpoint).

   e. If “ACR Selection” event is subscribed, the EES shall send notification to the EAS to update the selected ACR scenario list applicable for a particular AC (ACID, UE ID) if an update was received as described in clause 8.15.2.2.

2. The EES sends ACR management event notification to the EAS. The EES includes the ACR management event notification information of the UE(s) and optionally the timestamp. If the event triggering the notification is DNAI change, the timestamp can be included to indicate the age of the user plane path management event notification information. The EES may only provide part of information included in the user plane path management event notification from 3GPP network (e.g. target DNAI). If the EAS had provided "Indication of EAS acknowledgement", the EES waits for acknowledgement from the EAS before it sends AF acknowledgement to the 3GPP core network.

If the event is "ACT start/stop", the notification shall include the endpoint address of the other EAS and the UE ID. The "ACT start" notification may include ACR parameters as per clause 8.8.3.9. Upon receiving the notification about the start of the ACR execution with "ACT start" event, the S-EAS avoids triggering a second ACR execution for the same identity (ACID, UE ID, S-EAS endpoint and T-EAS endpoint) until the current ACR execution is completed.

NOTE: How long the detection entity should wait for current ACT to complete in order to start to detect or to decide another ACR is up to the implementation.

If the event is “ACR Selection”, the notification shall include the selected ACR scenario list, ACID and UE ID. Upon receiving the notification, the EAS determines if it should perform ACR detection and/or ACR decision for a particular AC (ACID, UE ID).

3. If the EAS had included Indication of EAS Acknowledgement within ACR management event subscribe request described in clause 8.6.3.2.1, the EAS sends EAS Acknowledgement as a response to ACR management event notification to the EES either immediately or after the required ACT is completed. The EAS may reply in negative, e.g., the EAS may determine not to perform ACR. Then, the EES sends the AF acknowledgement to the 3GPP core network.

   If the EAS had included Indication of EAS acknowledgement for service continuity planning within ACR management event subscribe request described in clause 8.6.3.2.1, the EAS sends EAS Acknowledgement as a response to ACR management event notification for service continuity planning of which detailed procedure is described in step 4 of clause 8.8.3.9.

8.6.3.2.4 Subscription update

Figure 8.6.3.2.4-1 illustrates the subscription update operation between the EAS and the EES for ACR management event notifications.

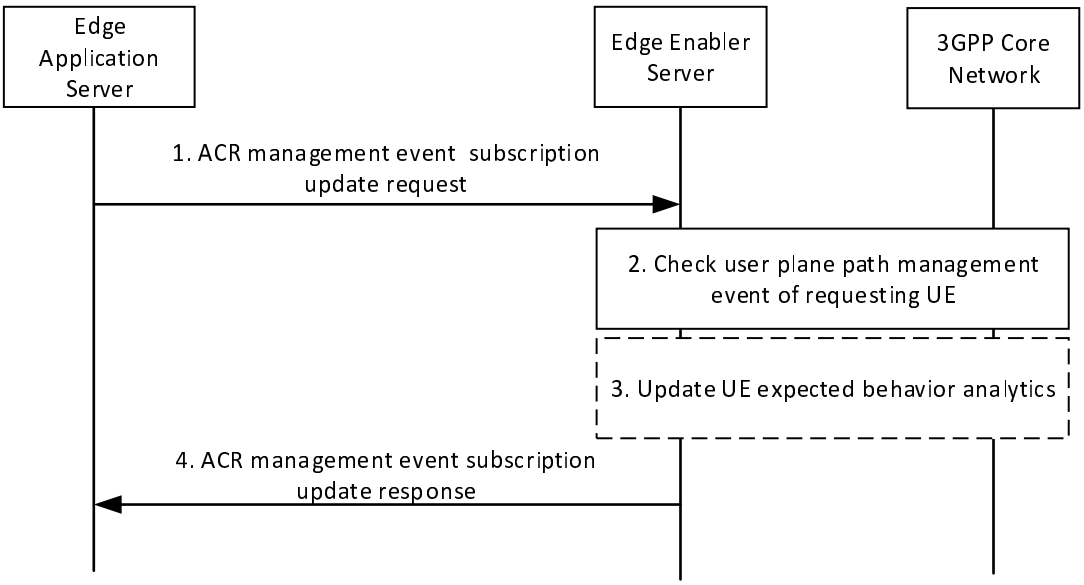

Figure 8.6.3.2.4-1: ACR management event API: Subscription update operation

1. The EAS sends ACR management event subscription update request to update an existing subscription. The subscription update request may include Event ID, Event Filter, Event Report, Subscription Type (Early and/or Late notification defined in clause 5.6.7 of 3GPP TS 23.501 [2]) and/or Indication of EAS Acknowledgement.

2. The EES checks if the EAS is authorized for the operation.

   If authorized and if the subscription in step 1 includes only "ACT start/stop" event, the EES stores the updated subscription related to the EAS and step 3 is skipped.

If authorized, and if the subscription in step 1 includes at least one of the "user plane path change", "ACR monitoring" and "ACR facilitation" events, the EES checks if there exists a subscription with the 3GPP core network for the user plane path management event notifications corresponding to the updated information obtained in step 1 as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], which may be triggered by other EAS for the same UE.

a. if a subscription with 3GPP core network does not exist corresponding to the updated information, then the EES subscribes with the 3GPP core network (PCF, NEF or SCEF+NEF) for the user plane path management event notifications of the UE(s) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3] If the EAS provides Subscription Type and/or Indication of EAS Acknowledgement, the EES includes the type of subscription and/or the indication of "AF acknowledgement to be expected" as information on AF subscription to corresponding SMF events within the AF Request;

b. if a subscription with 3GPP core network exists corresponding to the updated information, then the EES uses the locally cached user plane path management event notification information of the UE(s) to respond to the EAS.

The EES stores the updated subscription related to the EAS.

3. The EES may update the subscription to the UE expected behaviour analytics.

4. The EES responds with ACR management event subscription response.

8.6.3.2.5 Unsubscribe

Figure 8.6.3.2.5-1 illustrates the unsubscribe operation between the EAS and the EES for ACR management event notifications.

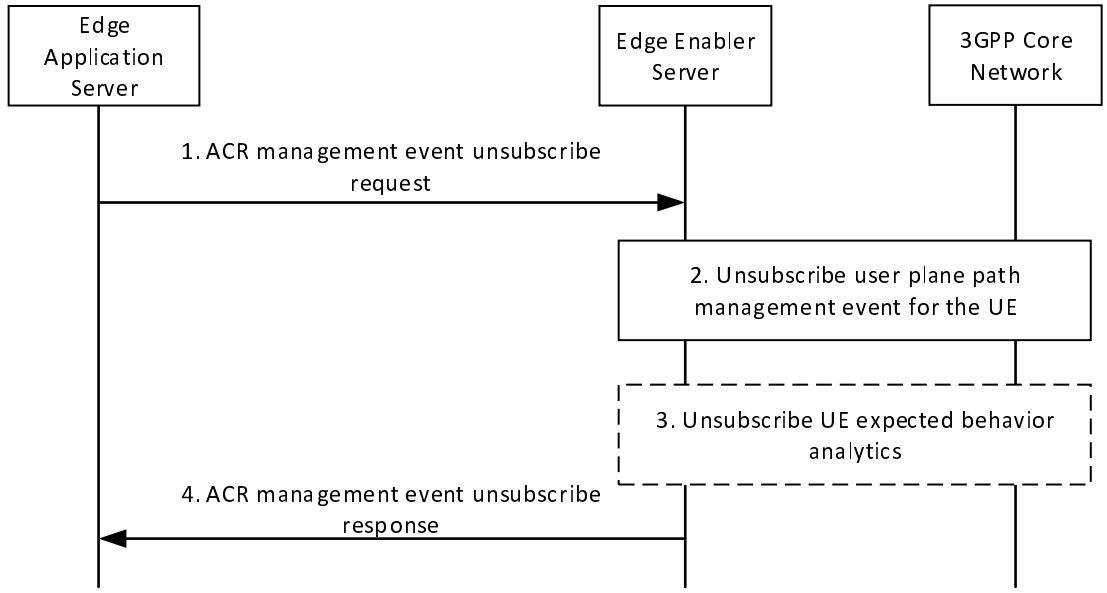

Figure 8.6.3.2.5-1: ACR management event API: Unsubscribe operation

1. The EAS sends ACR management event unsubscribe request to the EES to cancel the ACR management event subscription.

2. The EES checks if another EAS requires to track the UE's user plane path change or not. If not, the EES unsubscribes the user plane path management event notifications from the 3GPP core network for the corresponding UE.

3. The EES unsubscribes from the UE expected behaviour analytics, if applicable.

4. The EES checks if the EAS is authorized for the operation. If authorized, the EES removes the subscription related to the EAS and sends ACR management event unsubscribe response to the EAS.

8.6.3.3 Information flows

8.6.3.3.1 General

The following information flows are specified for ACR management event API:

- ACR management event subscription, notification, subscription update and unsubscribe.

8.6.3.3.2 ACR management event subscribe request

Table 8.6.3.3.2-1 describes the information elements for an ACR management event subscribe request from the EAS to the EES.

Table 8.6.3.3.2-1: ACR management event subscribe request

Information element	Status	Description
EASID	M	The identifier of the EAS
Security credentials	M	Security credentials of the EAS
UE ID (NOTE 1)	O	The identifier of the UE (i.e., GPSI)
UE Group ID (NOTE 1)	O	Identifies a group of UEs as defined in clause 7.2.7
Event ID(s)	M	Event ID: - user plane path change - ACR monitoring - ACR facilitation - ACT start/stop - ACR selection
Indication of service continuity planning (NOTE 3)	O	Indicates that whether the service continuity planning is required i.e. whether EES shall monitor UE entering the predicted location.
Traffic filter information	O	The traffic filter information includes IP flow description, domain description (domain name, applicable protocol and matching criteria) or URI. Applicable for the "user plane path change" event, the "ACR monitoring" event and "ACR facilitation" event.
Event Report (NOTE 2)	O	Event Reporting Information as specified in 3GPP TS 23.502 [3]
Notification Target Address	M	Notification Target Address of the EAS where the notification is to be sent by the EES
Type of subscription	O	Indicates Early and/or Late notification to inform if the notification needs to be received before and/or after UP path configuration. Applicable for the "user plane path change" event.
Indication of EAS acknowledgement	O	This IE indicates the EES to include indication of "AF acknowledgement to be expected" within the AF request for subscribing UP path management events to 3GPP network and that the EAS will provide an acknowledgement as a response for the notifications of UP path management events to the EES. Applicable for the "user plane path change" event.
Indication of EAS acknowledgement for service continuity planning	O	This IE indicates that the EAS will provide an acknowledgement as a response to the notification of ACR management notification related to service continuity planning.
Event Filter	O	Event filter as specified in 3GPP TS 23.501 [2]
EAS characteristics for ACR	O	Set of characteristics to determine required EAS as detailed in Table 8.5.3.2-2. Applicable for the "ACR monitoring" event and "ACR facilitation" event.
NOTE 1: Either UE ID or UE Group ID shall be provided if the Event ID(s) includes any of the "user plane path change", "ACR monitoring" and "ACR facilitation" events. UE ID or UE Group ID are not applicable to "ACT start/stop" and "ACR selection" event. NOTE 2: This IE shall be present if the Event ID(s) includes any of the "user plane path change", "ACR monitoring" and "ACR facilitation" events. This IE is not applicable to "ACT start/stop" and "ACR selection" event. NOTE 3: This IE is applicable for "ACR monitoring", "ACR facilitation".		

8.6.3.3.3 ACR management event subscribe response

Table 8.6.3.3.3-1 describes the information elements for an ACR management event subscribe response from the EES to the EAS.

Table 8.6.3.3.3-1: ACR management event API subscribe response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time. If the Expiration time IE is not included, it indicates that the subscription never expires.
Failure response (NOTE)	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
NOTE: One of these IEs shall be present in the message.		

8.6.3.3.4 ACR management event notification

Table 8.6.3.3.4-1 describes the information elements for an ACR management event notification from the EES to the EAS.

Table 8.6.3.3.4-1: ACR management event notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
List of event notifications	M	A list of event notifications for one or more UEs.
> Event ID	M	The event ID for which the notification is triggered: - user plane path change - ACR monitoring - ACR facilitation - ACT start/stop - ACR Selection
> Event report (NOTE 1)	O	Event reporting information as specified in clause 5.2.8.3.1 of 3GPP TS 23.502 [3]
> Timestamp	O	The timestamp of each event report.
> EAS endpoint	O	The T-EAS endpoint shall be included for the "ACR monitoring" event and "ACR facilitation" event. In case of "ACT start/stop" event, the endpoint address of the EAS to or from which the ACT is needed to start/stop.
> Indication of service continuity planning	O	Indicating EES will monitor UE entering the predicted location.
> Selected ACR scenario list (NOTE 2)	O	The list of ACR scenarios.
> EAS bundle list (NOTE 2)	O	The EAS bundle list.
>> EAS ID (NOTE 4)	M	EAS ID in a bundle.
>> DNAIs and service area of the EAS	O	For the EAS ID in a bundle, it includes the DNAIs and/or service area, as described in "EAS Geographical Service Area" IE, "EAS Topological Service Area" IE and "List of EAS DNAI(s)" IE of Table 8.2.4-1.
> ACR parameters (NOTE 3)	O	ACR parameters
>> Prediction expiration time	O	The estimated time the UE may reach the Predicted/Expected UE location or EAS service area at the latest.
UEID	O	The identifier of the UE
ACID	O	The identifier of the AC
NOTE 1: This IE shall be present if the Event ID(s) includes any of the "user plane path change", "ACR monitoring" and "ACR facilitation" events. This IE is not applicable to "ACT start/stop" and "ACR Selection" events. NOTE 2: This IE shall be present only in case of "ACR Selection" event. NOTE 3: This IE is applicable only when the ACT start event notification is used to send ACR parameters to the T-EAS as per clause 8.8.3.9. NOTE 4: Main EAS ID in a bundle does not need to be included.		

8.6.3.3.5 ACR management event subscription update request

Table 8.6.3.3.5-1 describes the information elements for an ACR management event subscribe request from the EAS to the EES.

Table 8.6.3.3.5-1: ACR management event subscription update request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription ID	M	The identifier of the subscription to be updated.
Event ID(s) (NOTE)	O	Event ID(s) as specified in 3GPP TS 23.501 [2]
Event Report (NOTE)	O	Event Reporting Information as specified in 3GPP TS 23.502 [3]
Type of subscription (NOTE)	O	Indicates Early and/or Late notification to inform if the notification needs to be received before and/or after UP path configuration.
Indication of EAS acknowledgement (NOTE)	O	This IE indicates the EES to include indication of "AF acknowledgement to be expected" within the AF request for subscribing UP path management events to 3GPP network and that the EAS will provide an acknowledgement as a response for the notifications of UP path management events to the EES.
Event Filter (NOTE)	O	Event filter as specified in 3GPP TS 23.501 [2]
EAS characteristics for ACR (NOTE)	O	Set of characteristics to determine required EAS as detailed in Table 8.5.3.2-2. Applicable for the "ACR monitoring" event and "ACR facilitation" event.
NOTE: At least one of these IEs shall be present in the message.		

8.6.3.3.6 ACR management event subscription update response

Table 8.6.3.3.6-1 describes the information elements for an ACR management event subscription update response from the EES to the EAS.

Table 8.6.3.3.6-1: ACR management event subscription update response

Information element	Status	Description
Successful response(NOTE 2)	O	Indicates that the subscription update request was successful.
> Expiration time (NOTE 1)	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response(NOTE 2)	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure
NOTE 1: If the Expiry time IE is not included, it indicates that the subscription never expires. NOTE 2: One of these IEs shall be present in the message.		

8.6.3.3.7 ACR management event unsubscribe request

Table 8.6.3.3.7-1 describes the information elements for an ACR management event unsubscribe request from the EAS to the EES.

Table 8.6.3.3.7-1: ACR management event unsubscribe request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request

8.6.3.3.8 ACR management event unsubscribe response

Table 8.6.3.3.8-1 describes the information elements for an ACR management event unsubscribe response from the EES to the EAS.

Table 8.6.3.3.8-1: ACR management event unsubscribe response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the unsubscribe request was successful.
Failure response (NOTE)	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure
NOTE: One of these IEs shall be present in the message.		

8.6.3.4 APIs

8.6.3.4.1 General

Table 8.6.3.4.1-1 illustrates the API for ACR management event.

Table 8.6.3.4.1-1: Eees_ACRManagementEvent API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_ACRManagementEvent	Subscribe	Subscribe/Notify	EAS
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.6.3.4.2 Eees_ACRManagementEvent_Subscribe operation

API operation name: Eees_ACRManagementEvent_subscribe

Description: The consumer subscribes to receive an ACR management event.

Inputs: See clause 8.6.3.3.2.

Outputs: See clause 8.6.3.3.3.

See clause 8.6.3.2.2 for details of usage of this operation.

8.6.3.4.3 Eees_ACRManagementEvent_Notify operation

API operation name: Eees_ACRManagementEvent_Notify

Description: The consumer is notified of an event by the EES.

Inputs: See clause 8.6.3.3.4.

Outputs: None.

See clause 8.6.3.2.3 for details of usage of this operation.

8.6.3.4.4 Eees_ACRManagementEvent_UpdateSubscription operation

API operation name: Eees_ACRManagementEvent_UpdateSubscription

Description: The consumer updates an existing subscription for an ACR management event.

Inputs: See clause 8.6.3.3.5.

Outputs: See clause 8.6.3.3.6.

See clause 8.6.3.2.4 for details of usage of this operation.

8.6.3.4.5 Eees_ACRManagementEvent_Unsubscribe operation

API operation name: Eees_ACRManagementEvent_Unsubscribe

Description: The consumer unsubscribes for the previously subscribed events.

Inputs: See clause 8.6.3.3.7.

Outputs: See clause 8.6.3.3.8.

See clause 8.6.3.2.5 for details of usage of this operation.

8.6.4 AC information exposure API

8.6.4.1 General

AC information exposure enables EASs to obtain information about capabilities of ACs from the EESs. This information may facilitate communications between EASs and ACs, e.g. push notifications. The information shared is subject to access control as well as privacy and security mechanisms.

8.6.4.2 Procedures

8.6.4.2.1 General

8.6.4.2.2 Subscribe

Figure 8.6.4.2.2-1 illustrates the AC information subscription procedure between the EAS and the EES.

Pre-conditions:

1. The EAS is registered with the EES; and
2. The AC Profiles of the ACs on the UE are available at the EEC on the UE.

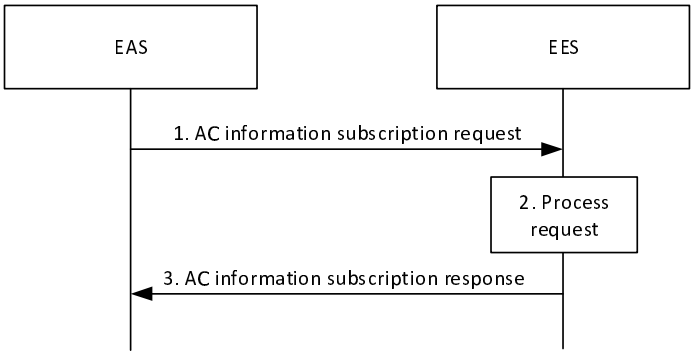

Figure 8.6.4.2.2-1: AC information subscription

1. The EAS sends an AC information subscription request to the EES. The request may contain filters to retrieve information about particular ACs e.g. AC profile parameters or parameter ranges to be matched, specific UE Identifiers, location ranges, etc.

NOTE: The trigger conditions of the AC information API (e.g. resource load predictive analytics) are up to service logic, which is out of scope of this specification.

2. Upon receiving the request from the EAS, the EES performs an authorization check to verify whether the EAS has authorization to perform the operation. The EES determines the matching AC information corresponding to the filter provided and composes a result. The EES stores the subscription information for future processing.

3. The EES sends an AC information subscription response to the EAS with the result composed in step 2.

8.6.4.2.3 Notify

Figure 8.6.4.2.3-1 illustrates the AC information notification procedure between the EES and the EAS.

Pre-conditions:

1. The EAS subscribed for AC information at the EES.

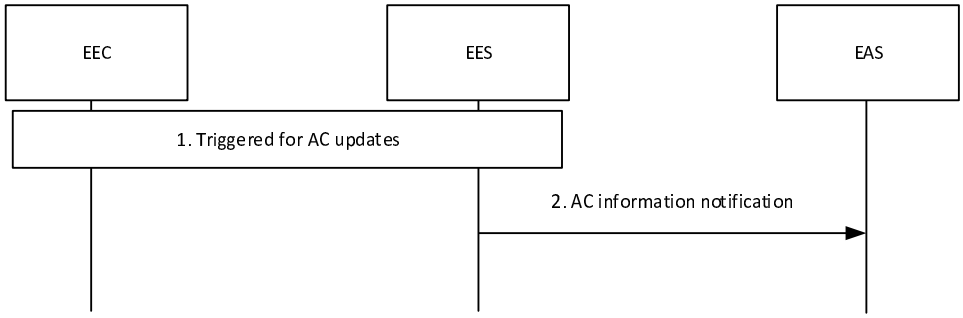

Figure 8.6.4.2.3-1: AC information notification

1. The EES is triggered for AC information updates, e.g. it receives an EEC registration request, it determines if it matches the filter provided by the EAS, e.g. if the AC Geographical Service Area is included in the EAS provided Geographical Service Area.
2. The EES sends an AC information notification to the EAS.

8.6.4.2.4 Subscription update

Figure 8.6.4.2.4-1 illustrates the AC information subscription update procedure between the EAS and the EES.

Pre-conditions:

1. The EAS has subscribed for AC information as described in clause 8.6.4.2.2.

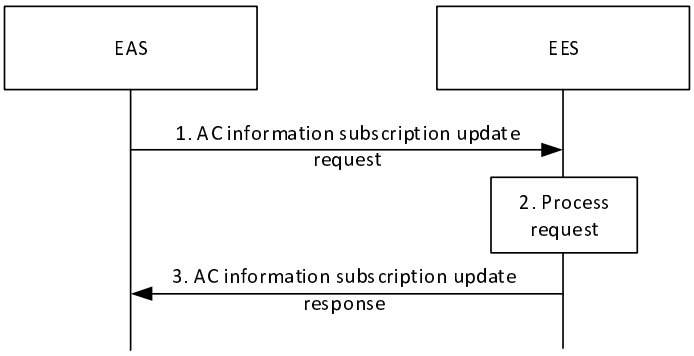

Figure 8.6.4.2.4-1: AC information subscription update

1. The EAS sends an AC information subscription update request to the EES. The request may contain updated filters to retrieve information about particular ACs e.g. AC profile parameters or parameter ranges to be matched, specific UE Identifiers, location ranges, etc.
2. Upon receiving the request from the EAS, the EES performs an authorization check to verify whether the EAS has authorization to perform the operation. If authorized, the EES updates the stored subscription information.

3. The EES sends an AC information subscription update response to the EAS.

8.6.4.2.5 Unsubscribe

Figure 8.6.4.2.5-1 illustrates the AC information unsubscribe procedure between the EAS and the EES.

Pre-conditions:

1. The EAS has subscribed for AC information as described in clause 8.6.4.2.2.

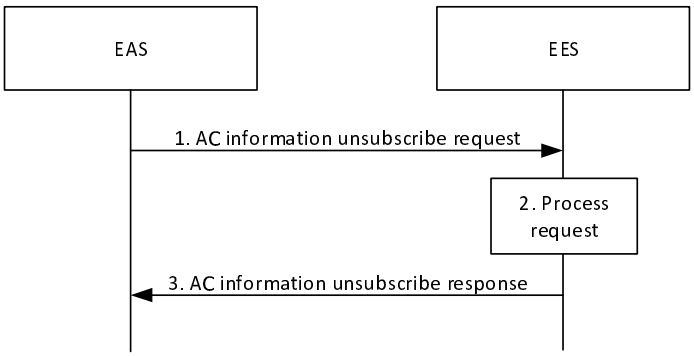

Figure 8.6.4.2.5-1: AC information unsubscribe

1. The EAS sends an AC information unsubscribe request to the EES.
2. Upon receiving the request from the EAS, the EES performs an authorization check to verify whether the EAS has authorization to perform the operation. If authorized, the EES cancels the subscription as requested in step 1.
3. The EES sends an AC information unsubscribe response to the EAS.

8.6.4.3 Information flows

8.6.4.3.1 General

8.6.4.3.2 AC information subscription request

Table 8.6.4.3.2-1 describes the information flow for an AC information subscription request from the EAS to the EES.

Table 8.6.4.3.2-1: AC information subscription request

Information element	Status	Description
EASID	M	The identifier of the EAS
Security credentials	M	Security credentials of the EAS
Subscription type	M	Choice of "One time" or "Event based" determining the type of processing requested
Notification Target Address	M	The Notification Target Address (e.g. URL) where the notifications destined for the EAS should be sent to.
Filters	O	List of characteristics for discovery purposes, as detailed in Table 8.6.4.3.2-2.
Event conditions	O	Parameters indicating notification event conditions e.g. number of notifications instances, subscription timeout, etc.
Trigger parameters	O	Parameters indicating notification triggering conditions e.g. EEC registration, EAS discovery.

Table 8.6.4.3.2-2: Filters

Information element	Status	Description
ACID(s)	O	List of identities of AC(s) to be matched
UE ID(s)	O	List of UE identifiers to be matched
AC Type(s)	O	List of categories or types of ACs (e.g. V2X) to be matched
ECSP ID(s)	O	Identifier(s) for the ECSP associated with the EEC.
Operation Schedule	O	EAS operation schedule (e.g. time windows) to be matched
Geographical Service Area	O	EAS service area for identifying UEs with matching expected geographical location(s) (e.g. route). This geographic information can express a geographic point, polygon, route, signalling map, or waypoint set.
Topological Service Area	O	EAS service area for identifying UEs with matching expected topological location(s). See possible formats in Table 8.2.7-1.
Maximum AC Service KPIs (NOTE)	O	Maximum value for identifying the ACs to be matched. Both Minimum required AC Service KPIs and Expected AC Service KPIs from the AC Profiles provided during registration (Table 8.4.2.3.2-1) and/or discovery subscription (Table 8.5.3.4-1) need to be lower than this value.
Min AC Service KPIs (NOTE)	O	Minimum value for identifying the ACs to be matched. Both Minimum required AC Service KPIs and Expected AC Service KPIs from the AC Profiles provided during registration (Table 8.4.2.3.2-1) and/or discovery subscription (Table 8.5.3.4-1) need to be greater than this value.
UE location(s)	O	List of locations (e.g. routes) of the UE(s) for which the request applies
EAS bundle indication	O	Indicator for identifying ACs which include EAS bundle information in the AC Profile and the EAS bundle includes the requesting EAS. If Bundle ID or EAS bundle requirements filters are not included, the presence of this IE signifies that all ACs which include EAS bundle information in the AC Profile match.
> Bundle ID	O	A bundle ID as described in clause 7.2.10 for identifying ACs with EAS bundle information in the AC Profile and with matching bundle EAS identification information.
> Bundle type	O	Type of the EAS bundle as described in clause 7.2.10
> EAS bundle requirements	O	Bundle requirements (as described in clause 8.2.10) for identifying ACs with EAS bundle information in the AC Profile and with matching bundle requirements.
> Partial EAS bundle determination	O	Indicator for identifying ACs which include EAS bundle information in the AC Profile but for which only an EAS subset has been determined by EES.
NOTE: Maximum and minimum AC Service KPIs values may be provided for any IEs from Table 8.2.3-1.		

8.6.4.3.3 AC information subscription response

Table 8.6.4.3.3-1 describes the information flow for the AC information subscription response from EAS to the EES.

Table 8.6.4.3.3-1: AC information subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.6.4.3.4 AC information notification

Table 8.6.4.3.4-1 describes the information flow for an AC information notification from the EES to the EAS.

Table 8.6.4.3.4-1: AC information notification

Information element	Status	Description
Subscription Identifier	M	Subscription identifier for which the notification is generated.
List of clients	O	List of clients matched based on the given filtering criteria, with elements listed below
>AC Profile(s)	M	Profiles of ACs as described in Table 8.2.2-1.
>UE ID(s)	O	UE identifier for the UE hosting the AC
>UE location(s)	O	UE location for the UE hosting the AC

8.6.4.3.5 AC information subscription update request

Table 8.6.4.3.5-1 describes the information flow for an AC information subscription update request from the EAS to the EES.

Table 8.6.4.3.5-1: AC information subscription update request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription ID	M	Subscription identifier corresponding to the subscription.
Filter	O	List of characteristics for discovery purposes, as detailed in Table 8.6.4.3.2-2.
Event conditions	O	Parameters indicating notification event conditions e.g. number of notifications instances, subscription timeout, etc.
Trigger parameters	O	Parameters indicating notification triggering conditions e.g. EEC registration, EAS discovery.

8.6.4.3.6 AC information subscription update response

Table 8.6.4.3.6-1 describes the information flow for the AC information subscription update response from EAS to the EES.

Table 8.6.4.3.6-1: AC information subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.6.4.3.7 AC information unsubscribe request

Table 8.6.4.3.7-1 describes the information flow for an AC information unsubscribe request from the EAS to the EES.

Table 8.6.4.3.7-1: AC information unsubscribe request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription Identifier	M	Subscription identifier for the corresponding subscription request.

8.6.4.3.8 AC information unsubscribe response

Table 8.6.4.3.8-1 describes the information flow for the AC information unsubscribe response from EAS to the EES.

Table 8.6.4.3.8-1: AC information unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.6.4.4 APIs

8.6.4.4.1 General

Table 8.6.4.4.1-1 illustrates the API for AC information exposure.

Table 8.6.4.4.1-1: Eees_AppClientInformation API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_AppClientInformation	Subscribe	Subscribe/Notify	EAS
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.6.4.4.2 Eees_AppClientInformation_Subscribe operation

API operation name: Eees_AppClientInformation_subscribe

Description: The consumer subscribes to receive an AC information.

Inputs: See clause 8.6.4.3.2.

Outputs: See clause 8.6.4.3.3.

See clause 8.6.4.2.2 for details of usage of this operation.

8.6.4.4.3 Eees_AppClientInformation_Notify operation

API operation name: Eees_AppClientInformation_Notify

Description: The consumer is notified of an event by the EES.

Inputs: See clause 8.6.4.3.4.

Outputs: None.

See clause 8.6.4.2.3 for details of usage of this operation.

8.6.4.4.4 Eees_AppClientInformation_UpdateSubscription operation

API operation name: Eees_AppClientInformation_UpdateSubscription

Description: The consumer updates an existing subscription for AC information.

Inputs: See clause 8.6.4.3.5.

Outputs: See clause 8.6.4.3.6.

See clause 8.6.4.2.4 for details of usage of this operation.

8.6.4.4.5 Eees_AppClientInformation_Unsubscribe operation

API operation name: Eees_AppClientInformation_Unsubscribe

Description: The consumer unsubscribes for the previously subscribed events.

Inputs: See clause 8.6.4.3.7.

Outputs: See clause 8.6.4.3.8.

See clause 8.6.4.2.5 for details of usage of this operation.

8.6.5 UE Identifier API

8.6.5.1 General

EES exposes UE Identifier API to the EAS and EEC in order to provide an identifier uniquely identifying a UE. This API is used by an EAS or EEC to obtain the identifier of the UE if the EAS or EEC does not have it (e.g. hasn't already cached). This identifier, called UE ID and defined in clause 7.2.6, is used by the EAS to invoke capability APIs specific to UEs over EDGE-3 and/or EDGE-7 depending on the UE ID type.

The EAS's direct invocation of the UE Identifier API of the EES may result in UE ID not found response (e.g. if the NATed UE's public IPv4 address can't be resolved by the core network). Under such circumstances, the EAS may choose to signal its AC to trigger the UE ID query onto the EEC over EDGE-5 (see clause 8.14.2.6). In turn, the EEC would invoke the EES's UE Identifier API using the UE's CN assigned IP addresses (i.e. IPv4 and/or IPv6) which should result in return of the UE ID to the EEC and from thereon to the AC and the EAS.

NOTE 1: To overcome CN UE's assigned private IP address reuse issue (e.g. UE's private IPv4 reuse by 5GC), the EES would need to be pre-configured with the public IP address range (used by the NAT function over N6) and its associated IP domain.

NOTE 2: EEC retrieval of the UE's IP address from the device is out of scope.

8.6.5.2 Procedure

Figure 8.6.5.2-1 illustrates the interactions between the EES and the EAS or EEC.

Pre-conditions:

1. The EAS or EEC is authorized to discover and to use UE Identifier API provided by the EES.
2. When the EEC is used to invoke the UE Identifier API with the UE IPv6 address as the input parameter, the UE IPv6 address may or may not be NATed. If NATed however, the IPv6 may not be reused (i.e. assigned to more than one UE simultaneously). If the EEC already has the UE ID (GPSI as per clause 7.2.6), and it needs the Edge UE ID to share with an AC/EAS, this procedure can still be used to retrieve Edge UE ID.

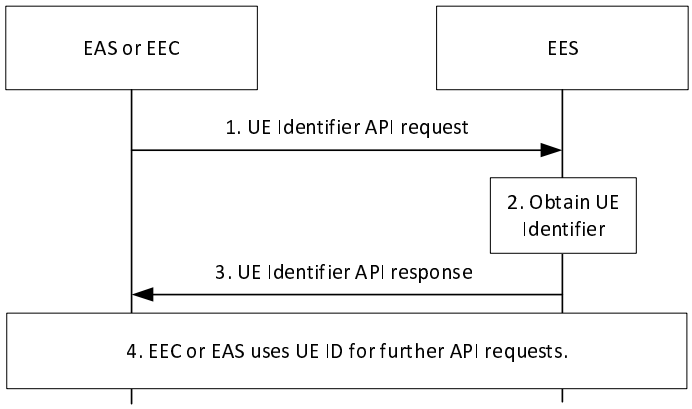

Figure 8.6.5.2-1: UE Identifier API

1. The EAS or EEC invokes UE Identifier API exposed by the EES. If it is the EAS invoking the API and it recognizes that the UE's IP address is a public IP address, i.e., the UE is behind a NAT, the Port Number and associated IP address should be included in user information.

2. The EES uses the received user information in the step 1 (e.g. IP address) and obtains the UE identifier by interacting with NEF as specified in clause 4.15.10 of 3GPP TS 23.502 [3]. If it is the EEC invoking the API with only UE IP address, it shall be interpreted by EES that EEC is requesting the UE ID for interaction with EES (hence EES shall use its own AF Identifier towards NEF and consequently the UE ID is EES specific). When the EES needs to interact with the NEF's Nnef_UEId_Get (see TS 23.502 clause 4.15.10 "AF specific UE ID retrieval") as per EAS request, the EES may use either its own AF Identifier or EASID as AF Identifier instead of its own AF Identifier.

3. The EES provides the UE identifier to the EAS or to EEC (i.e. whichever invoked the API). The UE identifier returned in the response which is referred to as UE ID may be the 3GPP Core Network assigned UE ID (aka AF-specific UE ID; see TS 23.502 clause 4.15.10) or the EES-generated Edge UE ID as defined in clause 7.2.9. If UE ID (GPSI as per clause 7.2.6) is included in the request received from EEC, the EES can provide the Edge UE ID based on the received UE ID and step 2 can be skipped. For EEC requesting the UE ID for interaction with EES, the EES returns its 3GPP Core Network assigned UE ID (aka AF specific UE ID, which is a GPSI in the form of an External ID as per clause 7.2.6) to the EEC.

NOTE 1: User consent aspect on sharing the AF specific UE identifier with particular EAS is described in 3GPP TS 33.558 [23].

4. The EAS uses the UE ID received in step 3 to invoke capability exposure API(s) provided by the EES over EDGE-3 and/or EDGE-7 depending on the UE ID type. The EEC can use the UE ID which is EES specific received in step 3 to invoke API(s) provided by the EES over EDGE-1 reference point.

NOTE 2: UE ID of type CN-assigned can be used over EDGE-1, EDGE-3 and EDGE-7 whereas the UE ID of type EES-generated Edge UE ID can be used over EDGE-3 only.

8.6.5.3 Information flows

8.6.5.3.1 General

The following information flows are specified for UE Identifier API:

- UE Identifier request and response.

8.6.5.3.2 UE Identifier API request

Table 8.6.5.3.2-1: UE Identifier API request

Information element	Status	Description
User information (NOTE 1) (NOTE 3)	O	Information about the User or UE available in the EAS or EEC, e.g. IP address.
UE ID (NOTE 2) (NOTE 3)	O	UE ID in the form of GPSI as per clause 7.2.6.
EAS ID list (NOTE 4)	O	Identifier of the EAS(s) for which the UE IDs are requested for by EAS or EEC given the User information (e.g. IP address).
EAS Provider ID	O	Identifier of the ASP that provides the EAS.
Application Port ID (NOTE 5)	O	Application Port ID, as defined in 3GPP TS 23.502 [3], associated with the EAS.
Security Credentials	M	Security credentials of the EAS or EEC.
NOTE 1: This IE is Mandatory when EAS invoke the UE ID API. When EEC invokes the API, if available, this IE contains both UE's private IPv6 address (due to the existence of NAT66) and UE's private IPv4 address. When EAS invokes the API, it may recognize the UE IP address is a public IP address different from the actual UE IP address (private IP address), i.e., the UE is behind a NAT, and should therefore include the Port Number and associated IP address as part of the User information. NOTE 2: This IE is used when invoked by the EEC and if the EEC have the UE ID already in a form not desired to be shared with the EAS. NOTE 3: At least one of them shall be present. NOTE 4: This IE is Mandatory when EAS invoke the UE ID API. NOTE 5: This IE may only be present when EAS invoke the UE ID API.		

NOTE: It is outside the scope of this release of this specification how to verify the IP address provided in the request and whether the UE-provided IP address is trusted or not.

8.6.5.3.3 UE Identifier API response

Table 8.6.5.3.3-1: UE Identifier API response

Information element	Status	Description
Successful response	O	Indicates that the UE identifier request was successful.
> UE ID list	M	List of all the UE IDs Identifier uniquely identifying the UE(s).
>> UE ID	M	AF-specific UE ID or Edge UE ID
>> UE ID type	M	Indication whether the UE ID is CN assigned AF-specific UE ID or Edge UE ID.
>> EAS ID	O	It is present if the EAS ID was provided in the request (see EAS ID list in Table 8.6.5.3.2-1).
Failure response	O	Indicates that the UE identifier request failed.
> Cause	O	Indicates the cause of UE identifier request failure

8.6.5.4 APIs

8.6.5.4.1 General

Table 8.6.5.4.1-1 illustrates the APIs for UE Identifier.

Table 8.6.5.4.1-1: Eees_UE_Identifier API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_UEIdentifier	Get	Request/Response	EAS, EEC

8.6.5.4.2 Eees_UEIdentifier_Get operation

API operation name: Eees_UEIdentifier_Get

Description: The consumer requests identifier of a UE.

Inputs: See clause 8.6.5.3.2.

Outputs: See clause 8.6.5.3.3.

See clause 8.6.5.2 for details of usage of this operation.

8.6.6 Session with QoS API

8.6.6.1 General

The EES exposes the Session with QoS API to the EAS in order to support the setup of a data session between AC and EAS with a specific QoS and the modification of the QoS of this data session.

The Session with QoS API exposed by the EES relies on the northbound Policy Authorization Service API exposed by the PCF as specified in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [12], if the EES is connected to the PCF via the N5 reference point, or on the northbound AF Session with QoS Service API exposed by the NEF as specified in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [12], if the EES is connected to the PCF via an NEF.

This API supports to apply the required QoS for both ongoing session and future session for a UE or a group of UEs.

The level of support of the Session with QoS API may change due to UE mobility between 5GC and EPC. E.g. QoS monitoring is only applicable in 5GC. If an EES exposes the Session with QoS API to EAS(s) for a UE, the EES monitors such changes and provides the available information to the EAS.

Alternatively to using the API described in the following clauses, the EAS may also act as an AF and directly access the 3GPP Core Network capabilities to request an AF session with QoS (see clause 8.7.2). For any data session between AC and EAS, the EAS shall use only one of these alternatives.

8.6.6.2 Procedures

8.6.6.2.1 General

8.6.6.2.2 Create a session

Figure 8.6.6.2.2-1 illustrates the session with QoS create operation between the EAS and the EES. It is used to request reservation of resources for a data session between AC and EAS with a specific QoS and to subscribe to certain session with QoS event notifications.

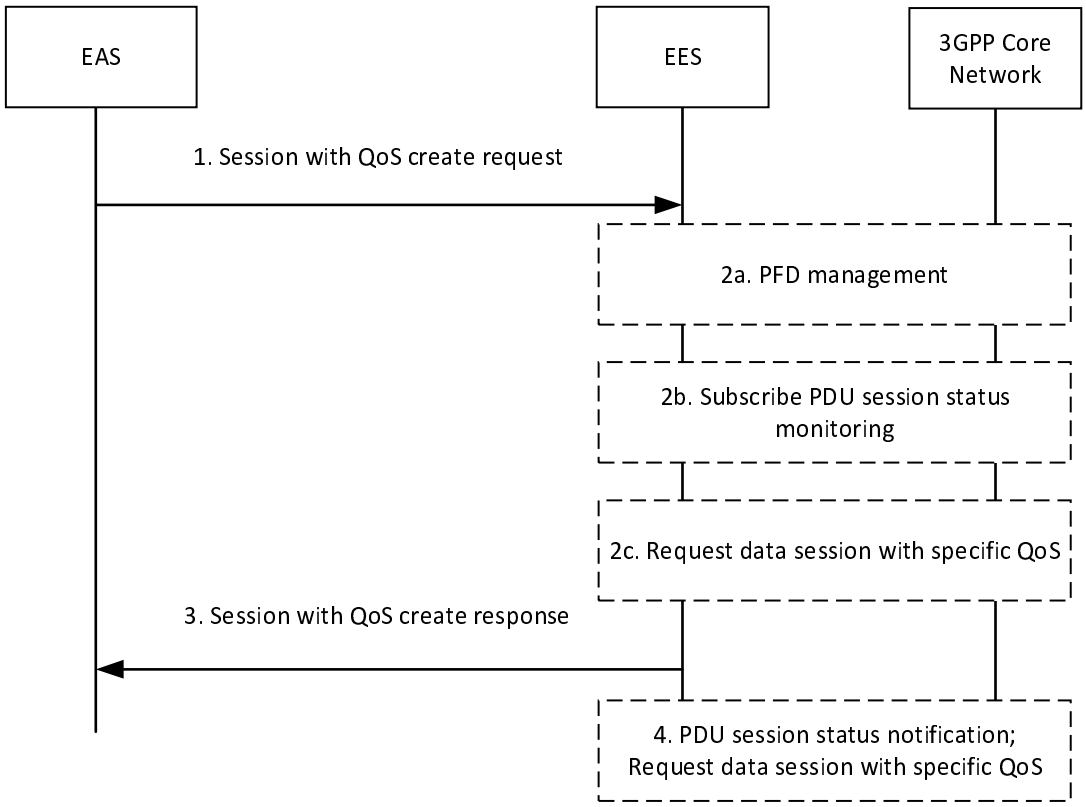

Figure 8.6.6.2.2-1: Session with QoS API: create operation

1. The EAS requests establishment of a data session between the AC and the EAS with a specific QoS (either QoS reference or bandwidth). If the data session can adjust to different QoS parameter combinations, the request may include a list of alternative QoS references in a priority order. The EAS shall include the UE's IP address, UE ID or UE Group ID, the DNN and S-NSSAI used for the data session between AC and EAS. With the same request the EAS subscribes to receive certain session with QoS event notifications (e.g. notifications related to QoS monitoring, usage monitoring for sponsored data connectivity and/or QoS targets can no longer (or can again) be fulfilled).

2. The EES checks if the EAS is authorized for this operation for the UE. If authorized, then the following services of 3GPP CN may be used by the EES:

   a. the EES invokes the PFD management procedure with the 3GPP Core Network as described in 3GPP TS 23.682 [10] and 3GPP TS 23.502 [8] with an application id. At least one of the IP flow description, domain description or URI sent by the EAS is used for requesting PFD management service. Further the EES provides the same application id for requesting data session with specific QoS in step 2c or step 4.

NOTE 1: PFD management can be optionally supported in MNO. If EES cannot invoke step 2a, it responds EAS with appropriate error.

NOTE 2: The EES can map the EASID into the application id that is used to invoke the PFD management procedure.

   b. the EES invokes the Event Monitoring service for PDU session status with the 3GPP Core Network, as described in 3GPP TS 23.502 [3].

   c. the EES invokes the Policy Authorization Create service or the AF Session with QoS service with the 3GPP Core Network (PCF or NEF, respectively) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], providing the specific QoS (QoS reference or bandwidth) to the PCF as described in 3GPP TS 23.503 [12], clause 6.1.3.22. Additionally, the EES may subscribe to notifications of resource allocation outcome and to other events described in clause 6.1.3.18 of 3GPP TS 23.503 [12], e.g. notifications of when the QoS targets can no longer (or can again) be fulfilled.

The usage of step 2b and step 2c is as follows:

- If the request is for a group of UEs identified by the UE Group ID or for a single UE identified by the UE ID, then EES executes step 2b. If UE (single UE or UE group member) already has ongoing PDU session, then UE IP address is retrieved in step 2b. Further the EES executes step 2c; otherwise the EES waits for further notification for PDU session status in step 4.

- If the request is for a single UE identified by the IP address, then EES executes step 2c.

3. If the operation in step 2 is successful, the EES responds with a Context ID and a Result. The Context ID is to be used by the EAS for further requests (e.g. session with QoS update requests) pertaining to the same UE. If the EAS is not authorized or any other failure happens during the operation, the EES provides a rejection response with cause information.

4. When the EES receives the corresponding UE IP address for the single UE or UE group member from the PDU session status notification sent by the 3GPP Core Network, the EES requests data session with specific QoS as described in step 2c.

NOTE 3: The EES will report the resource allocation outcome, e.g. the successful allocation of the Service Data Flow(s) related to the data session, with a separate session with QoS notify operation (see TS 23.503 [12], clause 6.1.3.18).

8.6.6.2.3 Update a session

Figure 8.6.6.2.3-1 illustrates the session with QoS update request operation between the EAS and the EES. It is used to request a modification of the QoS of the data session between AC and EAS.

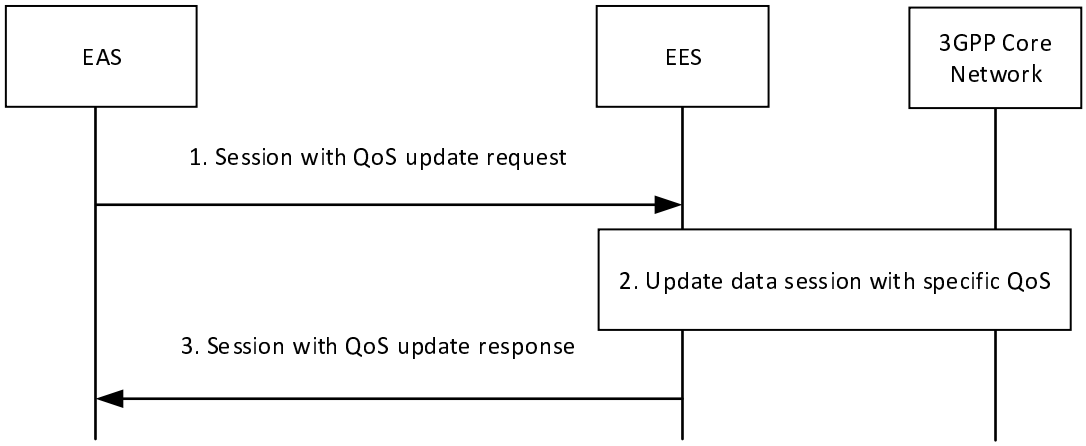

Figure 8.6.6.2.3-1: Session with QoS API: update operation

1. The EAS requests a modification of the QoS of the data session between the AC and the EAS, e.g. by including a different QoS reference or different bandwidth value. The EAS shall include the Context ID.

   The EAS may also request a modification of the event monitoring by subscribing to new events and updating or removing subscriptions to existing events.

2. The EES checks if there is a context for the Context ID available and whether the EAS is authorized for this operation. If yes and the UE IP address is known by the EES, the EES invokes the Policy Authorization Update service or AF Session with QoS Update service with the 3GPP Core Network (PCF or NEF, respectively) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], providing the updated information to the PCF or NEF, respectively. The EES may subscribe to additional events or unsubscribe to certain events, if necessary.

3. If the operation is successful, the EES responds with a Context ID and a Result. If the EAS is not authorized or any other failure happens during the operation, the EES provides a rejection response with cause information.

NOTE: The EES will report the resource allocation outcome, e.g. the successful modification of the Service Data Flow(s) related to the data session, with a separate session with QoS notify operation (see 3GPP TS 23.503 [12], clause 6.1.3.18).

8.6.6.2.4 Revoke a session

Figure 8.6.6.2.4-1 illustrates the session with QoS revoke operation between the EAS and the EES. It is used to revoke the data session between AC and EAS with a specific QoS and to unsubscribe to the related session with QoS event notifications.

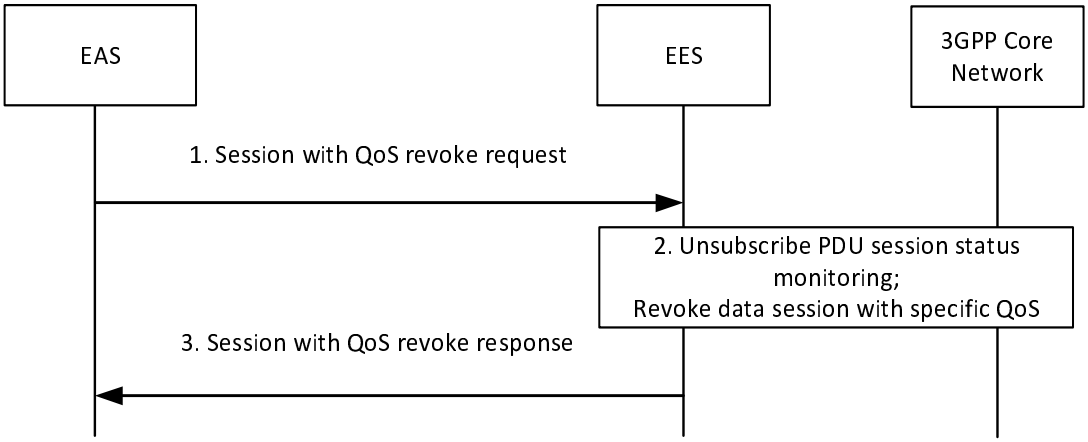

Figure 8.6.6.2.4-1: Session with QoS API: revoke operation

1. The EAS requests a revoke of the data session with QoS between the AC and the EAS. The EAS shall include the Context ID.
2. The EES checks if there is a context for the Context ID available and whether the EAS is authorized for this operation. If yes, then the EES unsubscribes from the PDU session status monitoring (if applicable) and invokes the Policy Authorization Delete service or AF Session with QoS Revoke service with the 3GPP Core Network (PCF or NEF, respectively) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]. This deletes the application session context at the PCF or NEF and removes the subscription to any session with QoS event notifications.
3. If the operation is successful, the EES responds with a Context ID and a Result. If the EAS is not authorized or any other failure happens during the operation, the EES provides a rejection response with cause information.

8.6.6.2.5 Notify

Figure 8.6.6.2.5-1 illustrates the notify operation between the EES and the EAS for session with QoS event notifications.

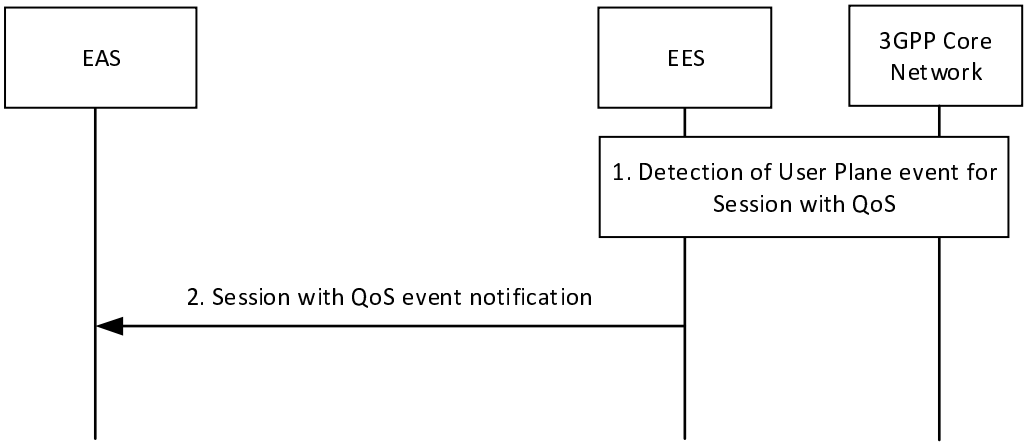

Figure 8.6.6.2.5-1: Session with QoS API: notify operation

1. The EES detects a user plane event associated with the established session (i.e. it receives a Policy Authorization Notify operation from the PCF or an AF Session with QoS Notify operation from the NEF as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]). The EES determines to notify the session with QoS event notification information (e.g., resource allocation outcome or information that the QoS targets can no longer (or can again) be fulfilled) to the EASs which have subscribed to the session with QoS event notification.

2. The EES sends a session with QoS event notification to the EAS. The EES includes the session with QoS event notification information of the UE.

8.6.6.3 Information flows

8.6.6.3.1 General

The following information flows are specified for Session with QoS API:

- Session with QoS create request and response;
- Session with QoS update request and response;
- Session with QoS revoke request and response; and
- Session with QoS event notification.

8.6.6.3.2 Session with QoS create request

Table 8.6.6.3.2-1 describes the information elements for a Session with QoS create request from the EAS to the EES.

Table 8.6.6.3.2-1: Session with QoS create request

Information element	Status	Description
EASID	M	The identifier of the EAS
Security credentials	M	Security credentials of the EAS
UE IP address (NOTE 1)	O	The UE IP address.
UE ID (NOTE 1)	O	The identifier of the UE (i.e. GPSI)
UE Group ID (NOTE 1)	O	Identifies a group of UEs as defined in clause 7.2.7
IP flow description (NOTE 4)	O	The IP flow description for the application traffic.
Domain description (NOTE 4)	O	The domain description including domain name, applicable protocol and matching criteria (e.g. TLS SNI).
URI (NOTE 4)	O	Uniform resource identifier. It represents the application traffic URI.
Requested QoS reference (NOTE 2)	O	Refers to pre-defined QoS information for the data session between AC and EAS (NOTE 3).
List of alternative QoS references	O	A list of alternative QoS references, referring to pre-defined QoS information for the data session between AC and EAS and containing one or more QoS reference parameters in a prioritized order (NOTE 3).
Event list	O	A list of associated events to which the EAS subscribes (see 3GPP TS 23.503 [12], clause 6.1.3.18).
> Event specific data	O	For usage monitoring: the sponsoring information (sponsor id, ASP id). For QoS monitoring: Target of monitoring (DL, UL or roundtrip packet delay).
> Frequency of reporting	O	The reporting frequency (e.g. event triggered) and additional related data (e.g. threshold, minimum waiting time) as described in clause 6.1.3.21 of 3GPP TS 23.503 [12], applicable for QoS monitoring event.
Notification Target Address	M	The Notification Target Address (e.g. URL) where the notifications destined for the EAS should be sent to.
DNN	O	DNN for the data session between AC and EAS
S-NSSAI	O	S-NSSAI for the data session between AC and EAS
Requested bandwidth (NOTE 2)	O	Bandwidth requested for the data session between AC and EAS
NOTE 1: Only one of UE IP address, UE ID or UE Group ID shall be provided. NOTE 2: Only one of requested QoS reference or requested bandwidth shall be provided. NOTE 3: The pre-defined QoS information may be configured in the EES or in the 3GPP Core Network (see 3GPP TS 23.503 [12], clause 6.1.3.22). NOTE 4: At least one of these information elements shall be present.		

8.6.6.3.3 Session with QoS create response

Table 8.6.6.3.3-1 describes the information elements for a Session with QoS create response from the EES to the EAS.

Table 8.6.6.3.3-1: Session with QoS create response

Information element	Status	Description
Successful response	O	Indicates that the Session with QoS create request was successful.
> Context ID	M	Context identifier corresponding to the information stored for the request in the EES
Failure response	O	Indicates that the Session with QoS create request failed.
> Cause	O	Indicates the cause of Session with QoS create request failure

8.6.6.3.4 Session with QoS update request

Table 8.6.6.3.4-1 describes the information elements for a Session with QoS update request from the EAS to the EES.

Table 8.6.6.3.4-1: Session with QoS update request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Context ID	M	Context identifier corresponding to the information stored for the request in the EES.
Requested QoS reference (NOTE 1)	O	Refers to pre-defined QoS information for the data session between AC and EAS (NOTE 2).
List of alternative QoS references	O	A list of alternative QoS references, referring to pre-defined QoS information for the data session between AC and EAS and containing one or more QoS reference parameters in a prioritized order (NOTE 2).
Event list	O	A list of associated events to which the EAS subscribes (see 3GPP TS 23.503 [12], clause 6.1.3.18).
> Event specific data	O	For usage monitoring: the sponsoring information (sponsor id, ASP id). For QoS monitoring: Target of monitoring (DL, UL or roundtrip packet delay).
> Frequency of reporting	O	The reporting frequency (e.g. event triggered) and additional related data (e.g. threshold, minimum waiting time) as described in clause 6.1.3.21 of 3GPP TS 23.503 [12], applicable for QoS monitoring event.
Requested bandwidth (NOTE 1)	O	Bandwidth requested for the data session between AC and EAS
NOTE 1: Only one of requested QoS reference or requested bandwidth shall be provided. NOTE 2: The pre-defined QoS information may be configured in the EES or in the 3GPP Core Network (see 3GPP TS 23.503 [12], clause 6.1.3.22).		

8.6.6.3.5 Session with QoS update response

Table 8.6.6.3.5-1 describes the information elements for a Session with QoS update response from the EES to the EAS.

Table 8.6.6.3.5-1: Session with QoS update response

Information element	Status	Description
Successful response	O	Indicates that the Session with QoS update request was successful.
Failure response	O	Indicates that the Session with QoS update request failed.
> Cause	O	Indicates the cause of Session with QoS update request failure

8.6.6.3.6 Session with QoS revoke request

Table 8.6.6.3.6-1 describes the information elements for a Session with QoS revoke request from the EAS to the EES.

Table 8.6.6.3.6-1: Session with QoS event API revoke request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Context ID	M	Context identifier corresponding to the information stored for the request in the EES

8.6.6.3.7 Session with QoS revoke response

Table 8.6.6.3.7-1 describes the information elements for a Session with QoS revoke response from the EES to the EAS.

Table 8.6.6.3.7-1: Session with QoS revoke response

Information element	Status	Description
Successful response	O	Indicates that the Session with QoS revoke request was successful.
Failure response	O	Indicates that the Session with QoS revoke request failed.
> Cause	O	Indicates the cause of Session with QoS revoke request failure

8.6.6.3.8 Session with QoS event notification

Table 8.6.6.3.8-1 describes the information elements for a Session with QoS event notification from the EES to the EAS.

Table 8.6.6.3.8-1: Session with QoS event notification

Information element	Status	Description
Context ID	M	Context identifier corresponding to the information stored in the EES during the initial session with QoS create request.
Event report (NOTE)	M	Event reporting information as specified in clause 6.1.3.18 of 3GPP TS 23.503 [12].
NOTE: Only the following events are applicable: - Reporting Usage for Sponsored Data Connectivity - Service Data Flow deactivation - Resource allocation outcome - QoS targets can no longer (or can again) be fulfilled - QoS Monitoring parameters		

8.6.6.4 APIs

8.6.6.4.1 General

Table 8.6.6.4.1-1 illustrates the API for Session with QoS.

Table 8.6.6.4.1-1: Eees_SessionWithQoS API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_SessionWithQoS	Create	Request/Response	EAS
	Update		
	Revoke		
	Notify	Subscribe/Notify (NOTE)	EAS
NOTE: The Subscribe operation is embedded in the Request operation of the Create and Update API operation.			

8.6.6.4.2 Eees_SessionWithQoS_Create operation

API operation name: Eees_SessionWithQoS_Create

Description: The consumer requests a data session with the UE with a specific QoS and may also subscribe to certain event notifications related to the user plane traffic.

Inputs: See clause 8.6.6.3.2.

Outputs: See clause 8.6.6.3.3.

See clause 8.6.6.2.2 for details of usage of this operation.

8.6.6.4.3 Eees_SessionWithQoS_Update operation

API operation name: Eees_SessionWithQoS_Update

Description: The consumer requests a modification of the QoS of the data session with the UE and may also update event notifications related to the user plane traffic.

Inputs: See clause 8.6.6.3.4.

Outputs: See clause 8.6.6.3.5.

See clause 8.6.6.2.3 for details of usage of this operation.

8.6.6.4.4 Eees_SessionWithQoS_Revoke operation

API operation name: Eees_SessionWithQoS_Revoke

Description: The consumer requests a revoke of the data session with QoS with the UE and unsubscribes to all related event notifications.

Inputs: See clause 8.6.6.3.6.

Outputs: See clause 8.6.6.3.7.

See clause 8.6.6.2.4 for details of usage of this operation.

8.6.6.4.5 Eees_SessionWithQoS_Notify operation

API operation name: Eees_SessionWithQoS_Notify

Description: The consumer is notified by the EES of an event related to the user plane traffic.

Inputs: See clause 8.6.6.3.8.

Outputs: None.

See clause 8.6.6.2.5 for details of usage of this operation.

8.6.7 Application traffic influence trigger from EAS

8.6.7.1 General

An EAS can explicitly request EES to influence the EAS traffic from UE(s) with necessary information. Then the EES can trigger the AF request to influence traffic routing towards the 3GPP CN for one or more UE(s) accessing the EAS.

8.6.7.2 Procedure

8.6.7.2.1 Procedure of application traffic influence trigger from EAS

Figure 8.6.7.2.1-1 illustrates the procedure of application traffic influence trigger from EAS.

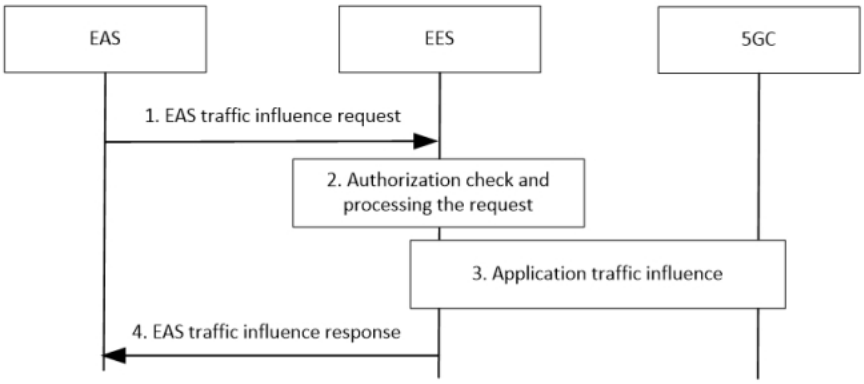

Figure 8.6.7.2.1-1: Application traffic influence trigger from EAS

1. The EAS sends an EAS traffic influence request.
2. The EES performs an authorization check to verify whether the EAS has the authorization to request application traffic influence.
3. Upon successful authorization, the EES includes transaction ID, target DNAI, traffic descriptor information and N6 routing information at target DNAI in the Nnef_TrafficInfluence_Create Request to the NEF, or Npcf_PolicyAuthorization_Create Request to the PCF, to influence the traffic for EAS as described in 3GPP TS 23.501, clause 5.6.7.1.
4. The EES sends the EAS traffic influence response.

8.6.7.2.2 Procedure of application traffic influence update trigger from EAS

Figure 8.6.7.2.2-1 illustrates the procedure of application traffic influence update trigger from EAS.

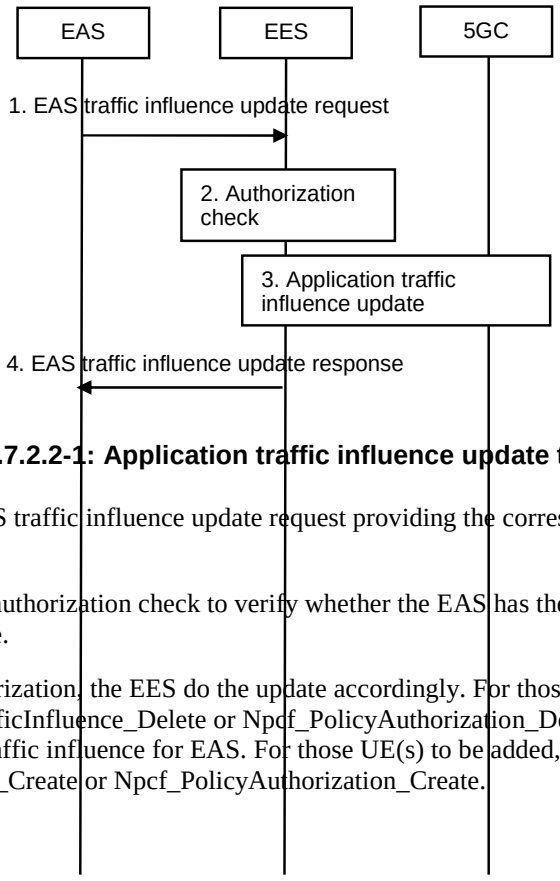

Figure 8.6.7.2.2-1: Application traffic influence update trigger from EAS

1. The EAS sends an EAS traffic influence update request providing the corresponding transaction ID, and updated target UE Identifier(s).
2. The EES performs an authorization check to verify whether the EAS has the authorization to request application traffic influence update.
3. Upon successful authorization, the EES do the update accordingly. For those UE(s) to be deleted, the EES invokes the Nnef_TrafficInfluence_Delete or Npcf_PolicyAuthorization_Delete Request to delete the original request to delete the traffic influence for EAS. For those UE(s) to be added, the EES invokes the Nnef_TrafficInfluence_Create or Npcf_PolicyAuthorization_Create.

4. The EES sends the EAS traffic influence update response.

8.6.7.2.3 Procedure of application traffic influence cancellation trigger from EAS

Figure 8.6.7.2.3-1 illustrates the procedure of application traffic influence cancellation trigger from EAS.

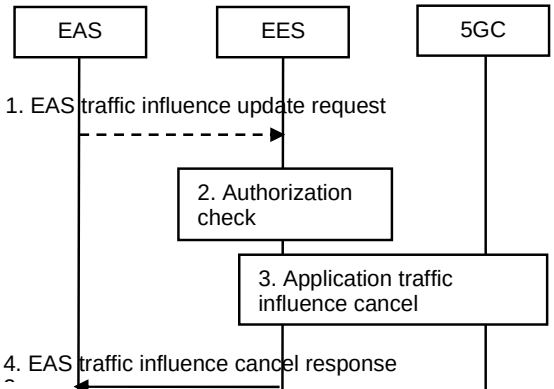

Figure 8.6.7.2.3-1: Application traffic influence cancellation trigger from EAS

1. The EAS sends an EAS traffic influence cancellation request providing the corresponding transaction ID.
2. The EES performs an authorization check to verify whether the EAS has the authorization to request application traffic influence cancellation.
3. Upon successful authorization, the EES includes transaction ID in the Nnef_TrafficInfluence_Delete Request to the NEF, or Npcf_PolicyAuthorization_Delete Request to the PCF, to delete the traffic influence for EAS as described in 3GPP TS 23.501, clause 5.6.7.1.
4. The EES sends the EAS traffic influence cancellation response.

8.6.7.3 Information flows

8.6.7.3.1 General

The following information flows are specified for application traffic influence trigger from EAS:

- Application traffic influence trigger from EAS request and response.
- Application traffic influence update trigger from EAS request and response.
- Application traffic influence cancellation trigger from EAS request and response.

8.6.7.3.2 Application traffic influence trigger from EAS request

Table 8.6.7.3.2-1: application traffic influence trigger from EAS request

Information element	Status	Description
EASID	M	Identifier of the EAS
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Target UE Identifier(s)	M	Indicates the target UE(s) or any UE.

8.6.7.3.3 Application traffic influence trigger from EAS response

Table 8.6.7.3.3-1: application traffic influence trigger from EAS response

Information element	Status	Description
Successful response	O	Indicates that the traffic influence request was successful.
>Transaction ID	M	Identifier of the traffic influence transaction used.
Failure response	O	Indicates that the traffic influence request has failed.
> Cause	O	Indicates the cause of failure

8.6.7.3.4 Application traffic influence update trigger from EAS request

Table 8.6.7.3.4-1: application traffic influence update trigger from EAS request

Information element	Status	Description
EASID	M	Identifier of the EAS
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Updated target UE Identifier(s)	M	Indicates the updated target UE(s) or any UE.
Transaction ID	M	Indicates the target transaction that is to be updated.

8.6.7.3.5 Application traffic influence update trigger from EAS response

Table 8.6.7.3.5-1: application traffic influence update trigger from EAS response

Information element	Status	Description
Successful response	O	Indicates that the traffic influence request was successful.
Failure response	O	Indicates that the traffic influence request has failed.
> Cause	O	Indicates the cause of failure

8.6.7.3.6 Application traffic influence cancellation trigger from EAS request

Table 8.6.7.3.6-1: application traffic influence cancellation trigger from EAS request

Information element	Status	Description
EASID	M	Identifier of the EAS
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Transaction ID	M	Indicates the target transaction that is to be updated.

8.6.7.3.7 Application traffic influence cancellation trigger from EAS response

Table 8.6.7.3.7-1: application traffic influence cancellation trigger from EAS response

Information element	Status	Description
Successful response	O	Indicates that the traffic influence request was successful.
Failure response	O	Indicates that the traffic influence request has failed.
> Cause	O	Indicates the cause of failure

8.6.7.4 APIs

8.6.7.4.1 General

Table 8.6.7.4.1-1 illustrates the APIs for application traffic influence trigger from EAS.

Table 8.6.7.4.1-1: Eees_TrafficInfluenceEAS API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_TrafficInfluenceEAS	Create	Request/Response	EAS
	Update	Request/Response	EAS
	Cancellation	Request/Response	EAS

8.6.7.4.2 Eees_TrafficInfluenceEAS_Create operation

API operation name: Eees_TrafficInfluenceEAS_Create

Description: The consumer requests traffic influence for EAS via EES.

Inputs: See clause 8.6.7.3.2.

Outputs: See clause 8.6.7.3.3.

See clause 8.6.7.2.1 for details of usage of this operation.

8.6.7.4.3 Eees_TrafficInfluenceEAS_Update operation

API operation name: Eees_TrafficInfluenceEAS_Update

Description: The consumer requests to update traffic influence for EAS via EES.

Inputs: See clause 8.6.7.3.4.

Outputs: See clause 8.6.7.3.5.

See clause 8.6.7.2.2 for details of usage of this operation.

8.6.7.4.4 Eees_TrafficInfluenceEAS_Cancellation operation

API operation name: Eees_TrafficInfluenceEAS_Cancellation

Description: The consumer requests to cancel traffic influence for EAS via EES.

Inputs: See clause 8.6.7.3.6

Outputs: See clause 8.6.7.3.7

See clause 8.6.7.2.3 for details of usage of this operation.

8.7 Network capability exposure to EAS

8.7.1 General

The network capability exposure to EAS(s) depends on the deployment scenarios and the business relationship of the ASP/ECSP with the PLMN operator. The following mechanisms are supported:

- Direct network capability exposure.
- Network capability exposure via EES.

8.7.2 Direct network capability exposure

The EAS(s) (acting as trusted or untrusted AF) may directly access the 3GPP Core Network capabilities as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.682 [17].

NOTE: An EAS may use its EASID, clause 7.2.4, as the AF Identifier, 3GPP TS 23.502 [3] when invoking the capabilities of the 3GPP Core Network.

8.7.3 Network capability exposure via EES

The EES may re-expose the network capabilities of the 3GPP core network to the EAS(s) as per the CAPIF architecture specified in 3GPP TS 23.222 [6].

Depending on the deployment models (centralized or distributed) employed,

- the EES assumes the role of the API exposing function (may also acts as the API topology hiding entry) as described in 3GPP TS 23.222 [6]; and
- the EAS assumes the role of an API invoker.

If CAPIF is supported, the EAS interacts with the CAPIF core function and the EES. The EES may further interact with 3GPP northbound service API provider (e.g. SCEF/NEF/SCEF+NEF) or directly with 3GPP core network entities (e.g. PCF) to satisfy the service API invocation requests from the EASs.

The EES may expose the network capabilities of the 3GPP Core Networks to the EAS(s) by supporting the functionalities of 3GPP northbound service API provider (e.g. SCEF, NEF, SCEF+NEF).

NOTE 1: Details of how to select a proper 3GPP network exposure function (e.g. selecting NEF, SCEF, or SCEF+NEF) for the UE(s) is outside scope of this specification.

NOTE 2: When interacting with the 3GPP northbound service provider, the EES acting as an Application Function (AF) of the 3GPP CN (3GPP TS 23.503 [12]) may use its EESID (as described in clause 7.2.3) as the AF Identifier (3GPP TS 23.502 [3]) for API invocations. Alternatively, the EES can use the EASID (as described in clause 7.2.4) of the EAS for which it is re-exposing the 3GPP core network capabilities as the AF Identifier.

8.8 Service continuity

8.8.1 General

8.8.1.1 High level overview

When a UE moves to a new location, different EASs can be more suitable for serving the ACs in the UE. Such transitions can result from a non-mobility event also, requiring support from the enabling layer to maintain the continuity of the service.

This clause describes the features that support service continuity for ACs in the UE to minimize service interruption while replacing the S-EAS, with a T-EAS.

Generally, one AC on the UE has one associated application context at the S-EAS. To support service continuity, this application context is transferred from the S-EAS to a T-EAS.

The capabilities for supporting service continuity provided at the Edge Enabler Layer may consider various application layer scenarios in which there may be involvement of AC and one or more EAS(s).

Following intra-EDN, inter-EDN, between EDN and Cloud, and LADN (overlapping LADN service areas) related scenarios are supported for service continuity:

- UE mobility, including predictive or expected UE mobility;
- Overload situations in S-EAS or EDN; and

- Maintenance aspects such as graceful shutdown of an EAS.

NOTE 1: The scenarios which require ACR for service continuity, cannot use non-overlapping LADNs.

NOTE 2: Overload situations in S-EAS or EDN can be captured based on edge load analytics via utilizing SEAL ADAE capability (see clauses 6.7 and 8.8 of TS 23.436 [28]), which provide statistics or predictions on the expected load of S-EAS or EDN.

NOTE 3: The ACR between EDN and the Cloud may be triggered if no suitable target EAS is found.

To support the need of ACR, following entity roles are identified:

- detection entity, detecting or predicting the need of ACR;
- decision-making entity, deciding that the ACR is required; and
- execution entity, executing ACR.

A detection entity detects the probable need for ACR by monitoring various aspects, such as UE's location or predicted/expected UE location and indicates to the decision-making entity to determine if the ACR is required. The EEC, EES and EAS can potentially perform the detection role:

A decision-making entity determines that ACR is required and instructs the execution entity to perform ACR. The decision-making entity makes a ACR decision to start the ACR execution. In different scenarios of ACR in 8.8.2, the EEC, EAS, EES can potentially perform the decision role respectively.

An execution entity performs ACR as and when instructed by the decision-making entity. ACR execution starts with T-EAS discovery, which can be triggered by EEC, EAS and EES.

NOTE 3: After a decision that another EAS is to serve the UE, the S-EAS can decide if the existing Application Context is transferred to the new EAS.

The EAS may utilize the following capabilities provided by the EES for supporting service continuity at the application layer:

- Subscribe to service continuity related events and receive corresponding notifications;
- Discover the T-EAS; and
- ACR from a S-EAS to a T-EAS.

The EES can utilize the following capabilities provided by the ECS for supporting service continuity at the application layer:

- Retrieve the T-EES.

The EEC may determine if the ACR is required by detecting that the UE moved or is predicted or expected to move outside the service area (see clause 7.3.3). The service area can be provided to the EEC by either the ECS during Service Provisioning or EES during EAS Discovery. For the PDU Session of SSC mode 3, if the UE receives PDU Session Modification Command as specified in clause 4.3.5.2 of 3GPP TS 23.502 [3], the EEC may determine that the ACR is required. For IPv6 multi-homed PDU Session of SSC mode 3, the EEC may determine that ACR is required if the UE is notified of the existence and availability of a new IPv6 prefix as specified in clause 4.3.5.3 of 3GPP TS 23.502 [3].

NOTE 4: For IPv6 multi-homed PDU Session of SSC mode 3, the EEC can be aware of the notification about the IPv6 prefix configuration due to change of PSA UPF based on the UE implementation.

After successful ACR:

- The EES is informed of the completion by the EAS; and
- The EEC is informed of the completion by the EES.

In general, a number of steps are required in order to perform ACR. The potential roles of an edge enablement layer in ACR include:

- providing detection events;

- selecting the T-EAS(s); and
- supporting the transfer of the application context from the S-EAS(s) to the T-EAS(s).

If the UE is connected to the 5GC, the EES/EAS acting as AF may utilize AF traffic influence functionality from the 3GPP CN as specified in 3GPP TS 23.502 [3].

A high level overview of ACR is illustrated in Figure 8.8.1.1-1.

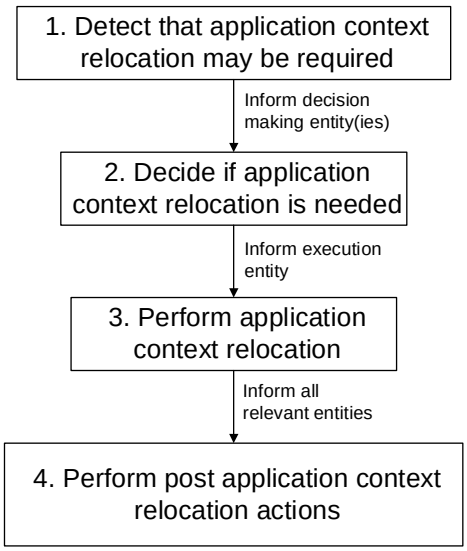

Figure 8.8.1.1-1: High level overview of ACR

ACR can be performed for service continuity planning, which means that the first three steps in Figure 8.8.1.1-1 detection, decision and execution, are performed as defined in clause 8.8.1.2, e.g. when the UE is predicted to move outside the service area of the serving EAS. In such a case the T-EAS is to service the UE when it moves to the expected location.

EES can handle multiple ACR requests simultaneously. When there are multiple simultaneous ACR, the ACR shall be uniquely identified by ACID, EEC ID (or UE ID), S-EAS endpoint and T-EAS endpoint.

8.8.1.2 ACR with service continuity planning

Service continuity planning is an Edge Enabler Layer value-add feature of providing support for seamless service continuity, when information about planned, projected, or anticipated behaviour is available at EESs or provided by EECs.

To implement this functionality an EES may utilize:

- information provided by the EEC e.g., AC Schedule, Expected AC Geographical Service Area, Expected AC Service KPIs, Preferred ECSP list; and
- 3GPP core network capabilities utilized by EES as described in clause 8.10.3.

In service continuity planning, the Application Context may be duplicated and sent from the S-EAS to the T-EAS before the UE moves to the expected location. In this case, the Application Contexts in S-EAS and T-EAS are synchronized when the Application Context is updated until the AC connects to the T-EAS.

NOTE 1: The information elements of the Application Context and how the Application Context is synchronized between the S-EAS and the T-EAS is up to implementation of the application.

NOTE 2: In the case of EELManagedACR, the Application Context synchronization is accomplished using the same mechanism as when transferring the context from the S-EES to the T-EES.

For additional details on service continuity planning for ACR, see clauses 8.8.2.2, 8.8.2.3, 8.8.2.4, 8.8.2.5 and 8.8.2.6.

8.8.1.3 Unused contexts handling during ACR including service continuity planning

The interval between ACT initiation and ACR status update message from EAS to EES (i.e. taking the context into use) can be significant (e.g. in the predicted case). During this interval, the following events are possible:

a) The UE remains communicating with the S-EAS, e.g. the UE does not move to the service area of the T-EAS; or

b) The UE moves to a service area served by a different T-EAS (other than the T-EAS towards which the ACR was initiated).

For the ACRs initiated by the EEC, in case of events a) and b) the EEC should re-send an ACR request with the information of the current ACR and the updated information as described in clause 8.8.3.4 and defined in clause 8.8.4.4. For a) if the action is initiation the EEC sets T-EAS endpoint under ACR initiation action to indicate the S-EAS. For b) if the action is initiation the UE sets T-EAS endpoint under ACR initiation action to the new T-EAS.

NOTE: Timeouts if required for discarding unused contexts for ACR scenarios can be specified in stage 3.

8.8.1.4 Modification of ACR parameters during ACR for service continuity planning

During an ACR for service continuity planning, the circumstances can change which results in the changes in the parameters related to ACR. In such cases modification of the ACR will be required. For example, the EEC or EES can monitor the UE’s mobility and obtain updates in the predicted location or other ACR parameters e.g. prediction expiration time.

For ACRs initiated by the S-EES, the S-EES may detect a change of the expected UE behaviour. In particular, S-EES acting as AF, may receive a UE location report or a monitoring event report from 5GC (assuming that S-EES has subscribed to consume 5GC services like LCS or NEF monitoring events related to UE actual location, or UE mobility analytics from NWDAF). In case of a change in ACR parameters, e.g. prediction expiration time, the S-EES performs ACR parameter information procedure as described in clause 8.8.3.9 to send the updated parameters to T-EES and T-EAS

For the ACRs initiated by the EEC, the EEC/AC may detect a change of the expected UE location. For example, EEC may detect the UE location update as a result of a UE mobility event or obtain an indication from the AC that the expected UE location or UE mobility or both are changed. In this case, in case of a change in ACR parameters, e.g. prediction expiration time, the EEC launches ACR with action "ACR modification" with the information identifying the current ACR and the updated parameters as described in clause 8.8.3.4 and defined in clause 8.8.4.4. If the request is to the S-EES, the S-EES performs ACR parameter information procedure as described in clause 8.8.3.9 to send the updated parameters to T-EES and T-EAS.

If the ACR modification requires the change of T-EAS, this case is described in clause 8.8.1.3.

8.8.1.5 Service continuity between CAS and EAS

Service continuity between CAS and EAS can be supported with CES or without CES, corresponding to the architecture options described in clause 6.2d and 6.2c.

ACR scenarios between CAS and EAS are described in clause 8.8.2A and clause 8.8.2B.

8.8.1.6 Service continuity for EAS bundle

This clause describes solution of relocating EASs in a bundle together instead of individual relocation for AC-EAS sessions one by one. To avoid ACR being triggered for each EAS in a bundle with different initiators (e.g. EAS 1 and EAS 2 in a bundle trigger ACR simultaneously), a main EAS may be used and a main EES is used correspondingly. The main EAS or EES is responsible for ACR detection and initiation in the network side. The main EAS information is sent to EEL and the main EES is the EES registering the main EAS.

NOTE 1: ASP can have requirement of the dependencies between bundled EAS(s) when provisioning them for any deployment scenario, and indicate whether the affinity between them as strong (co-deployment is essential) or weak (co-deployment is only "nice to have").

NOTE 2: It is possible that some EASs in a bundle do not need relocation because the UE can still be served by these EASs. A deployment example is both EASs providing services covering the whole city and EASs providing services covering city district are serving the AC as an EAS bundle, and when UE moves from one district to another district in the city, only EASs serving the district from where UE is moving out need relocation.

NOTE 3: In the proxy type of bundle, the main EAS is the connecting EAS serving the AC.

NOTE 4: In current release of the specification, the main EAS is selected by ASP.

8.8.2 Scenarios

8.8.2.1 General

ACR functionality can be implemented flexibly, and may be focused either in the EEC or in the EAS/EES. The scenarios in this clause are different with regards to

a) whether the EEC is involved in the detection phase and decision phase or detection and decision involve the S-EAS or S-EES only;

b) whether T-EAS discovery is performed between EEC and T-EES or between S-EES and T-EES;

c) whether the EEC sends an Application Context Relocation Request towards the S-EES, the T-EES or none at all; and

d) whether the Application Context is pushed from the S-EAS to the T-EAS or pulled by the T-EAS from S-EAS.

Generally, AC, EEC, EES and EAS implementations will support only a subset of these scenarios; therefore, during EAS discovery and T-EAS discovery the S-EES and T-EES shall take the ACR scenarios supported by the AC and EEC and any preferences indicated by the EEC for specific ACR scenarios into account when identifying the EAS(s) for the EAS discovery response, as specified in clause 8.5.2.2 and clause 8.8.3.2, or for the EAS discovery notification, as specified in clause 8.5.2.3.3.

Furthermore, when the EEC performs EAS discovery or T-EAS discovery, the EES or T-EES shall inform the EEC about the ACR scenarios which are supported by the EAS or T-EAS, respectively.

The EEC shall take the information about supported ACR scenarios provided by the ECS, S-EES and T-EES into account when selecting an EES for EAS discovery or T-EAS discovery, respectively, and when selecting an EAS for edge services.

For clarity of description, scenarios in clauses 8.8.2.2, 8.8.2.3, 8.8.2.4, 8.8.2.5 and 8.8.2.6 describe the relocation of a single application context to a new EAS. Multiple ACs can be active in the UE and relocation can be executed for each AC (or group of ACs) that requires service continuity.

For each of the scenarios in clauses 8.8.2.2, 8.8.2.3, 8.8.2.4, 8.8.2.5 and 8.8.2.6, ACR for one or more ACs can result in the same EEC receiving services from more than one EES, which have the registration for the required EASs that can serve the ACs. In scenarios described in clause 8.8.2.4 and clause 8.8.2.5, a successful EEC context relocation procedure enables the EEC to become implicitly registered to the target EES without the EEC sending an EEC registration request.

If selected ACR scenario list exists, the ACR scenarios are initiated based on this list.

8.8.2.2 Initiation by EEC using regular EAS Discovery

In this scenario, ACR is a result of the UE moving to, or the UE expecting to move to, a new location which is outside the service area of the serving EAS. The EEC is triggered as a result of the UE's movement as described in 8.8.1.1 or by an AC as described in clause 8.14.2.4.

This scenario is based on Service Provisioning (as specified in clause 8.3) and EAS Discovery (as specified in clause 8.5) procedures to discover the T-EES and EAS that shall serve the AC as a result of the UE's new location, and that shall receive the Application Context from the serving EAS.

This scenario relies on the EDGE-5 interface between the EEC and AC.

Pre-conditions:

1. The AC in the UE already has a connection to a corresponding S-EAS;
2. The preconditions listed in clause 8.3.3.2.2 with regards to the EEC are fulfilled; and
3. The EEC is triggered when it obtains the UE's new location or is triggered by another entity such as an ECS notification or AC trigger.

NOTE 1: This scenario is applicable only for an Edge-aware AC and EAS.

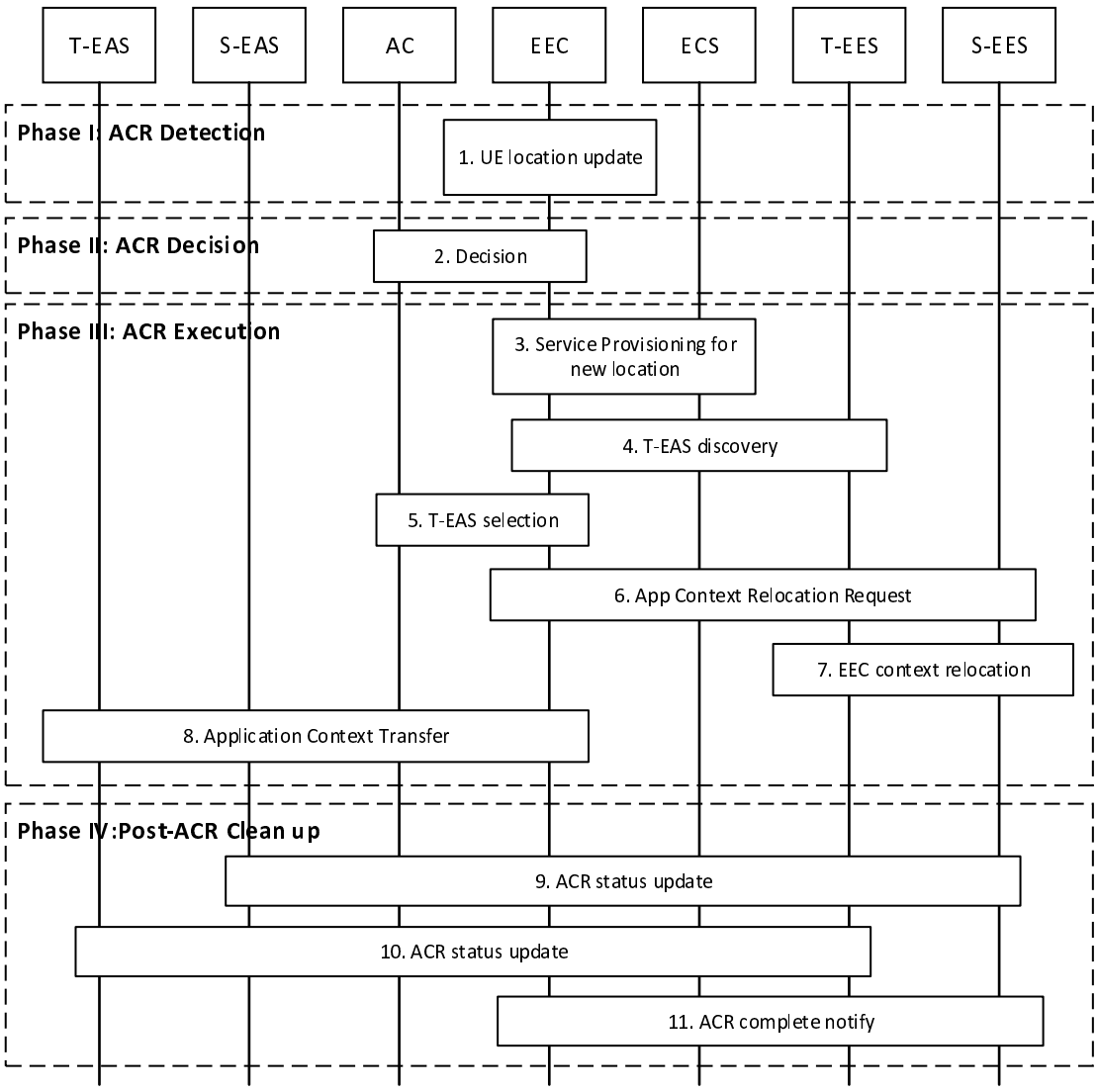

Figure 8.8.2.2-1: ACR initiated by the EEC and AC

Phase I: ACR Detection

1. The EEC detects the UE location update as a result of a UE mobility event and is provided with the UE's new location as described in clause 8.8.1.1. The EEC can also detect an expected or predicted UE location in the future as described in clause 8.8.1.1.

NOTE 2: If the EEC is triggered by an external entity such as by a notification from the ECS, a list of new EESs (to be used as T-EESs) is provided by that notification and step 3 below is skipped.

Phase II: ACR Decision

2. Either the AC or the EEC makes the decision to perform the ACR. If the EEC has received information of on-going ACR, then it should not initiate an ACR with the same ACR identity uniquely identified by ACID, EEC ID (or UE ID), S-EAS endpoint and T-EAS endpoint again per clause 8.8.3.5.3.

NOTE 3: Which applications require ACR can be decided based on the application profile, e.g. requirement of service continuity of the application.

If the change in UE's location does not trigger a need to change the serving EAS, steps 3 onwards are skipped. The EEC remains connected to the serving EES(s) and the AC remains connected to its corresponding serving EAS.

Phase III: ACR Execution

3. The EEC performs Service Provisioning (as specified in clause 8.3) for all active applications that require ACR. Since the location of the UE has changed, the Service Provisioning procedure results in a list of T-EESs that are relevant to the supplied applications and the new location of the UE. When in step 1 the ACR for service continuity planning is triggered, then the Connectivity information and UE Location in the Service Provisioning procedure (as specified in clause 8.3) contains the expected Connectivity information and expected UE Location.

   If Service Provisioning results in no T-EES, and if ACR to CAS is supported, then the procedure for ACR with CAS applies as specified in clause 8.8.2A.2.

4. The EEC performs EAS discovery (as specified in clause 8.5) for the desired T-EASs by querying the T-EESs that were established in step 3 (or provided in the notification from the ECS – if it was the trigger). If EEC registration configuration for the EESs established in step 2 indicates that EEC registration is required, the EEC performs EEC registration with the EESs (as specified in clause 8.4.2.2.2) before sending the EAS discovery request. Step 5 is skipped if EAS discovery procedure results in only one discovered T-EAS.

   When in step 1 the ACR for service continuity planning is triggered, and the "General context holding time duration" is included in the replied EAS discovery response, the EEC can make ACR request before it reaches respective T-EAS service area within the time period indicated by the IE.

5. The AC and EEC select the T-EAS to be used for the application traffic.

NOTE 4: Several EEC registrations with different EESs may result from T-EAS discovery process during a single ACR operation.

6. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the S-EES with predicted/expected UE location or Expected AC Geographical Service Area, the ACR action indicating ACR initiation and the corresponding ACR initiation data (without the need to notify the EAS). When the S-EES receives the predicted/expected UE location or Expected AC Geographical Service Area from the EEC, then the S-EES will determine to monitor the UE mobility. The S-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable), as described in clause 8.8.3.4. If the EEC has not subscribed to receive ACR information notifications for ACR complete events from the S-EES, the EEC subscribes for the notifications as described in clause 8.8.3.5.2.

NOTE 5: It is expected that the AC will inform EAS about UE location monitoring is not needed

7. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.

8. The AC is triggered by the EEC to start ACT. The AC decides to initiate the transfer of application context from the S-EAS to the T-EAS. There may be different ways of transferring context and they are all outside the scope of this specification.

   When in step 1 the ACR for service continuity planning has been triggered, the AC connects to the T-EAS when the UE moves to the predicted location. Otherwise, the rest of this step is skipped.

   After the ACT is completed, the AC remains connected to the T-EAS and disconnects from the S-EAS; the EEC is informed of the completion.

NOTE 6: Whether and how the AC initiates the ACT is out of scope of the present document

When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the expected/predicted location the EEC does not connect to T-EES, the AC does not connect to the T-EAS.

NOTE 7: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 8: It is out of scope of this specification how the AC informs the S-EAS and T-EAS that ACT was part of service continuity planning. When in step 1 the ACR for service continuity planning is triggered, the S-EAS and the T-EAS can wait for the UE to move to the predicted location before they perform the Post ACR Clean up steps 9 and 10 if it is the EAS monitoring whether the UE moves to the predicted/expected location. When the S-EAS and the T-EAS do not wait for the UE (e.g., if the UE does not move to the predicted location), the S-EAS and the T-EAS can perform the Post ACR Clean up with failure messages.

NOTE 9: If the S-EAS and T-EAS are main EASs forming proxy bundle, other EASs of the bundle may transfer the application contexts in this step. How to execute ACT is out of scope of this document.

Phase IV: Post-ACR Clean up

9. The S-EAS sends the ACR status update message to the S-EES as specified in clause 8.8.3.8.

10. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 10: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 11: Steps 9 and 10 can occur in any order.

11. If the status in step 9 indicates a successful ACT, for non-planning case the S-EES sends the ACR information notification (ACR complete) message immediately to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. For the service continuity planning case, if it is EES monitors the UE mobility, then only when S-EES detects the UE has moved to the predicted/expected UE location or Expected AC Geographical Service Area and the status in step 9 indicates a successful ACT, then the S-EES sends ACR information notification (ACR complete) message to the EEC indicating that UE has moved to the predicted location when the ACR type is service continuity planning. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

8.8.2.3 EEC executed ACR via S-EES

In this scenario, the EEC is triggered as a result of the UE's movement as described in 8.8.1.1 or by an AC as described in clause 8.14.2.4. Figure 8.8.2.3-1 illustrates the EEC executing ACR via the S-EES.

Pre-condition:

1. The AC at the UE already has a connection to the S-EAS; and

2. The EEC is able to communicate with the S-EES.

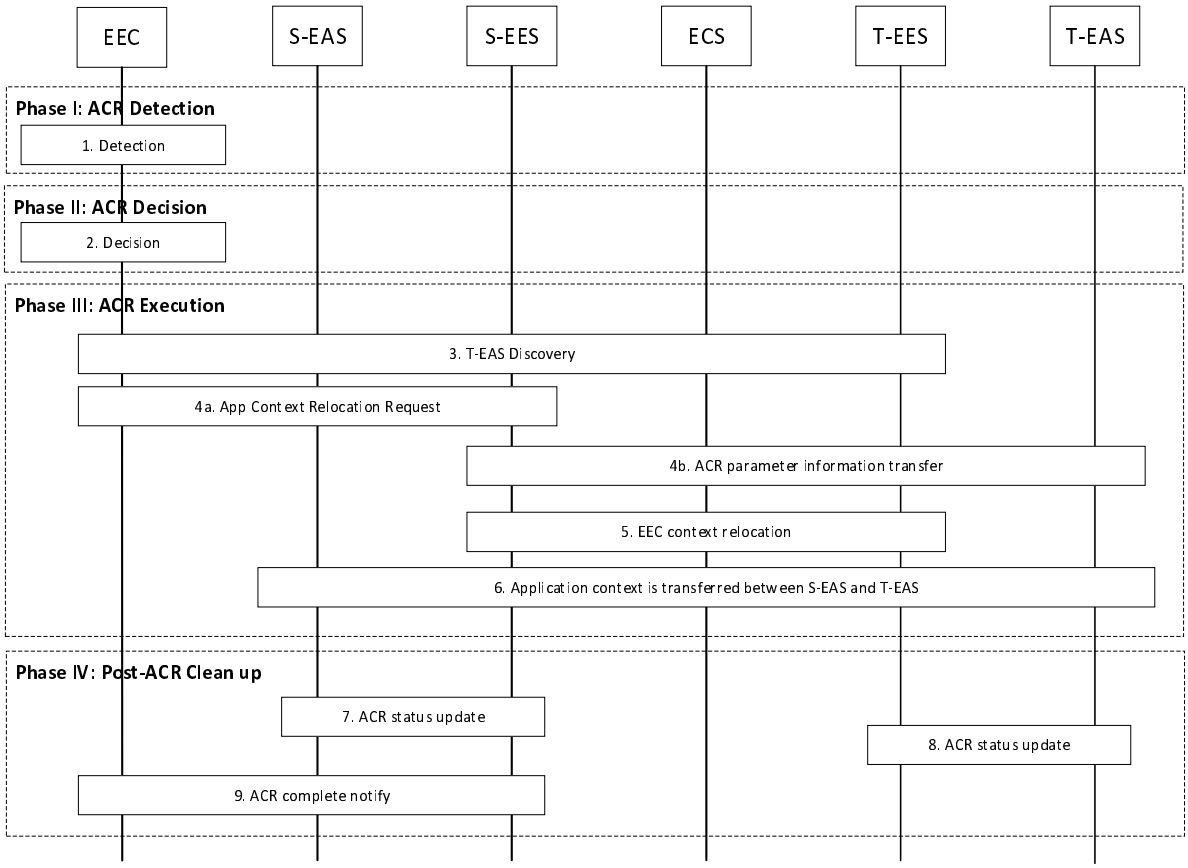

Figure 8.8.2.3-1: EEC executed ACR

Phase I: ACR Detection

1. The EEC detects that ACR may be required as described in clause 8.8.1.1. The EEC may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

Phase II: ACR Decision

2. The EEC decides to proceed required procedures for triggering ACR. If the EEC has received information of on-going ACR, then it should not initiate an ACR with the same ACR identity uniquely identified by ACID, EEC ID (or UE ID), S-EAS endpoint and T-EAS endpoint again per clause 8.8.3.5.3.

Phase III: ACR Execution

3. The EEC determines the T-EES by using the provisioned information or performing service provisioning procedure per clause 8.3 of the present document. When in step 1 the ACR for service continuity planning is triggered, then the Connectivity information and UE Location in the Service Provisioning (as specified in clause 8.3) procedure contains the expected Connectivity information and expected UE Location. If the UE is within the service area of the T-EES, upon selecting T-EES the UE may need to establish a new PDU connection to the target EDN. If EEC registration configuration for the T-EES indicates that EEC registration is required, the EEC performs EEC registration with the selected T-EES as specified in clause 8.4.2.2.2. The EEC can then discover and select T-EAS by performing EAS Discovery with the T-EES per clause 8.5.2 of the present document.

   If service provisioning results in no T-EES, and if ACR to CAS is supported, then the procedure for ACR with CAS applies as specified in clause 8.8.2A.3.

   When in step 1 the ACR for service continuity planning is triggered, and the "General context holding time duration" is included in the replied EAS discovery response, the EEC can make ACR request before it reaches respective T-EAS service area within the time period indicated by the IE.

NOTE 1: Several EEC registrations with different EESs may result from T-EAS discovery process during a single ACR operation.

4a. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the S-EES with predicted/expected UE location or Expected AC Geographical Service Area, the ACR action indicating ACR initiation and the corresponding ACR initiation data (with the need to notify the EAS). The S-EES authorises the request from the EEC. The S-EES decides to execute ACR based on the information received from the EEC, EEC context and/or EAS profile. The S-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable) and sends the ACR management notification for the "ACT start" event to the S-EAS, as described in clause 8.6.3, to initiate ACT between the S-EAS and the T-EAS. In ACT start, the S-EES includes indication of service continuity planning if the S-EES determine to monitor UE mobility. If the EEC has not subscribed to receive ACR information notifications for ACR complete events from the S-EES, the EEC subscribes for the notifications as described in clause 8.8.3.5.2.

4b. If the ACR request in step 4a includes ACR parameters, e.g. Prediction expiration time, the S-EES performs ACR parameter information procedure by sending the ACR parameter information request to the T-EES as described in clause 8.8.3.9.

5. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.

6. The S-EAS transfers the application context to the T-EAS at implementation specific time. This process is out of scope of the present specification.

   When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location, the EEC does not connect to T-EES, the AC does not connect to the T-EAS.

NOTE 2: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 3: When in step 1 the ACR for service continuity planning is triggered, the S-EAS and the T-EAS can wait for the UE to move to the predicted location before they perform the Post ACR Clean up steps 7 and 8 if it is the EAS monitoring whether the UE moves to the predicted/expected location. When the S-EAS and the T-EAS do not wait for the UE (e.g., if the UE does not move to the predicted location), the S-EAS and the T-EAS can perform the Post ACR Clean up with failure messages.

NOTE 4: If the S-EAS and T-EAS are main EASs forming proxy bundle, other EASs of the bundle may transfer the application contexts in this step. How to execute ACT is out of scope of this document.

Phase IV: Post-ACR Clean up

7. The S-EAS sends the ACR status update message to the S-EES as specified in clause 8.8.3.8.

8. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 5: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 6: Steps 7 and 8 can occur in any order.

9. If the status in step 7 indicates a successful ACT, for non-planning case the S-EES sends the ACR information notification (ACR complete) message immediately to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. For the service continuity planning case, if the EES monitors the UE mobility, then only when S-EES detects the UE has moved to the predicted/expected UE location or Expected AC Geographical Service Area and the status in step 7 indicates a successful ACT, then the S-EES sends ACR information notification (ACR complete) message to the EEC indicating that UE has moved to the predicted location when the ACR type is service continuity planning. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

8.8.2.4 S-EAS decided ACR scenario

In this scenario, the S-EAS may detect the need of ACR locally or is notified by the S-EES via ACR management notifications or UE location notifications. The S-EAS make the decision about whether to perform the ACR, and starts the ACR at a proper time.

NOTE 1: For this clause, S-EAS either supports ACR detection capability or performs subscription for ACR management event to EES.Pre-conditions:

1. The S-EAS may depend on the receipt ACR management events from the S-EES, e.g. "user plane path change" events or "ACR monitoring" events as described in clause 8.6.3, to detect the need for an ACR. The S-EAS may also depend on the receipt of UE location notification from the S-EES as described in clause 8.6.2.2.3, to detect the need for an ACR. For the following procedure it is assumed that the S-EAS has subscribed to continuously receive the respective events from the S-EES; and

2. The EEC has subscribed to receive ACR information notifications for target information notification events and ACR complete events from the S-EES, as described in clause 8.8.3.5.2.

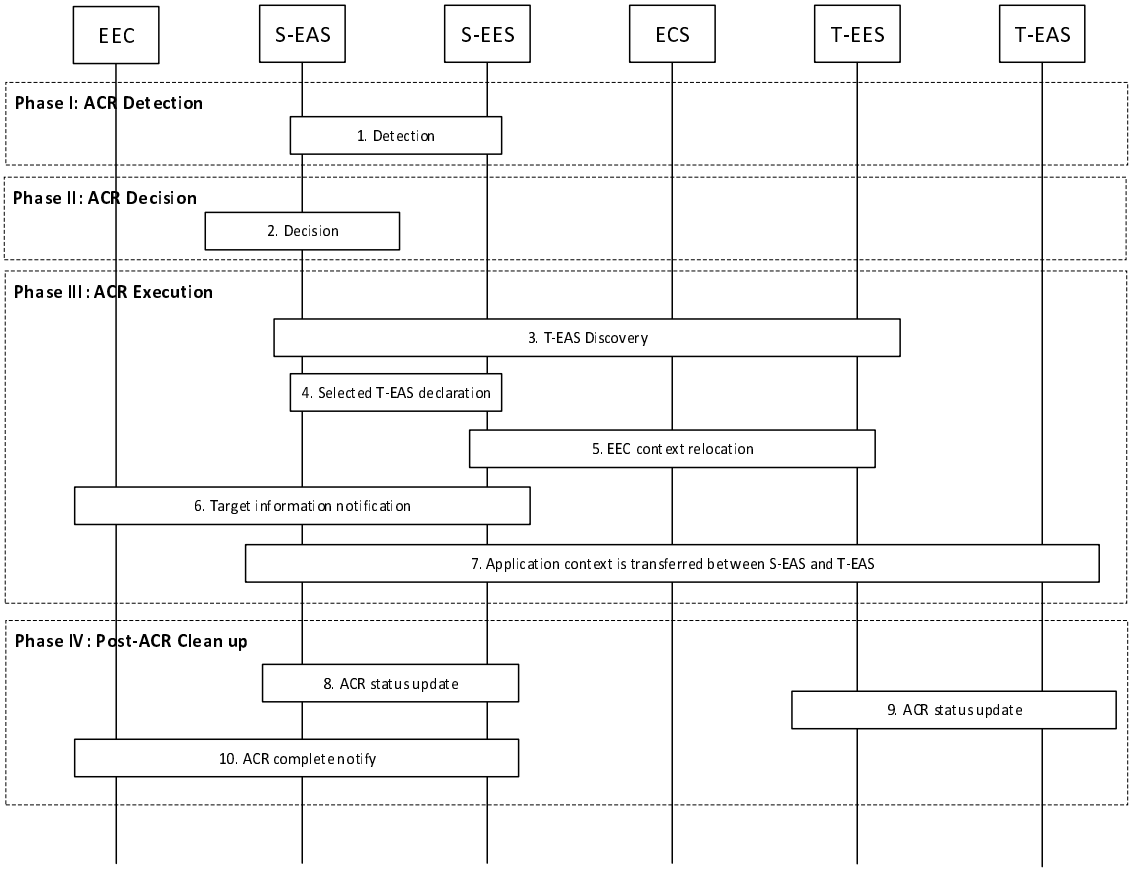

Figure 8.8.2.4-1: S-EAS decided ACR

S-EAS decided ACR is outlined with four main phases: detection, decision, execution and clean up.

Phase I: ACR Detection

1. The S-EAS either receives ACR management notifications from source Edge Enabler Sever indicating that ACR may be required ("ACR monitoring" event), or self detects the need for ACR (e.g. upon receipt of a "user plane path change" event or UE location notification). If the ACR management notification indicates "ACR monitoring" event, then the notification will also contain the T-EAS information (see clause 8.6.3.2.3). The S-EAS may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

NOTE 2: How the S-EAS self detects the local need for ACR is outside the scope of this specification.

Phase II: ACR Decision

2. The S-EAS makes the decision to perform the ACR If the S-EAS has received information of on-going ACR, then it should not initiate an ACR with the same ACR identity uniquely identified by ACID, EEC ID (or UE ID), S-EAS endpoint and T-EAS endpoint again. per clause 8.6.3.2.3.

NOTE 3: How the S-EAS determines when to start the ACR is outside the scope of this specification. The ASP can have service agreement with ECSP regarding which EES API to use for ACR detection.

Phase III: ACR Execution

3. The S-EAS discovers the T-EAS as described in clause 8.8.3.2. When in step 1 the ACR has been triggered for service continuity planning, then UE Location and Target DNAI values in the Retrieve T-EES procedure contain the expected UE Location and expected Target DNAI. After S-EAS determines the T-EAS to use, the S-EAS may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable).

   If T-EAS discovery results in no T-EAS, and if ACR to CAS is supported, then the procedure for ACR with CAS applies as specified in clause 8.8.2A.4.

4. The S-EAS sends selected T-EAS declaration message to S-EES, to inform S-EES the determined T-EAS to use as described in clause 8.8.3.7. The S-EAS may send the ACID and Predicted/Expected UE location or Expected AC Geographical Service Area to the EES. When the EES receives the predicted/expected UE location or Expected AC Geographical Service Area from the EAS, then the EES will determine to monitor the UE mobility.

5. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.

6. Based on the T-EAS selection information received from the S-EAS, the S-EES sends the target information notification to the EEC as described in clause 8.8.3.5.3. The selected T-EES may be included in the target information and the ACID which corresponds to the selected target EAS is included in the notification sent to the EEC as described in clause 8.8.3.5.3.

NOTE 4: Step 6 can be performed after step 4. The S-EES can send target information notification to the EEC immediately after having the target information in order to avoid EEC to initiate another ACR with the same identity.

7. The S-EAS transfers the application context to the T-EAS selected in step 3. This process is out of scope of the present specification.

   When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location, the EEC does not connect to T-EES, the AC does not connect to the T-EAS.

NOTE 5: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 6: When in step 1 the ACR has been triggered for service continuity planning, the S-EAS and the T-EAS can wait for the UE to move to the predicted location before they perform the Post ACR Clean up steps 8 and 9 if it is the EAS monitoring whether the UE moves to the predicted/expected location. When the S-EAS and the T-EAS do not wait for the UE (e.g., if the UE does not move to the predicted location), the S-EAS and the T-EAS can perform Post ACR Clean up with failure messages.

NOTE 7: If the S-EAS and T-EAS are main EASs forming proxy bundle, other EASs of the bundle may transfer the application contexts in this step. How to execute ACT is out of scope of this document.

Phase IV: Post-ACR clean up

8. The S-EAS sends the ACR status update message to the S-EES as specified in clause 8.8.3.8.

9. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 8: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 9: Steps 8 and 9 can occur in any order.

10. If the status in step 8 indicates a successful ACT, for non-planning case the S-EES sends the ACR information notification (ACR complete) message immediately to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. For the service continuity planning case, if it is EES monitors the UE mobility, then only when S-EES detects the UE has moved to the predicted/expected UE location or Expected AC Geographical Service Area and the status in step 8 indicates a successful ACT, then the S-EES sends ACR information notification (ACR complete) message to the EEC indicating that UE has moved to the predicted location when the ACR type is service continuity planning. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

8.8.2.5 S-EES executed ACR

Figure 8.8.2.5-1 illustrates the S-EES detecting, deciding and executing ACR from the S-EAS to the T-EAS. This may include EELManagedACR by S-EES when initiated by S-EAS as per clause 8.8.3.6. The EEC or the S-EAS may also detect the ACR as illustrated in figure 8.8.2.5-1.

NOTE 1: For this clause, S-EAS either supports ACR detection capability or performs subscription for ACR management event to EES.

Pre-condition:

1. The AC at the UE already has a connection to the S-EAS;
2. The EEC is able to communicate with the S-EES;
3. The EEC has subscribed to receive ACR information notifications for target information notification events and ACR complete events from the S-EES, as described in clause 8.8.3.5.2;
4. The S-EAS optionally subscribed to receive ACR management notifications for "ACR facilitation" events to the S-EES, in order to enable detection at S-EAS.
5. In case of EELManagedACR, the T-EAS has subscribed to receive ACT status notifications as described in clause 8.8.3.6.2.3.

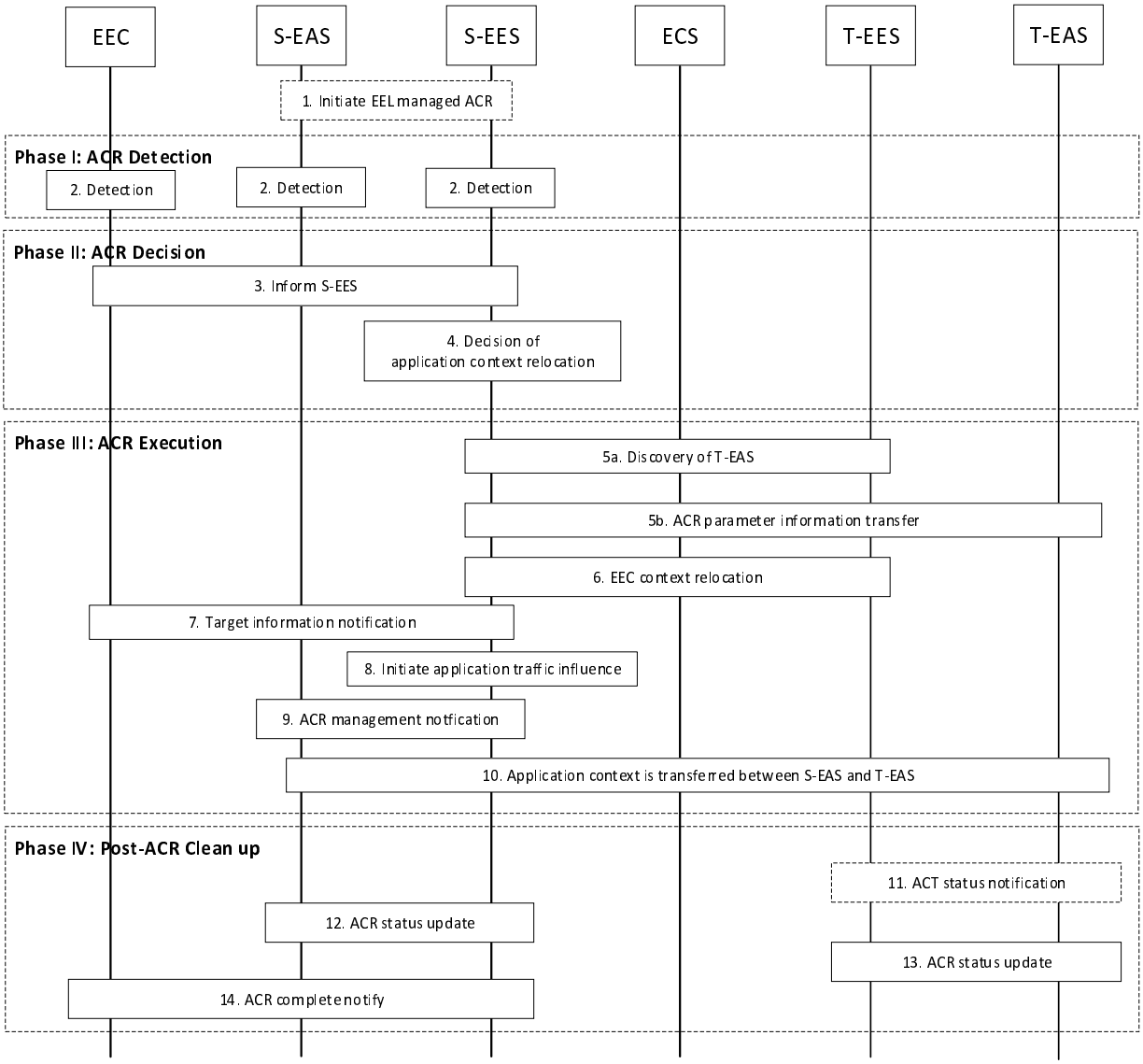

Figure 8.8.2.5-1: S-EES executed ACR

1. The S-EAS may initiate EELManagedACR with S-EES as specified in clause 8.8.3.6. The S-EAS and S-EES negotiate an address of the Application Context storage to S-EES. The S-EAS puts the Application Context at this address which can be further accessed by the S-EES when the ACT is required.

   In the EELManagedACR case, the S-EES executes steps 2 (i.e., S-EES is the detection entity), 4, 5, 6, 7, 8, 9, 10, 11, 13 and 14. Rest of steps are skipped.

Phase I: ACR Detection

2. Detection entities (S-EAS, S-EES, EEC) detect that ACR may be required and identify the ACID and Predicted/Expected UE location or Expected AC Geographical Service Area as described in clause 8.8.1.1. The detection by the S-EES may be triggered by the User Plane path change notification received from the 3GPP Core Network due to S-EAS request for "ACR facilitation" event (see clause 8.6.3) or due to step 1.

   The detection entity may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

Phase II: ACR Decision

3. The detection entity performs ACR launching procedure (as described in clause 8.8.3.4) with the ACR action indicating ACR determination and the corresponding ACR determination data. If the EEC or S-EAS detect the ACR event, the EEC or S-EAS may inform S-EES with ACID, and predicted/expected UE location or Expected AC Geographical Service Area in the ACR launching procedure.

4. The S-EES authorises the message if received. The S-EES decides to execute ACR based on the information received or local detection, and the information of EEC context or EAS profile, and then proceed the below steps. When the S-EES receives the predicted/expected UE location or Expected AC Geographical Service Area from the EEC or the EAS in ACR determination, or the S-EES received service continuity planning from EAS in ACR facilitation event subscription, then the S-EES will determine to monitor the UE mobility. If S-EES has received information of on-going ACR, then it should not initiate an ACR with the same ACR identity uniquely identified by ACID, EEC ID (or UE ID), S-EAS endpoint and T-EAS endpoint again per clause 8.6.3.2.3.

Phase III: ACR Execution

5a. The S-EES determines T-EES and T-EAS via the Discover T-EAS procedure in clause 8.8.3.2 of the present document. When in step 2 the ACR has been triggered for service continuity planning, then UE Location and Target DNAI values provided in the Retrieve T-EES procedure contain the expected UE Location and expected Target DNAI. The S-EES may decide not to perform ACR if T-EAS is not available.

   If T-EAS discovery results in no T-EAS, and if ACR to CAS is supported, then the procedure for ACR with CAS applies as specified in clause 8.8.2A.5.

5b. If required, the S-EES performs ACR parameter information procedure by sending the ACR parameter information request to the T-EES as described in clause 8.8.3.9. For example, when the ACR is for service continuity planning, and the S-EES has received it in ACR launch in step 2, the S-EES sends ACR parameter information request which includes Prediction expiration time.

6. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.

7. The S-EES sends the target information notification to the EEC as described in clause 8.8.3.5.3.

NOTE 2: Step 7 can be performed after step 5. The S-EES can send target information notification to the EEC immediately after having the target information in order to avoid EEC to initiate another ACR with the same identity

8. The S-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable).

9. The S-EES sends the ACR management notification (e.g. as notification for "ACR facilitation" event or "ACT start" event as described in clause 8.6.3 or due to step 1) to the S-EAS to initiate ACT between the S-EAS and the T-EAS.

10. The Application Context is transferred from S-EAS to the T-EAS at implementation specific time. In the case of EELManagedACR, the S-EES accesses the Application Context from the address as per step 1 and the S-EES and T-EES engage in the ACT from S-EAS to the T-EAS (obtained as per step 5) in a secure way. Further the T-EAS accesses the Application Context made available by the T-EES. If S-EAS performs the ACT directly with T-EAS, the specification of such process is out of scope of the present document.

NOTE 3: The Application Context is encrypted and protected by the application layer. The S-EES and the T-EES engage in the packet level transport of the Application Context and they have no visibility to the content of the Application Context.

When in step 2 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location, the EEC does not connect to T-EES, the AC does not connect to the T-EAS.

NOTE 3: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 4: When in step 2 the ACR has been triggered for service continuity planning, the S-EAS and the T-EAS can wait for the UE to move to the predicted location before they perform the Post ACR Clean up steps 12 and 13 if it is the EAS monitoring whether the UE moves to the predicted or expected location. When the S-EAS and the T-EAS do not wait for the UE (e.g., if the UE does not move to the predicted location), the S-EAS and the T-EAS can perform Post ACR Clean up with failure messages.

NOTE 5: If the S-EAS and T-EAS are main EASs forming proxy bundle, other EASs of the bundle may transfer the application contexts in this step. How to execute ACT is out of scope of this document.

Phase IV: Post-ACR Clean up

11. In case of EELManagedACR, once the ACT is successful, the T-EES sends an ACT status notification to the T-EAS as described in clause 8.8.3.6.2.4, indicating that the Application Context is available.

12. The S-EAS sends the ACR status update message to the S-EES as specified in clause 8.8.3.8.

13. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 6: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 7: Steps 12 and 13 can occur in any order.

14. If the status in step 12 indicates a successful ACT or in the EELManagedACR case, the S-EES sends the ACR information notification (ACR complete) message immediately to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. For the service continuity planning case, if it is EES monitors the UE mobility, then only when S-EES detects the UE has moved to the predicted/expected UE location or Expected AC Geographical Service Area and the status in step 12 indicates a successful ACT, then the S-EES sends ACR information notification (ACR complete) message to the EEC when the ACR type is service continuity planning. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

NOTE 8: The Application Client mechanism to support switchover of the application traffic to T-EAS is out of scope of the specification.

8.8.2.6 EEC executed ACR via T-EES

In this scenario, the EEC is triggered as a result of the UE's movement as described in 8.8.1.1 or by an AC as described in clause 8.14.2.4. Figure 8.8.2.6-1 illustrates the EEC executing ACR via the T-EES.

Pre-condition:

1. The EEC has the S-EAS information that serves the AC.

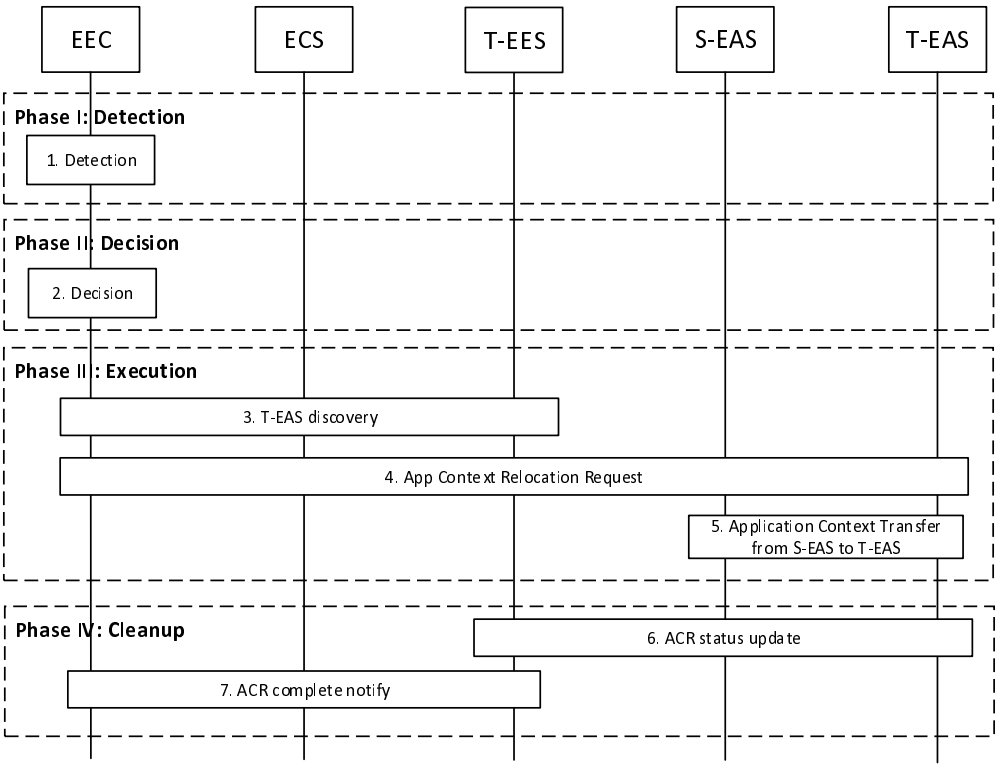

Figure 8.8.2.6-1: EEC executed ACR via T-EES

Phase I: ACR Detection

1. The EEC detects that ACR may be required as described in clause 8.8.1.1. The EEC may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

Phase II: ACR Decision

2. The EEC decides to proceed with required procedures for ACR. If the EEC has received information of on-going ACR, then it should not initiate an ACR with the same ACR identity uniquely identified by ACID, EEC ID (or UE ID), S-EAS endpoint and T-EAS endpoint again per clause 8.8.3.5.3.

NOTE 1: If supported, the AC can be involved in the decision. It is out of scope of the present document how the AC is involved.

Phase III: ACR Execution

3. The EEC determines the T-EES by using the provisioned information or performing service provisioning procedure per clause 8.3. When in step 1 the ACR for service continuity planning is triggered, then the Connectivity information and UE Location used in the service provisioning procedure contain the expected Connectivity information and expected UE Location. If the UE is within the service area of the T-EES, upon selecting the T-EES the UE may need to establish a new PDU connection to the target EDN. If EEC registration configuration for the T-EES indicates that EEC registration is required, the EEC performs registration with the selected T-EES as specified in clause 8.4.2.2.2. The EEC performs EAS Discovery with the T-EES per clause 8.5.2.

   When in step 1 the ACR for service continuity planning is triggered, and the "General context holding time duration" is included in the replied EAS discovery response, the EEC can make ACR request before it reaches respective T-EAS service area within the time period indicated by the IE.

NOTE 2: Several EEC registrations with different EESs may result from T-EAS discovery process during a single ACR operation.

4. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the T-EES with predicted/expected UE location or Expected AC Geographical Service Area, the ACR action indicating ACR initiation and the corresponding ACR initiation data (with the need to notify the EAS). When the T-EES receives the predicted/expected UE location or Expected AC Geographical Service Area from the EEC, then the T-EES will determine to monitor the UE mobility. If the received ACR initiation request contains an EEC context ID and the S-EES Endpoint, the T-EES performs an EEC Context Pull relocation (clause 8.9.2.2). The T-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable). Then the T-EES sends the ACR management notification with "ACT start" event message to the T-EAS, the T-EES includes indication of service continuity planning if the T-EES determines to monitor UE mobility during post-ACR phase. If the ACR request in ACR launching procedure includes ACR parameters, e.g. Prediction expiration time, the T-EES includes the ACR parameters in the notification to T-EAS. The EEC also subscribes to receive ACR information notifications for ACR complete events from the T-EES, as described in clause 8.8.3.5.2.

5. The T-EAS initiates ACT between the S-EAS and the T-EAS. This process is out of scope of the present specification.

When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location the EEC does not connect to T-EES, the AC does not connect to the T-EAS.

NOTE 3: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 4: When in step 1 the ACR has been triggered for service continuity planning, the S-EAS and the T-EAS can wait for the UE to move to the predicted location before the T-EAS performs the Post ACR Clean up step 6 if it is the EAS monitoring whether the UE moves to the predicted/expected location. When the S-EAS and the T-EAS do not wait for the UE (e.g., if the UE does not move to the predicted location), the T-EAS can perform Post ACR Clean up with failure messages.

NOTE 5: If the S-EAS and T-EAS are main EASs forming proxy bundle, other EASs of the bundle may transfer the application contexts in this step. How to execute ACT is out of scope of this document.

Phase IV: Post-ACR clean up

6. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 6: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

7. The T-EES immediately sends the ACR information notification (ACR complete) message to the EEC as described in clause 8.8.3.5.3 for non-planning case. For the service continuity planning case, if it is EES monitors the UE mobility, then only when T-EES detects the UE has moved to the predicted/expected UE location or Expected AC Geographical Service Area and the status in step 6 indicates a successful ACT, then the S-EES sends ACR information notification (ACR complete) message to the EEC indicating that UE has moved to the predicted location when the ACR type is service continuity planning. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

If the procedure fails after step 4, it will be terminated with an appropriate cause in the ACR information notification to the EEC in step 7. The EEC may then proceed attempting to obtain services from the T-EAS discovered in step 3 without service continuity support. Alternatively, the EEC may resume the present procedure starting with step 4 and selecting a different T-EES discovered in step 3 with EAS service continuity support.

NOTE 7: The support of ACR between EDNs operated by different ECSPs is dependent on business agreement between the ECSPs.

8.8.2.7 ACR for direct EAS bundle, executed by EEC

In this scenario, the EEC executes necessary ACR for AC-EAS service session(s) in a bundle, and it follows the scenario described in clause 8.8.2.3 with the following differences:

- all T-EAS(s) in a bundle requiring service continuity are discovered and selected during step 3. If the affinity is set to strong, then T-EASs are from the same EDN.

NOTE: T-EAS(s) should be within the same EDN as preferred if EAS affinity is preferred, or different EDNs if no T-EAS(s) in same EDN available, if the EAS affinity is set to weak.

- all bundled T-EAS endpoints are sent to the corresponding S-EES(s) in the ACR request and the S-EES(s) may apply AF traffic influence for the received T-EAS(s) in step 4a.

- Each associated EES (i.e. EES serving bundle EASs) aggregates ACR status update from its served and bundled EASs in step 7 and step 8 and sends ACR complete notification to the EEC in step 9.

- The EEC collects ACR complete notifications in step 9 and completes the ACR for the EAS bundle.

8.8.2.8 ACR for EAS bundle, executed by S-EAS

In this scenario, the main S-EAS executes and triggers necessary ACR for all AC-EAS service session(s) in a bundle.

This scenario description is same as described for figure 8.8.2.4-1 except for the following clarifications:

Pre-condition:

1. The main S-EAS may depend on the receipt of ACR management events from its S-EES, e.g. "user plane path change" events or "ACR monitoring" events as described in clause 8.6.3, to detect the need for an ACR. The main S-EAS may also depend on the receipt of UE location notification from its S-EES as described in clause 8.6.2.2.3, to detect the need for an ACR. For the following procedure it is assumed that the main S-EAS has subscribed to continuously receive the respective events; and

2. The EEC has subscribed to receive ACR information notifications for target information notification events and ACR complete events from S-EESs serving the EAS bundle, as described in clause 8.8.3.5.2.

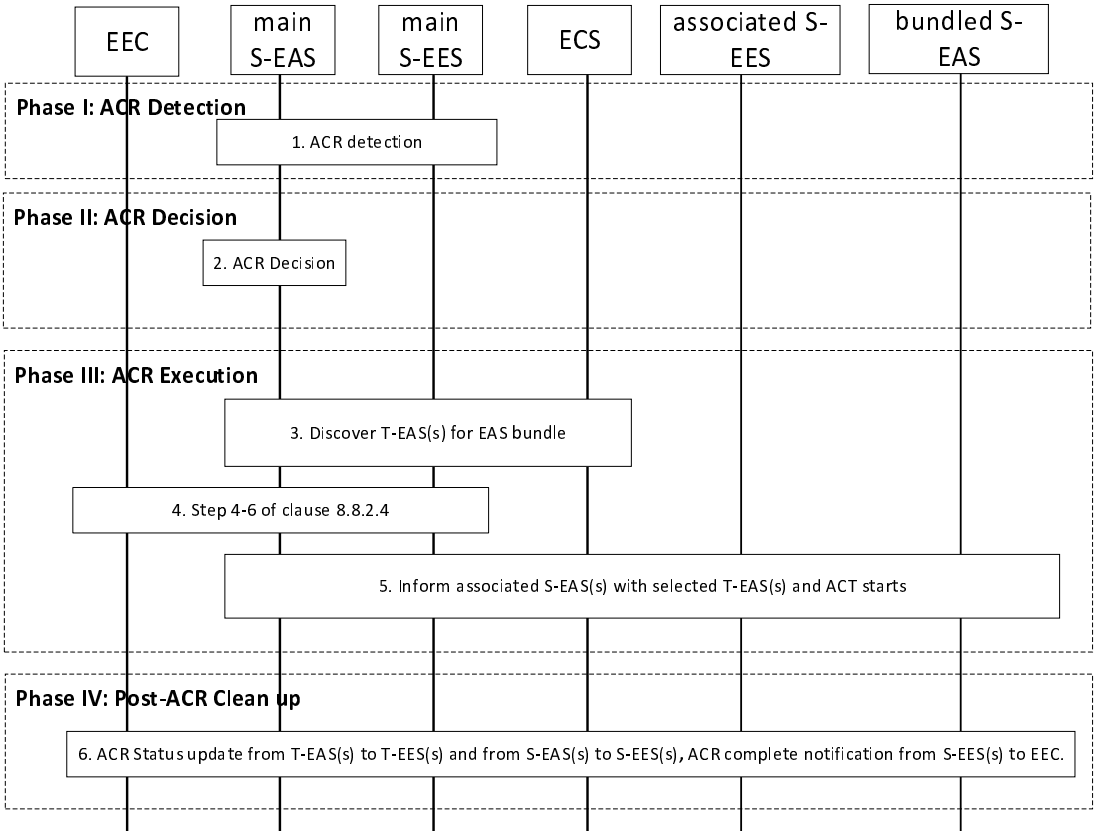

Figure 8.8.2.8-1: S-EAS executed ACR for EAS bundle

Phase I: ACR Detection

1. ACR is detected, the procedure is same as step 1 of clause 8.8.2.4.

Phase II: ACR Decision

2. The main S-EAS performs ACR decision for bundled EASs.

NOTE 1: The main S-EAS is aware of all bundle EASs service area and/or DNAIs so it can decide whether to perform ACR for the corresponding EASs.

Phase III: ACR Execution

3. The main S-EAS discovers from all candidate T-EAS(s) in EAS bundle as described in clause 8.8.3.2. If the affinity is set to strong, then T-EASs are from the same EDN. The main S-EAS may apply AF traffic influence for all bundled T-EAS(s).

NOTE: T-EAS(s) should be within the same EDN as preferred if EAS affinity is preferred, or different EDNs if no T-EAS(s) in same EDN available, if the EAS affinity is set to weak.

4. The procedure is same as step 4 to step 6 of clause 8.8.2.4. The main S-EAS sends selected T-EAS declaration message to the main S-EES with the selected T-EASs, the main S-EES sends selected T-EAS(s) to the EEC.

5. The main S-EES informs associated S-EESs with bundled T-EASs. Then ACT starts between the S-EAS(s) and T-EAS(s) in a bundle requiring service continuity.

Phase IV: Post-ACR Clean up

6. During post-ACR, all S-EASs and T-EASs send ACR status update to S-EES and T-EES, respectively, as described in step 8 and step 9 of clause 8.8.2.4. The EEC collects ACR complete notifications from all S-EESs and ACR for EAS bundle is completed.

8.8.2.9 ACR for EAS bundle, executed by S-EES

In this scenario, a main S-EES (serving a main S-EAS) executes and triggers necessary ACR for AC-EAS service session(s) in a bundle.

This scenario description is same as described for figure 8.8.2.5-1 except for the following clarifications:

Pre-condition:

1. The AC at the UE already has a connection with S-EASs in a bundle;
2. The EEC subscribes to receive ACR information notifications for target information notification events and ACR complete events from S-EESs serving the EAS bundle, as described in clause 8.8.3.5.2;
3. The main S-EAS may subscribe to receive ACR management notifications for "ACR facilitation" events to the main S-EES, in order to enable ACR detection at the main S-EES.

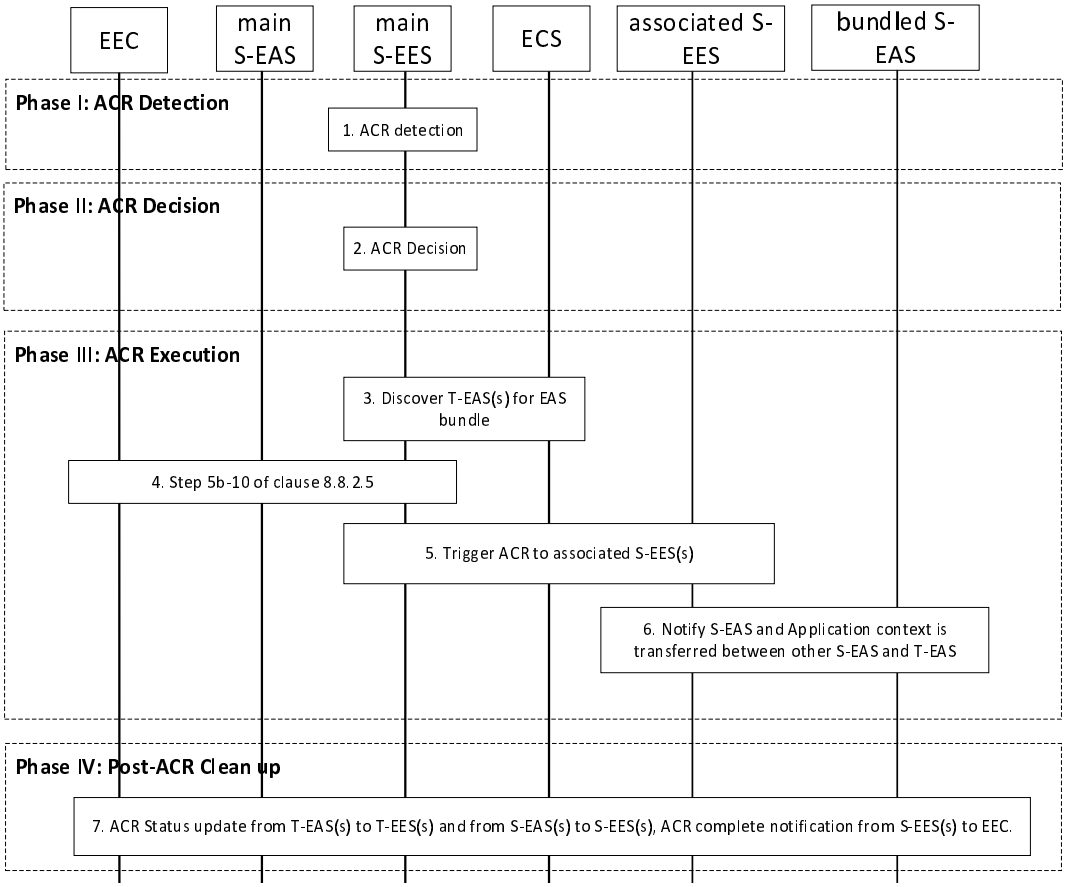

Figure 8.8.2.9-1: S-EES executed ACR for EAS bundle

Phase I: ACR Detection

1. The main S-EES detects the need for ACR, the procedure is same as step 2 of clause 8.8.2.5.

Phase II: ACR Decision

2. The main S-EES performs ACR decision for bundled EASs.

NOTE 1: The main S-EES is aware of all bundle EASs service area and/or DNAIs so it can decide whether to perform ACR for the corresponding EASs.

Phase III: ACR Execution

3. The main S-EES discovers all candidate T-EAS(s) in EAS bundle as described in clause 8.8.3.2. If the affinity is set to strong, then T-EASs are from the same EDN.

NOTE 2: T-EAS(s) should be within the same EDN as preferred if EAS affinity is preferred, or different EDNs if no T-EAS(s) in same EDN available, if the EAS affinity is set to weak.

4. The procedure is same as step 5b to step 10 of clause 8.8.2.5. The main S-EES sends selected T-EAS(s) to the EEC, triggers application traffic influence for T-EAS(s) and notifies the main S-EAS with selected T-EAS of the same EAS service. The main S-EES may notify more S-EAS(s) with selected T-EAS of the corresponding EAS service.

5. The main S-EES performs ACR launching procedure (as described in clause 8.8.3.4) with the ACR action indicating ACR initiation and the corresponding ACR initiation data to the associated S-EES(s).

6. The associated S-EES(s) notifies the corresponding bundled S-EAS(s) and ACT starts between the S-EAS(s) and T-EAS(s) in a bundle requiring service continuity.

Phase IV: Post-ACR Clean up

7. During post-ACR, all S-EASs and T-EASs send ACR status update to S-EES and T-EES, respectively, as described in step 12 and step 13 of clause 8.8.2.5. The EEC collects ACR complete notifications from all S-EESs and ACR for EAS bundle is completed.

8.8.2A Scenarios for ACR between EAS and CAS

8.8.2A.1 General

Service continuity between CAS and EAS is supported without CES, corresponding to the architecture options described in clause 6.2c. The ACR can be triggered by a change or expected change in UE location or in case of an overload situation or maintenance aspects in the S-EAS or EDN if no suitable target EAS is found as described in clause 8.8.1.1 depending on the scenario.

To facilitate future ACRs from the CAS back to EAS, the EEC may request and receive an AF-specific UE ID or Edge UE ID from the S-EES as described in clause 8.6.5, which can be used by the CAS to perform EAS discovery on the S-EES when there is an ACR from CAS back to an EAS. The EEC may also request to subscribe to notifications from the S-EES via the SEAL notification management service as described in clause 9.1 to receive ACR notifications if the EEC is no longer within reach from the S-EES.

8.8.2A.2 Enabling ACR with CAS - Initiation by EEC using regular EAS Discovery

In this scenario, ACR is a result of the UE moving to, or the UE expecting to move to, a new location which is outside the service area of the serving EAS. It further relies on the EEC being triggered as a result of the UE's movement.

This scenario is based on Service Provisioning (as specified in clause 8.3) and DNS procedures to discover the CAS that shall serve the AC as a result of the UE's new location, and that shall receive the Application Context from the serving EASs. The scenario below describes the relocation of a single application context to a CAS. However, it should be repeated for each active AC in the UE for which EAS or EDN is not available on that UE location.

This scenario description is same as described for figure 8.8.2.2-1 except for the following clarifications:

Pre-conditions: Same pre-conditions apply described for figure 8.8.2.2-1.

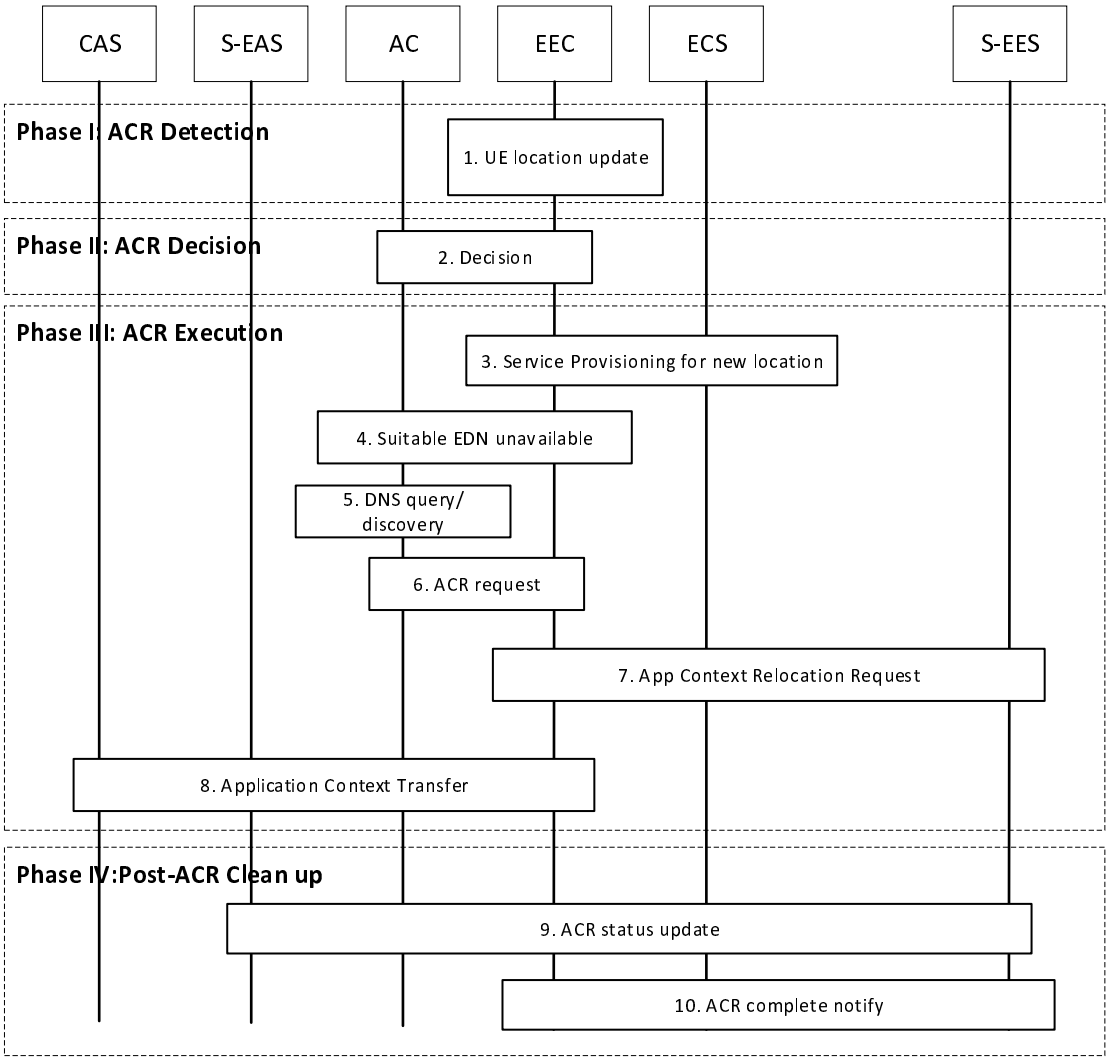

Figure 8.8.2A.2-1: Enabling ACR with CAS - Initiation by EEC using regular EAS Discovery

Phase I: ACR Detection

1. Same as step 1 described for figure 8.8.2.2-1.

Phase II: ACR Decision

2. Same as step 2 described for figure 8.8.2.2-1.

Phase III: ACR Execution

3. The EEC performs Service Provisioning (as specified in clause 8.3) for all active applications that require ACR. Since the location of the UE has changed, this procedure results in unavailability of T-EESs that are relevant to the supplied applications and the new location of the UE.

4. If the change in the UE's location triggers a need to change the S-EAS but the EEC is not provided with a T-EAS, the EEC informs the AC of the unavailability of a suitable EDN for the new location of the UE.

5. The AC triggers the UE to perform DNS resolution for the CAS relevant for the AC. The UE may need to establish a new PDU connection to the CAS.

6. The AC sends ACR request to the EEC and the EEC responds ACR response to the AC.

7. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the S-EES with the ACR action indicating ACR initiation and the corresponding ACR initiation data (along with the details of the CAS and

without the need to notify the EAS). The S-EES may apply the AF traffic influence with the N6 routing information of the CAS in the 3GPP Core Network (if applicable), as described in clause 8.8.3.4. Based on the received CAS information, the S-EES informs the CAS with the S-EES endpoint information by selected EES declaration request as described in clause 8.8.3.10.

8. The AC is triggered by the EEC to start ACT. The AC decides to initiate the transfer of application context from the S-EAS to the CAS.

   After the ACT is completed, the AC remains connected to the CAS and disconnects from the S-EAS; the EEC is informed of the completion of the ACT.

   The S-EAS or CAS can further decide to terminate the ACR, and the CAS can discard the application context (e.g. based on monitoring the location of the UE). It is up to the implementation of the S-EAS and CAS whether and how to make such a decision.

Phase IV: Post-ACR Clean up

9. Same as step 9 described for figure 8.8.2.2-1.

10. Same as step 11 described for figure 8.8.2-1.

8.8.2A.3 Enabling ACR with CAS - EEC executed ACR via S-EES

In this scenario, the EEC is triggered as a result of the UE's movement as described in clause 8.8.1.1. Figure 8.8.2A.3-1 illustrates the EEC executing ACR via the S-EES.

This scenario description is same as described for figure 8.8.2.3-1 except for the following clarifications:

Pre-conditions: Same pre-conditions apply described for figure 8.8.2.3-1.

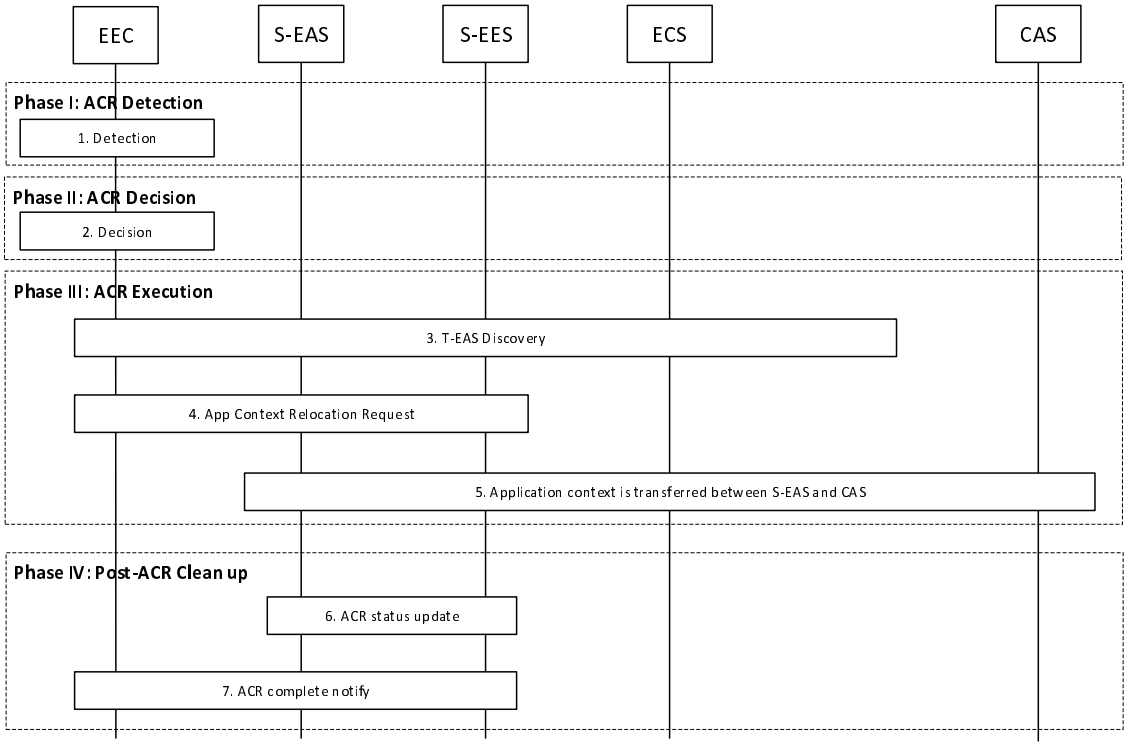

Figure 8.8.2A.3-1: Enabling ACR with CAS - EEC executed ACR via S-EES

Phase I: ACR Detection

1. Same as step 1 described for figure 8.8.2.3-1.

Phase II: ACR Decision

2. Same as step 2 described for figure 8.8.2.3-1.

Phase III: ACR Execution

3. The EEC performs Service Provisioning (as specified in clause 8.3) for all active applications that require ACR. Since the location of the UE has changed, this procedure results in unavailability of T-EESs that are relevant to the supplied applications and the new location of the UE. Service provisioning or discovery of relevant T-EAS may not result in EES configuration or T-EAS is not discovered respectively. If no T-EES is available based on service provisioning response, the AC or EECtriggers the UE to perform DNS resolution for the cloud application server relevant for the AC as described in clause 8.14.2.5.3, 8.14.3.12 and 8.14.3.15. The UE may need to establish a new PDU connection to the CAS.

4. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the S-EES with the ACR action indicating ACR initiation and the corresponding ACR initiation data (along with the details of the CAS and with the need to notify the EAS). The S-EES authorises the request from the EEC. The S-EES decides to execute ACR based on the information received from the EEC and/or EAS profile. The S-EES may apply the AF traffic influence with the N6 routing information of the CAS in the 3GPP Core Network (if applicable) and sends the ACR management notification for the "ACT start" event to the S-EAS, as described in clause 8.6.3, to initiate ACT between the S-EAS and the CAS. Based on the received CAS information, the S-EES informs the CAS with the S-EES endpoint information by selected EES declaration request as described in clause 8.8.3.10. If the EEC has not subscribed to receive ACR information notifications for ACR complete events from the S-EES, the EEC subscribes for the notifications as described in clause 8.8.3.5.2.

5. The S-EAS transfers the application context to the CAS at implementation specific time. This process is out of scope of the present specification.

NOTE 1: The S-EAS or CAS can further decide to terminate the ACR, and the CAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and CAS whether and how to make such a decision.

Phase IV: Post-ACR Clean up

6. Same as step 7 described for figure 8.8.2.3-1.

7. Same as step 9 described for figure 8.8.2.3-1.

NOTE 2: The CAS can perform capability exposure subscription with 3GPP CN directly, upon receiving the application context, which may be helpful for handling future ACR scenarios e.g. ACR from cloud to edge.

8.8.2A.4 Enabling ACR with CAS - S-EAS decided ACR

In this scenario, the S-EAS may detect the need of ACR locally or is notified by the S-EES via ACR management notifications for "ACR monitoring" events. The S-EAS make the decision about whether to perform the ACR, and starts the ACR at a proper time.

This scenario description is same as described for figure 8.8.2.4-1 except for the following clarifications:

Pre-conditions: Same pre-conditions apply described for figure 8.8.2.4-1.

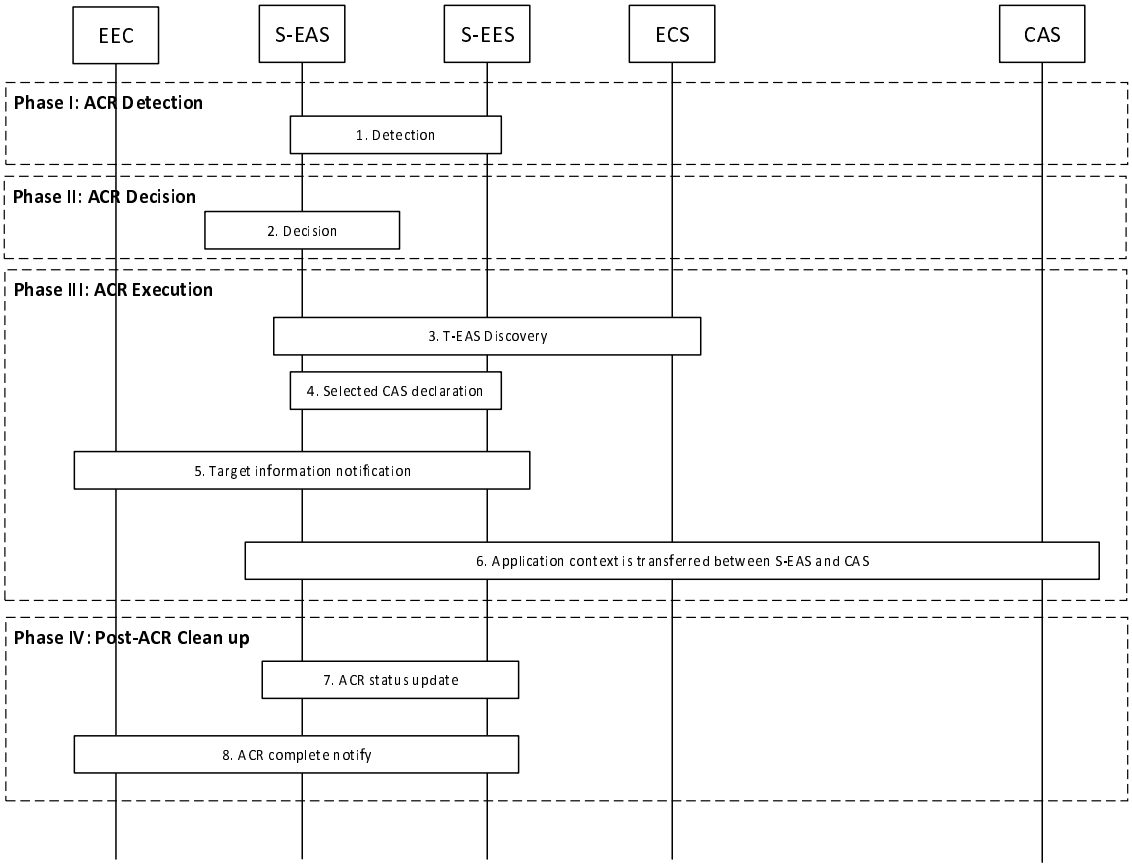

Figure 8.8.2A.4-1: Enabling ACR with CAS - S-EAS decided ACR scenario

S-EAS decided ACR is outlined with four main phases: detection, decision, execution and clean up.

Phase I: ACR Detection

1. Same as step 1 described for figure 8.8.2.4-1.

Phase II: ACR Decision

2. Same as step 2 described for figure 8.8.2.4-1.

Phase III: ACR Execution

3. If the ACR required is self detected, the S-EAS requests the S-EES to discover the targets. When S-EES determines that no relevant EAS is available for the UE's location, the discovery response returns T-EAS discovery failure. After S-EAS determines to use CAS and performs the DNS query/discovery, the S-EAS may apply the AF traffic influence with the N6 routing information of the CAS in the 3GPP Core Network (if applicable).

4. The S-EAS sends selected CAS declaration message to S-EES, to inform S-EES the determined CAS to use as described in clause 8.8.3.7, where T-EAS in that procedure is assumed to be CAS. Based on the received CAS information, the S-EES informs the CAS with the S-EES endpoint information by selected EES declaration request as described in clause 8.8.3.10.

5. Based on the CAS selection information received from the S-EAS, the S-EES sends the target information notification to the EEC as described in clause 8.8.3.5.3.

6. The S-EAS transfers the application context to the CAS selected in step 3. This process is out of scope of the present specification.

NOTE 1: The S-EAS or CAS can further decide to terminate the ACR, and the CAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and CAS whether and how to make such a decision.

Phase IV: Post-ACR Clean up

7. Same as step 8 described for figure 8.8.2.4-1.

8. Same as step 10 described for figure 8.8.2-1.

NOTE 2: The CAS can perform capability exposure subscription with 3GPP CN directly, upon receiving the application context, which may be helpful for handling future ACR scenarios e.g. ACR from cloud to edge.

8.8.2A.5 Enabling ACR with CAS - S-EES executed ACR

Figure 8.8.2A.5-1 illustrates the S-EES detecting, deciding and executing ACR from the S-EAS to the CAS. This may include EELManagedACR by S-EES when initiated by S-EAS as per clause 8.8.3.6.

This scenario description is same as described for figure 8.8.2.5-1 except for the following clarifications:

Pre-conditions: Same pre-conditions apply described for figure 8.8.2.5-1, with the clarification that T-EAS is CAS and pre-condition 5 for EELManagedACR is not applicable.

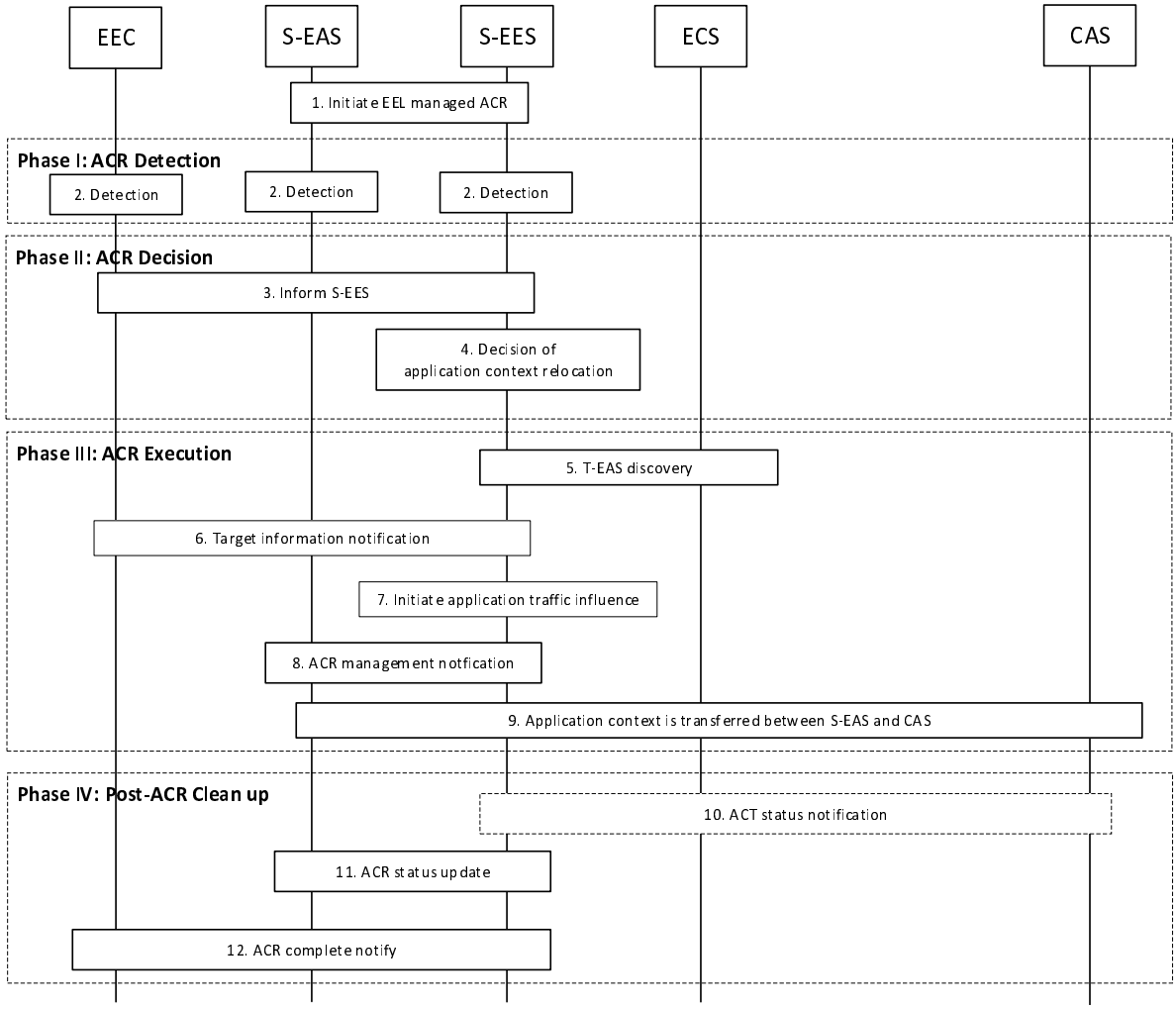

Figure 8.8.2A.5-1: Enabling ACR with CAS - S-EES executed ACR

1. Same as step 1 described for figure 8.8.2.5-1.

Phase I: ACR Detection

2. Same as step 2 described for figure 8.8.2.5-1.

Phase II: ACR Decision

3. Same as step 3 described for figure 8.8.2.5-1.

4 Same as step 4 described for figure 8.8.2.5-1.

Phase III: ACR Execution

5. The S-EES determines the targets via the Discover T-EAS procedure in clause 8.8.3.2.

   If T-EAS discovery fails, then S-EES triggers DNS query message using the endpoint information (e.g., FQDN) in the S-EAS profile (e.g., EASID).

   Based on the determination of CAS, the S-EES informs the CAS with the S-EES endpoint information by selected EES declaration request as described in clause 8.8.3.10. For EELmanagedACR, the CAS subscribe to S-EES to receive ACT status notifications.

6. Same as step 7 described for figure 8.8.2.5-1.

7. The S-EES may apply the AF traffic influence with the N6 routing information of the CAS in the 3GPP Core Network (if applicable).

8. The S-EES sends the ACR management notification (e.g. as notification for "ACR facilitation" event or "ACT start" event as described in clause 8.6.3 or due to step 1) to the S-EAS to initiate ACT between the S-EAS and the CAS.

9. The Application Context is transferred from S-EAS to the CAS at implementation specific time. In the case of EELManagedACR, the S-EES accesses the Application Context from the address as per step 1 and the S-EES either engage in the ACT from S-EAS to the CAS (obtained as per step 5) in a secure way. Further the CAS accesses the Application Context. The S-EAS may also perform the ACT directly with CAS, the specification of such process is out of scope of the present document.

NOTE 1: The Application Context is encrypted and protected by the application layer. The S-EES engages in the packet level transport of the Application Context and has no visibility to the content of the Application Context.

NOTE 2: The S-EAS or CAS can further decide to terminate the ACR, and the CAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and CAS whether and how to make such a decision.

Phase IV: Post-ACR Clean up

10. Same as step 11 described for figure 8.8.2.5-1.

11. Same as step 12 described for figure 8.8.2.5-1.

12. If the status in step 11 indicates a successful ACT, the S-EES sends the ACR information notification (ACR complete) message to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3.

NOTE 3: The Application Client mechanism to support switchover of the application traffic to CAS is out of scope of the specification.

8.8.2A.6 CAS decided ACR scenario via last S-EES

In this scenario, the CAS detects the need for ACR and makes the decision about whether to perform the ACR and starts the ACR at a proper time.

During the ACR execution phase, the CAS may need to determine an EES in the service area of the EEC before continuing with T-EAS discovery. The CAS may send the EAS discovery request to the S-EES that selects an appropriate T-EES and T-EAS as per clause 8.8.3.2 where the CAS acts as a S-EAS.

Pre-conditions:

- The CAS has a business relationship with the ECSP, otherwise, the EES will reject the CAS request during authorization.
- Prior to being connected to the CAS, the EEC was connected to an S-EES that may still hold its context and the CAS knows the S-EES (e.g. as in clause 8.8.3.10 when ACR is performed from EAS to CAS).
- AC has obtained the UE ID as per clause 8.14.2.6 and forwarded it to the CAS while performing ACR from EAS to CAS as described in clause 8.8.2A.1 or the CAS knows UE ID having used the procedure defined in clause 8.6.5.

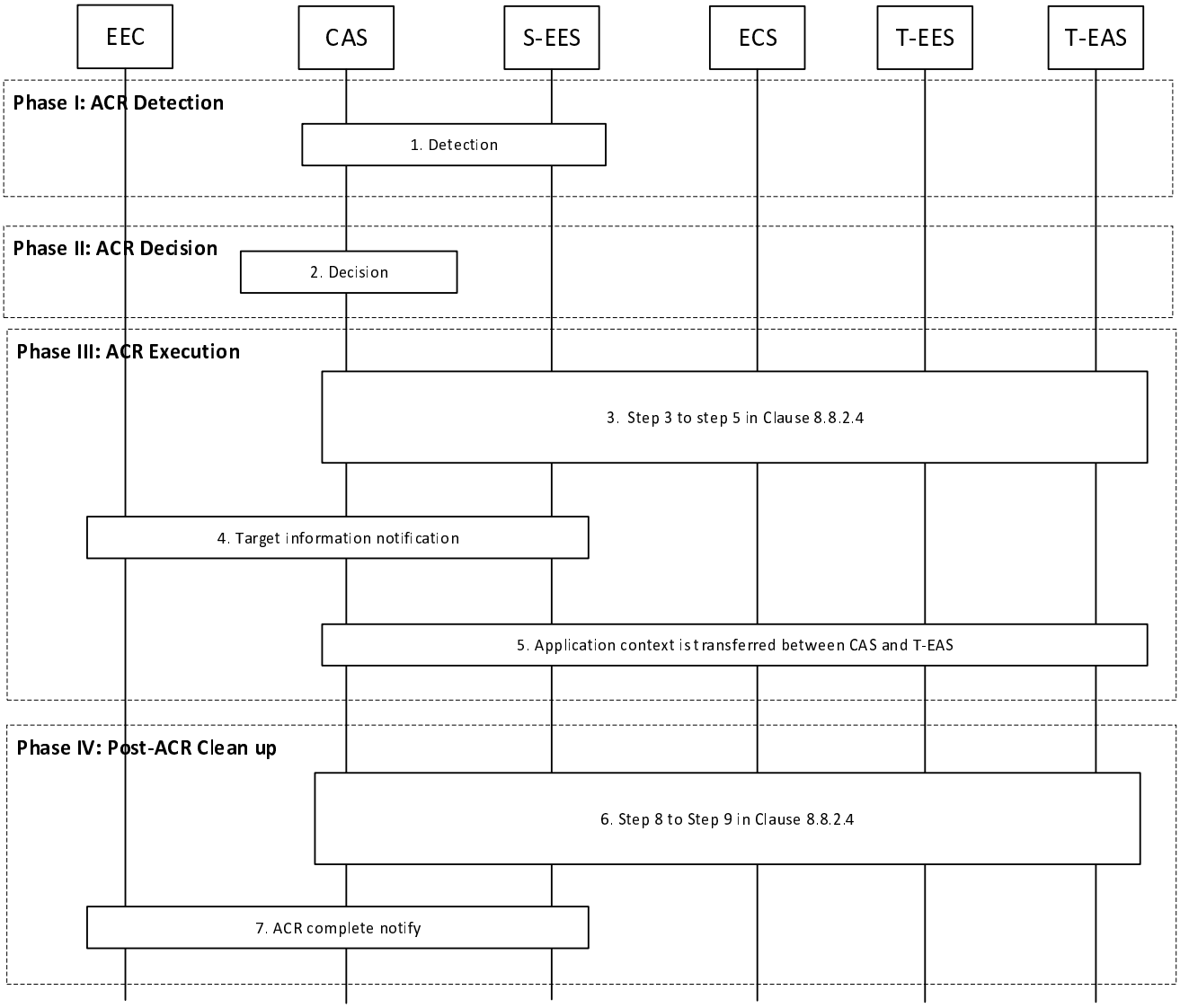

Figure 8.8.2A.6-1: CAS decided ACR with T-EAS Discovery via S-EES

Phase I: ACR Detection

1. The CAS detects the need for ACR. The CAS either receives ACR management notifications from S-EES indicating that ACR may be required ("ACR monitoring" event), or self detects the need for ACR (e.g. upon receipt of a "user plane path change" event).

Phase II: ACR Decision

2. The CAS makes the decision to perform the ACR.

Phase III: ACR Execution

3. Same as steps 3 to 5 in clause 8.8.2.4 where the CAS acts as an S-EAS and it may provide the UE ID in the T-EAS discovery request for the S-EES to identify the UE during discovery. If ACR monitoring event is used in step 1, the T-EAS discovery in step 3 of clause 8.8.2.4 is skipped by the CAS.

4. If the S-EES can communicate with the EEC, step 6 from clause 8.8.2.4 is performed to notify the EEC of the selected T-EES. Otherwise, the notification is sent to the EEC via the SEAL notification management service as described in clause 9.1 if the EEC has subscribed to receive notifications from the S-EES or via Application Triggering via core network.

5. Same as step 7 in clause 8.8.2.4 where the CAS acts as an S-EAS.

Phase IV: Post-ACR Clean up

6. Same as step 8 to step 9 in clause 8.8.2.4 where the CAS acts as an S-EAS.

7. If the S-EES can communicate with the EEC, step 10 from clause 8.8.2.4 is performed. Otherwise, the notification is sent to the EEC via the SEAL notification management service as described in clause 9.1 if the EEC has subscribed to receive notifications from the S-EES or via Application Triggering via core network.

8.8.2B Scenarios for ACR between EAS and CAS with CES

8.8.2B.1 General

Since the EAS may have service area restriction, once the UE is moving out of the current edge coverage, to keep service continuity, the application client needs to communicate with the CAS. The ACR can also be triggered in case of an overload situation or maintenance aspects in the S-EAS or EDN if no suitable target EAS is found as described in clause 8.8.1.1 depending on the scenario. Service continuity between CAS and EAS is supported with CES, corresponding to the architecture options described in clause 6.2d.

CAS(s) are registered in the CES via CLOUD-1 reference point which enables the CES to provide appropriate CAS to S-EAS or S-EES.

DNS can be used for CAS discovery by the UE.

The EES of the source EDN may interact with the CES via ECI-4 reference point and application context is transferred from source EAS to the CAS. Later, if the UE is moving to an area with edge coverage, the CES may interact with the EES in the target EDN via ECI-4 reference point and application context is transferred from the CAS to target EAS.

8.8.2B.2 ACR from edge to cloud

8.8.2B.2.1 General

The following clauses describe ACR scenarios from edge to cloud.

8.8.2B.2.2 Initiation by EEC using regular EAS Discovery

The scenario described in clause 8.8.2A.2 applies with the following differences:

- After step 7, the S-EES relocates context to the CES. The relocation procedure re-uses the procedure described in clause 8.9.2.3 where T-EES is replaced by CES.

- During post-ACR clean up, the CAS triggers ACR status update towards the CES in order to finish ACR.

8.8.2B.2.3 EEC executed ACR via S-EES

The scenario described in clause 8.8.2A.3 applies with the following differences:

- After step 4, the S-EES relocates context to the CES. The relocation procedure re-uses the procedure described in clause 8.9.2.3 where T-EES is replaced by CES.

- During post-ACR clean up, the CAS triggers ACR status update towards the CES in order to finish ACR.

8.8.2B.2.4 S-EAS decided ACR

The scenario described in clause 8.8.2.4 applies with the following differences:

- The CES replaces the T-EES and the CAS replaces the T-EAS.

8.8.2B.2.5 S-EES executed ACR

The scenario described in clause 8.8.2.5 applies with the following differences:

- The CES replaces the T-EES and the CAS replaces the T-EAS.

8.8.2B.3 ACR from cloud to edge

8.8.2B.3.1 General

The following clauses describe ACR scenarios from cloud to edge.

8.8.2B.3.2 Initiation by EEC using regular EAS Discovery

The scenario described in clause 8.8.2.2 applies with the following differences:

- The CES replaces the S-EES and the CAS replaces the S-EAS.
- The EEC subscribes to ECS with service provisioning subscription for ACR detection and service provisioning in step 3 is skipped.

8.8.2B.3.3 EEC executed ACR via CES

The scenario described in clause 8.8.2.3 applies with the following differences:

- The CES replaces the S-EES and the CAS replaces the S-EAS.
- The EEC subscribes to ECS with service provisioning subscription for ACR detection and service provisioning in step 3 is skipped.

8.8.2B.3.4 CAS decided ACR

The scenario described in clause 8.8.2.4 applies with the following differences:

- The CES replaces the S-EES and the CAS replaces the S-EAS.
- The CAS subscribes to CES with ACR management events with "ACR monitoring" for ACR detection and step 3 T-EAS discovery is skipped.

8.8.2B.3.5 CES executed ACR

The scenario described in clause 8.8.2.5 applies with the following differences:

- The CES replaces the S-EES and the CAS replaces the S-EAS.
- The ACR is only detected by the CES. The CAS subscribes to CES with ACR management events with "ACR facilitation" for ACR detection and step 5a T-EAS discovery is skipped.

NOTE: Detection by other entities is not specified in this release.

8.8.3 Procedures

8.8.3.1 General

8.8.3.2 Discover T-EAS

Figure 8.8.3.2-1 illustrates the procedure for fetching T-EAS information. This procedure may be utilized by a S-EAS, which undertakes the transfer of application context information to a T-EAS directly, or can be invoked by the S-EES itself on deciding to execute ACR.

T-EAS discovery procedure also supports EAS retrieval which enables a S-EAS to obtain T-EAS(s) serving the application group so that the S-EAS can start communication with obtained EAS(s) for EAS synchronization.

Pre-conditions:

1. Information related to the EES is available with the S-EAS, if the procedure is triggered by the S-EAS.

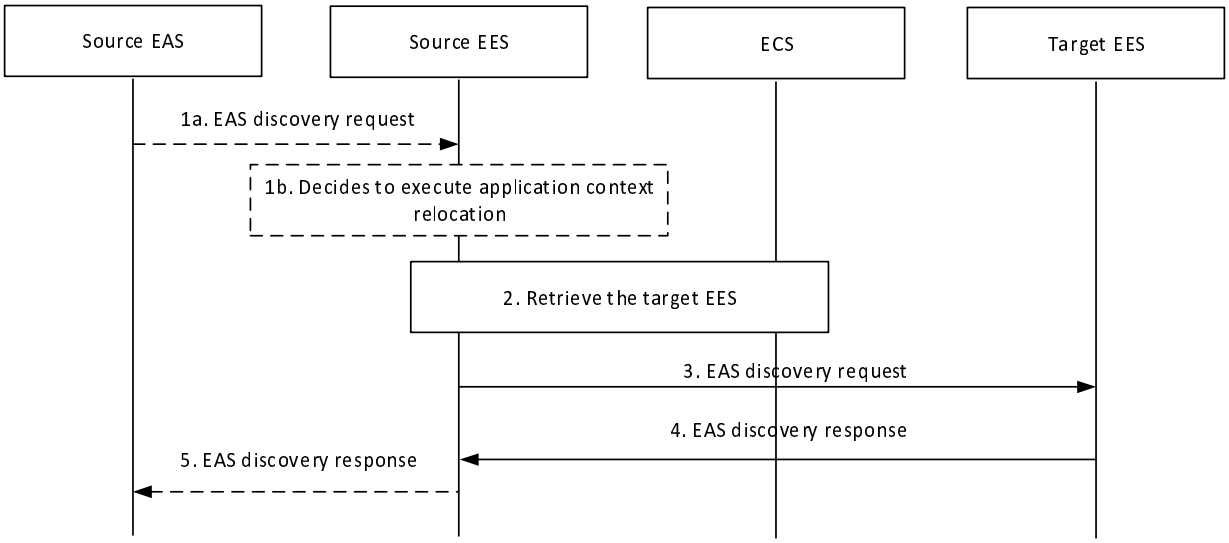

Figure 8.8.3.2-1: Discover T-EAS

1a. The S-EAS sends the EAS discovery request to the S-EES or the S-EES decides to execute the ACR. The EAS discovery request from the S-EAS includes the requestor identifier [EASID] along with the security credentials and includes EAS discovery filter matching its EAS profile. If target DNAI is available at the S-EAS via User Plane Path change event, the S-EAS provides the S-EES with the target DNAI. The S-EAS also includes an EAS service continuity support indicator indicating that the S-EAS decided ACR according to clause 8.8.2.4 is to be used for the ACR. The S-EAS includes the bundle ID and bundle type indicating the proxy bundle case to which the S-EAS belongs to. The request may include prediction expiration time.

The EAS may send EAS discovery request with EAS ID, Application Group ID and EAS synchronization support, which indicates the request to obtain EAS(s) currently serving the Application Group ID with the requested EAS ID in order to perform EAS synchronization.

NOTE 1: The trigger condition to invoke the Discover T-EAS API is up to application service logic, which is out of scope of this specification.

1b. The S-EES either receive the target DNAI for T-EES discovery from the step 1a or by the user plane management event notification from the core network.

2. If the request is received from the S-EAS, the S-EES checks whether the requesting EAS is authorized to perform the discovery operation.

If Application Group ID and EAS synchronization support in EAS characteristics are received and the ECS-ER is available, the S-EES checks with the ECS-ER with the received EAS ID and Application Group ID and obtains a list of EAS(s) supporting EAS synchronization and serving the application group for the desired application service identified by the EAS ID as described in clause 8.20. Step 2 to step 4 are skipped.

If the UE location is not known to the S-EES or provided by the S-EAS request, then the S-EES may interact with 3GPP core network to retrieve the UE location. If the S-EES decided to execute the ACR or when the requesting EAS is authorized, the S-EES checks if there exists a T-EAS information (registered or cached) that can satisfy the requesting EAS information, additional query filters and the Expected AC Service KPIs and the Minimum required AC Service KPIs if received from the EEC during the EAS discovery or from the S-EAS in step 1. In this case, the S-EES may collect Edge load performances from ADAES or OAM to find T-EAS(s) that satisfies the Expected AC service KPIs or the Minimum required AC Service KPIs. The S-EES may determine the use of statistics or prediction for evaluating KPIs based on the situation of the T-EAS discovery. If the S-EES finds the T-EAS(s) in the cached or registered information, the flow either continues with step 5 for the S-EAS triggered discovery or stops for the S-EES decided ACR execution, else the S-EES retrieves the T-EES address from the ECS as specified in clause 8.8.3.3 and continues with step 3.

3. The S-EES invokes the EAS discovery request on the T-EES retrieved from the ECS. The EAS discovery request includes the requestor identifier [EESID] along with the security credentials and includes EAS discovery filter. In the EAS discovery filter, the S-EES may include prediction expiration time, the Expected AC Service KPIs and the Minimum required AC Service KPIs if received from the EEC during the EAS discovery or from the S-EAS in step 1.

   The S-EES also includes the EEC service continuity support indicator received from the EEC during EAS discovery. If in step 1 the S-EES received an EAS service continuity support indicator from the S-EAS, then the S-EES includes this EAS service continuity support indicator and its own EES service continuity support indicator indicating the ACR scenarios supported by the EES. If in step 1 the S-EES decided to execute the ACR, the S-EES includes the EAS service continuity support indicator received from the S-EAS during EAS registration and includes an EES service continuity support indicator indicating that the S-EES executed ACR according to clause 8.8.2.5 is to be used for the ACR.

   Upon receiving the request, the T-EES may trigger the ECSP management system to instantiate the T-EAS that matches with EAS discovery filter IEs (e.g. ACID) as in clause 8.12.

4. The T-EES discovers the T-EAS(s) and responds with the discovered T-EAS information to the S-EES. To filter T-EAS(s), the T-EES utilizes the discovery filters (e.g. Expected AC Service KPIs and the Minimum required AC Service KPIs) and the indications which ACR scenarios are supported by the AC, the EEC, the T-EES and the S-EAS. If T-EES gets the Expected AC service KPIs or the Minimum required AC Service KPIs, the T-EES may collect edge load analytics from ADAES (as specified in clause 8.8.2 of TS 23.436 [28]) or performance data from OAM to find T-EAS(s) that satisfies the Expected AC service KPIs or the Minimum required AC Service KPIs. The T-EES may determine the use of statistics or prediction for evaluating KPIs based on the situation of the T-EAS discovery. The S-EES may cache the T-EAS information.

   When the bundle EAS information (i.e. list of EASID) is provided and the bundle type indicating the direct bundle, and the S-EES received associated T-EES(s) along with part of EAS ID list in the step2 from the ECS, then the S-EES discover the target direct bundle EAS(s) which belongs to same EDN for all the associated S-EES(s). The request message contains direct bundle EAS(s) information (i.e. list of EASID and direct bundle type), then the T-EES determines the direct bundle T-EAS(s) based on the bundle EAS information (e.g. list of EASIDs). Then the S-EES receives the direct bundle T-EAS(s) information from each associated T-EES(s).

NOTE 2: T-EES(s) may belongs to same EDN.

NOTE 3: The edge load analytics from ADAES can be either statistics or predictions on the T-EAS.

NOTE 4: The statistical KPI value can be used for both normal ACR and service continuity planning.

5. If the request was received from the S-EAS, the S-EES responds to the S-EAS with the discovered T-EAS Information.

   For responding S-EAS requesting EAS serving the application group, only EAS endpoint and EAS ID are included in EAS profile of Discovered EAS list.

8.8.3.3 Retrieve T-EES procedure

Figure 8.8.3.3-1 illustrates the procedure for the S-EES to retrieve the T-EES information from the ECS. This procedure is also applicable for the CES to retrieve the T-EES information.

Pre-condition:

1. The S-EES has been pre-configured with the address of the ECS; and
2. The AC at the UE already has on-going application traffic with the S-EAS.

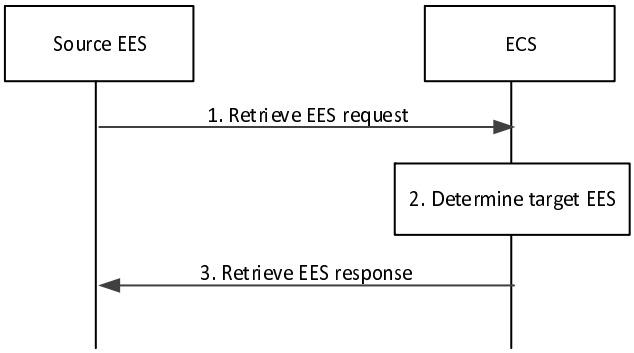

Figure 8.8.3.3-1: Retrieve T-EES procedure

1. The S-EES sends the Retrieve EES request (UE location information or UE identity, EASID of the S-EAS, bundle ID, bundle type (i.e. proxy bundle case), target DNAI and UE connectivity information) to the ECS in order to identify the T-EES which has an EAS available to serve the given AC in the UE. For obtaining announcement EES list, the Retrieve EES request includes application group id. The request message may also contain the AC, EEC service continuity support information.

2. If the request contains the UE identity (e.g. GPSI) but the UE location is not known to the ECS, then the ECS interacts with 3GPP core network to retrieve the UE location. The ECS determines T-EES(s) as per the parameters (e.g. EASID, target DNAI) in the request and the UE location information. If the request message contains the AC, EEC service continuity support information, then the ECS may identify the T-EES taking the AC, EEC, T-EES service continuity support into consideration. When the bundle ID and is provided and bundle type indicating the proxy bundle case then the ECS can identify the T-EES based on the bundle ID in the EES profile and in the request message to ensure T-EAS is able to invoke the required proxy bundle EAS(s) as the S-EAS does.

   If no ECS-ER is available and when the Retrieve EES request includes application group id to the ECS then the request EES list retrieval is for the announcement of common EAS, ECS determines the list of EESs serving the EASs (with same EASID) for the Group ID included in the Retrieve EES request.

   If the ECS does not identify any suitable EES(s) based on EDN configuration available at the ECS and UE's location, the ECS determines a partner ECS that may satisfy the requirements. Based on ECSP policy, the ECS may use preconfigured or OAM configured information about the partner ECSs or ECS discovery via ECS-ER as specified in clause 8.17.2.3 or both.

   If required by the ECSP policies, the ECS may use service provisioning information retrieval procedure as specified in clause 8.17.2.4 to obtain service provisioning information from the partner ECS.

   When the bundle EAS information is provided, then if bundle EAS information includes a list of EASIDs, then the ECS identifies the one or more T-EES associated with the same EDN which support all of the EASs within the same EDN based on the EES EDN information obtained in the EES profile and bundle EAS information (e.g. list of EASIDs).

NOTE 1: T-EES(s) may belongs to same EDN.

3. The ECS sends the Retrieve EES response. If the ECS has determined the EDN configuration information, the retrieve EES response includes the list of EDN configuration information to the S-EES. The list of EDN configuration information includes the EDN details with the endpoint information of T-EES(s) as described in table 8.3.3.3.3-2. If the ECS has determined suitable partner ECS(s) instead, the retrieve EES response includes a list of ECS configuration information.

   The ECS may provide associated T-EES(s) information (one or more T-EES information) to the S-EES in the Retrieve T-EES response along with the bundle EAS information (i.e. list of EASIDs). When S-EES receives multiple associated T-EES(s), then each associated T-EES information is provided along with the part of the EAS ID list.

If the retrieve EES response contains a list of ECS configuration information, the S-EES may initiate retrieve T-EES procedure with one or more ECS(s) listed in the retrieve EES response.

NOTE 2: The Retrieve EES request initiated by the S-EES can be restricted only to its registered ECS.

8.8.3.4 ACR launching procedure

Figure 8.8.3.4-1 illustrates the ACR launching procedure by the EEC or the S-EAS or the S-EES.

If this procedure is triggered by the EEC, depending on the ACR action indicated in the ACR request, the procedure is used for ACR initiation, ACR determination or ACR modification which is described in clause 8.8.1.4. The procedure of the ACR initiation can be re-sent as described in clause 8.8.1.3 to cancel an ACR.

If this procedure is triggered by the S-EAS, the procedure is used for ACR determination.

If this procedure is triggered by the S-EES to the associated S-EES(s), this procedure is used for the direct bundle EAS case.

Pre-condition:

For EEC as consumer:

1. The EEC has been authorized to communicate with the EES as specified in clause 8.11, if the procedure is triggered by the EEC.

For S-EAS as consumer:

1. Information related to the S-EES is available with the S-EAS.

For EES as consumer:

1. The S-EES obtained the associated S-EES(s) information as specified in clause 8.15.2.2.

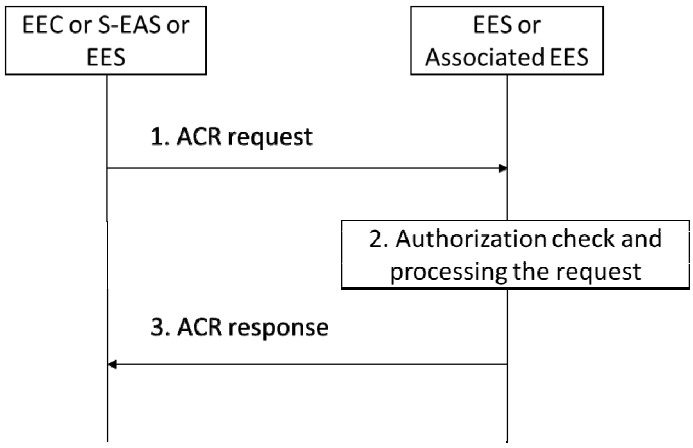

Figure 8.8.3.4-1: ACR launching procedure

1. The EEC or the S-EAS sends an ACR request message to the EES in order to start ACR. The ACR request message may include Predicted/Expected UE location or Expected AC Geographical Service Area to indicate that the EES should detect whether the UE has moves to the Predicted/Expected UE location or Expected AC Geographical Service Area or not in ACR clean-up phase. The ACR request message includes ACR action to indicate either ACR initiation request or ACR determination request. If the procedure is triggered by the S-EAS, the ACR request message is only for ACR determination.

   An ACR request for ACR initiation sent by the EEC:

   - includes an indication of whether the EEC requests the EES to perform EAS notification; and

- provides information used by EES to perform AF traffic influence as in 3GPP TS 23 501 [2].The EEC sent ACR request for ACR initiation shall include the simultaneous EAS connectivity information in service continuity (see table 8.8.4.4-1) if previously received as part of the AC profile.

An ACR request for ACR determination sent either by the EEC or the EAS informs the EES that the need for ACR has been detected by the requestor.

An ACR request for ACR modification sent by the EEC:

- includes IDs to identify the ACR that is requested to be modified; and
- includes the ACR parameters to be modified.

An ACR request for direct bundle EAS case sent by the S-EES:

- includes direct bundle T-EAS(s) received in step 4 in 8.8.3.2 related to the associated S-EES(s) based on the EASID, which EASID of the associated S-EES is corresponding to the direct bundle T-EAS(s) profile.

2. The EES checks if the requestor is authorized for this operation. If authorized, the EES processes the request and performs the required operations.

If the request in step 1 is for ACR initiation:

- the EES may use information provided in the request to apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable), as described in 3GPP TS 23.501 [2], clause 5.6.7.1; and

NOTE 1: The simultaneous EAS connectivity information sent by EES is used to maintain both S-PSA and T-PSA in supporting simultaneous connectivity with both S-EAS and T-EAS during the service continuity as described in clause 6.3.4 of 3GPP TS 23.548 [20].

NOTE 2: The EES acting as AF cannot be aware of if it is supported before invoking AF traffic influence API. If the EES is notified from the 3GPP CN that the simultaneous EAS connectivity is not supported as described in 3GPP TS 23.502 [3] during the invocation procedure of AF traffic influence API, then the EES can know that the simultaneous EAS connectivity is not supported and provide the response indicating simultaneous EAS connectivity unsupported to the EAS or EEC.

- if the EAS notification indication in ACR initiation data is provided in the step 1 request and the EAS has subscribed to receive such notification, the EES shall notify the EAS indicated in the ACR initiation data about the need to start ACR by sending an ACR management notification for the "ACT start" event, as described in clause 8.6.3.

If the request in step 1 is for ACR determination, the EES decides to execute ACR as described in clause 8.8.2.5.

If the request in step 1 includes Previous T-EAS Endpoint:

- if the previous EAS notification indication is provided in the step 1 request and the EAS has subscribed to receive such notification, the EES shall notify the EAS about the cancellation of the ACR with the previous T-EAS by sending an ACR management notification for the "ACT stop" event, as described in clause 8.6.3.
- The EAS will inform the remote EAS about application context cancellation, which is outside the scope of this specification. The T-EAS sends the ACR status update message to the T-EES which will include failed result with an appropriate cause indicating the reason for the failure.

If the request in step 1 is for ACR modification:

- the EES identifies the ACR to be modified based on the ID parameters in the request in step 1. If the request in step 1 is to the S-EES, the S-EES performs the ACR parameter information procedure as described in clause 8.8.3.9. If the request in step 1 is to the T-EES, and if the T-EAS has subscribed to receive ACR notifications, the T-EES shall notify the T-EAS by sending an ACR management notification, with "ACT start" event including ACR parameters from the request in step 1, e.g. Prediction expiration time.

If the request in step1 is for direct bundle EAS case, then the associated T-EES may use received direct bundle T-EAS(s) for ACR.

3. The EES responds to the requestor's request with an ACR response message.

In case of re-sending ACR initiation, if serving EES was changed and EEC context was relocated, the T-EES can clean up any relocated EEC context either indicated in the re-sent ACR request for scenario described in clause 8.8.2.6 or upon reception of the ACR status update with failed result from T-EAS for other scenarios.

8.8.3.5 ACR information subscription

8.8.3.5.1 General

Clause 8.8.3.5.2 and clause 8.8.3.5.3 together illustrate the ACR information procedure based on Subscribe/Notify model.

The ACR information procedure is utilized as a building block for a part of Post-ACR Clean up in clause 8.8.2 and Target information notification.

8.8.3.5.2 Subscribe

Figure 8.8.3.5.2-1 illustrates the ACR information subscription procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has received information (e.g. URI, IP address) related to the EES;
2. The EEC has received appropriate security credentials authorizing it to communicate with the EES as specified in clause 8.11; and
3. The EEC has optionally acquired a Notification Target Address to be used in its subscriptions to notifications.

NOTE: How the EEC acquires the notification target address or a notification channel URI to receive the notifications is out of scope of this release. The notification target address can terminate at the EEC (e.g. in an IoT device) if the deployment supports EEC reachability, or it can terminate at a push notification service. Details of the push notification service are out of scope of this release.

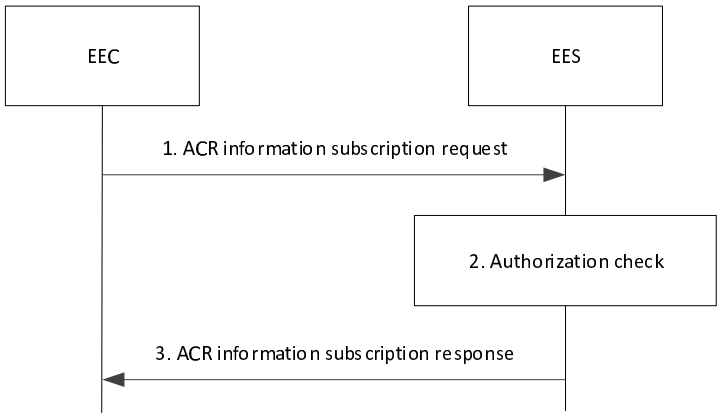

Figure 8.8.3.5.2-1: ACR information subscription

1. The EEC sends an ACR information subscription request to the EES. The request from EEC may include the ACIDs to indicate to the EES which ACs are served by the EEC that need to receive ACR information via EEL.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to subscribe ACR information about the requested EAS(s). If the request is authorized, the EES creates and stores the subscription for ACR information.
3. The EES sends an ACR information subscription response to the EEC, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EEC shall send an ACR information subscription update request prior to the expiration time. If

an ACR information subscription update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly unsubscribed.

8.8.3.5.3 Notify

Figure 8.8.3.5.3-1 illustrates the ACR information notification procedure between the EEC and the EES, which can be used by the EES to notify the EEC of the following:

- target information, i.e. the details of the selected T-EAS and, if required, the selected T-EES, during ACR as described in clauses 8.8.2.4 and 8.8.2.5;

NOTE: The T-EAS and T-EES information can be used to determine the PDU session(s) to provide connectivity to the T-EAS and the T-EES. If the ACR does not require change in EES, i.e. T-EES is same as S-EES, then the T-EES information can be skipped.

- ACR complete events.

Pre-conditions:

1. The EEC has subscribed with the EES for the ACR information as specified in clause 8.8.3.5.2.

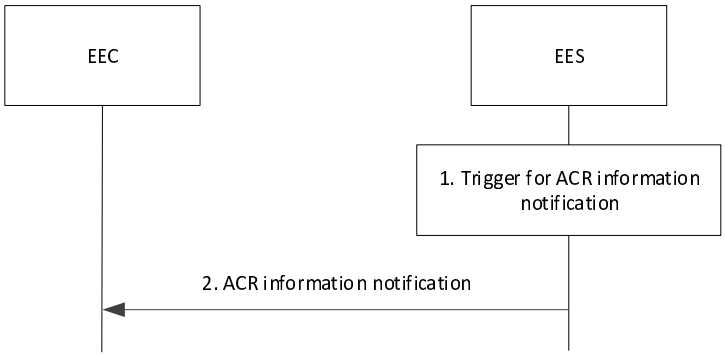

Figure 8.8.3.5.3-1: ACR information notification

1. An event (e.g. ACR complete, or Target information notification) occurs at the EES that satisfies trigger conditions for providing ACR information to a subscribed EEC.

2. The EES sends an ACR information notification to the EEC with the ACR information determined in step 1. The ACR information notification may include ACID to indicate the application context relocation of the AC is complete. If the S-EES has received the successful EEC Context Push response from T-EES, along with registration ID and the registration expiration time in the EEC Context Push relocation procedure, then the ACR information notification towards EEC also includes the registration ID and registration expiration time under EEC context relocation status (for successful status). Upon receiving the target information notification to indicate start of the ACR execution, the EEC avoids triggering a second ACR execution for the same ACR identity (ACID, UE ID, S-EAS endpoint and T-EAS endpoint) until the current ACR execution is completed.

   If during the ACR the EES has received the successful EEC Context Push response from the T-EES and the EEC Context Push response includes T-EES selected ACR scenario list in the EEC Context Push relocation procedure, then the ACR information notification towards the EEC includes the list from T-EES as the selected ACR scenario list under EEC context relocation status (for successful status). Upon receiving the ACR complete notification, if the selected ACR scenario list is not available (for successful status), the EEC may either select ACR scenario considering the supported ACR scenarios of AC, EEC, T-EES and T-EAS or request T-EES to select list of ACR scenarios as specified in clause 8.15.

   After the ACR complete notification with successful ACR, if the ACR complete notification indicates that EEC context relocation has failed the EEC can trigger EAS Information provisioning procedure to perform a re-selection of the ACR scenarios.

If EEC context does not exist, after the ACR complete notification with successful ACR, the EEC can trigger EAS Information provisioning procedure to select the ACR scenarios.

8.8.3.5.4 Subscription update

Figure 8.8.3.5.4-1 illustrates the ACR information subscription update procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the ACR information as specified in clause 8.8.3.5.2.

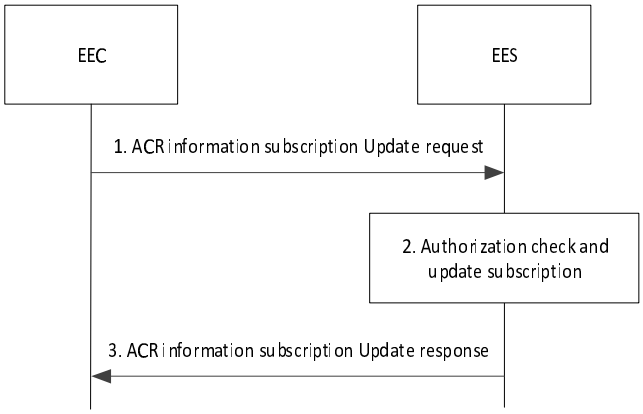

Figure 8.8.3.5.4-1: ACR information subscription update

1. The EEC sends an ACR information subscription update request to the EES.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized for the operation. If authorized, the EES updates the subscription.
3. The EES sends an ACR information subscription update response to the EEC.

8.8.3.5.5 Unsubscribe

Figure 8.8.3.5.5-1 illustrates the ACR information unsubscribe procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the ACR information as specified in clause 8.8.3.5.2.

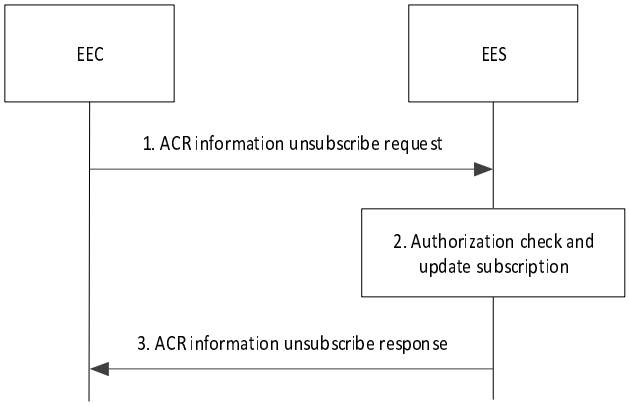

Figure 8.8.3.5.5-1: ACR information unsubscribe

1. The EEC sends an ACR information unsubscribe request to the EES.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized for the operation. If authorized, the EES terminates the subscription of the EEC.
3. The EES sends an ACR information unsubscribe response to the EEC.

8.8.3.6 EELManagedACR procedure

8.8.3.6.1 General

This clause introduces a procedure for ACR performed by the Edge Enabler Servers.

When S-EES receives a request for EELManagedACR from S-EAS, the S-EES performs the service operations for the service continuity including detecting the event which may trigger the ACR, making the ACR decision, discovering the T-EAS, accessing and transferring the Application Context to the T-EES/T-EAS, notifying the T-EAS about the available Application Context, notifying the 3GPP network about ACR information, notifying the EEC about the T-EAS information (as per EEC subscription).

The EELManagedACR procedure is designed as an asynchronous operation wherein the S-EES will generate notifications (e.g. failure of any ACR related operation) to the S-EAS while performing the ACR operations.

8.8.3.6.2 Procedure

8.8.3.6.2.1 General

This clause describes the procedures for S-EAS to request for EELManagedACR and for T-EAS to subscribe for ACT status notification.

8.8.3.6.2.2 ACR request

Figure 8.8.3.6.2.2-1 illustrates the procedure for EELManagedACR performed by the Edge Enabler Servers.

Pre-conditions:

1. Information related to the S-EES is available with the S-EAS.
2. The T-EAS has subscribed to the ACR related event from the T-EES.
3. The EEC has subscribed to the ACR related event from the S-EES.

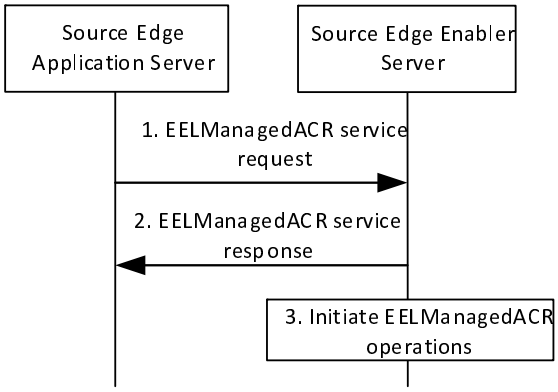

Figure 8.8.3.6.2.2-1: ACR procedure

1. The S-EAS sends an EELManagedACR service request (UE identifier, EAS characteristics for ACR) to request the S-EES to handle all the service operations of the ACR. The S-EAS may initiate this request with S-EES based on different triggers (e.g. when Application Client is connecting to the S-EAS). An address for accessing the Application Context may be provided if available, which allows the S-EES to access the Application Context generated by the S-EAS for ACT.

2. The S-EES checks whether the requesting EAS is authorized to perform the operation. If it is authorized, the S-EES responds with an EELManagedACR service response. If no address for accessing Application Context is provided by S-EAS in step 1, then the S-EES provides an address for storing the Application Context by S-EAS.

NOTE: How the EES accesses the Application Context related to the EAS from the address of the Application Context storage is up to implementation and outside the scope of the present document.

3. The S-EES determines the EELManagedACR operations to be executed as specified in clause 8.8.2.5.

8.8.3.6.2.3 ACT status subscription

Figure 8.8.3.6.2.3-1 illustrates the procedure for T-EAS to subscribe for ACT status during EELManagedACR.

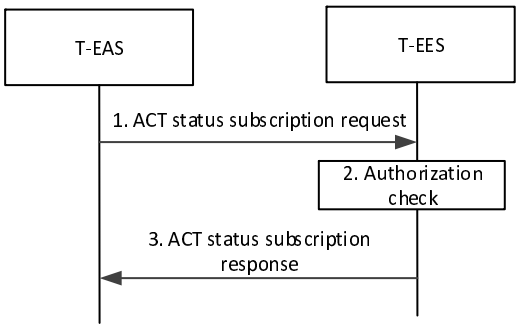

Figure 8.8.3.6.2.3-1: ACR procedure

1. The T-EAS sends an ACT status subscription request to the T-EES.

2. The T-EES checks whether the requesting T-EAS is authorized to perform the operation. If it is authorized, the T-EES creates the subscription.

3. The T-EES responds with the ACT status subscription response

8.8.3.6.2.4 ACT status notification

Figure 8.8.3.6.2.4-1 illustrates the procedure for T-EES to notify the T-EAS about the status of ACT during EELManagedACR.

Pre-conditions:

1. ACT between the S-EES and T-EES has been completed.

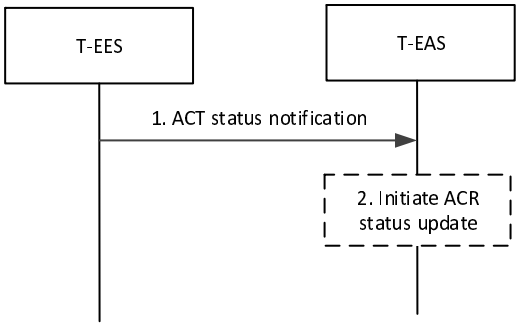

Figure 8.8.3.6.2.4-1: ACR procedure

1. The T-EES sends ACT status notification to the T-EAS, notifying about the status of the ACT between the Application Context received from the S-EES.
2. On receiving a notification about successful ACT, the T-EAS may initiate the ACR status update procedure as described in clause 8.8.3.8.

8.8.3.7 Selected T-EAS declaration

Figure 8.8.3.7-1 illustrates the interactions between the S-EAS and the S-EES for the selected T-EAS declaration.

Pre-conditions:

1. The S-EAS has discovered and selected the T-EAS as described in clause 8.8.3.2.

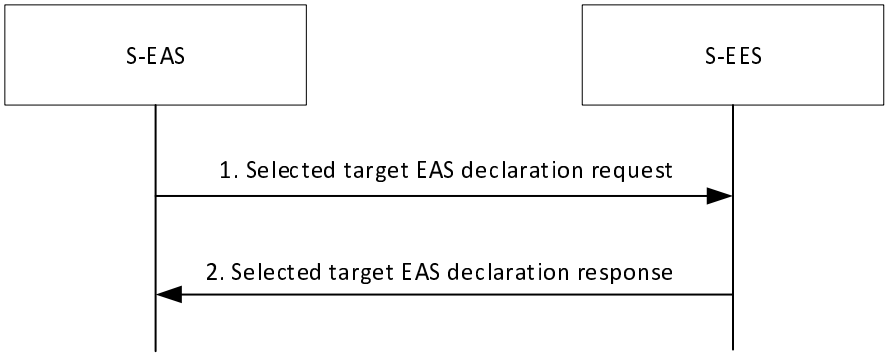

Figure 8.8.3.7-1: Selected target EAS declaration procedure

1. The S-EAS sends Selected target EAS declaration request message to the S-EES. The request includes the information of the selected T-EAS and may include ACID to indicate which AC the T-EAS is intended for.
2. The S-EES checks whether the requesting EAS is authorized to perform operation. If authorized, the S-EES responds to the received request with Selected target EAS notification declaration response message. The S-EES also determines the selected T-EES based on the declared T-EAS selection, then S-EES checks whether the EEC (serving the ACs) has subscribed for ACR related information.

8.8.3.8 ACR status update procedure

Figure 8.8.3.8-1 illustrates the procedure for ACR status update, which is triggered by the S-EAS or the T-EAS. In the post-ACR clean up phase of service continuity scenarios described in clause 8.8.2, this procedure may be used by EAS to indicate the status of ACT to their registrar EESs; or used by the T-EAS to update the notification target address and allow the T-EES to indicate the status of EDGE-3 subscription relocation to the T-EAS including subscription ID update for EDGE-3 subscriptions; or both.

Pre-condition:

1. The ACT procedure between the S-EAS and the T-EAS is either successfully completed or failed.

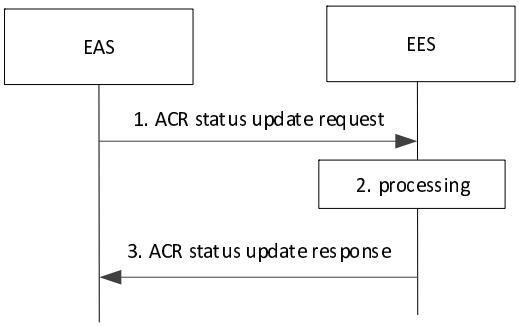

Figure 8.8.3.8-1: ACR status update procedure

1. The EAS sends ACR status update request message to the EES, the request may include the ACT result (success or failure). When sent by the T-EAS, the request may include a list of EDGE-3 subscription ID(s) and Notification Target Address for which the T-EAS wants to update. In case of EELManagedACR, the ACT result is not included by the T-EAS.

2. If the request is authorized by the EES, the EES processes the request. When sent by the T-EAS, if the EDGE-3 subscriptions are available in the T-EES or were successfully relocated during the EEC context relocation procedure, the T-EES updates the Notification Target Address if provided by the T-EAS and may update the list of EDGE-3 subscription ID(s) for the EDGE-3 subscriptions.

   When the ACR status update request message of step 1 includes the ACT result, it shall also include the UEID and endpoint information of the other EAS involved in the ACT. The EES uses UEID and EAS endpoint information to identify the corresponding ACR. In cases where the ACT result indicates failure of the ACR (i.e. failure with a cause indicating cancellation of the ACR), the T-EES which receives the ACR status update request message removes the transferred EEC context.

3. The EES responds with ACR status update response message to the EAS.If the EEC context has been established and during the ACR the T-EES has provided the Selected ACR Scenario list to the S-EES as a result of a successful push context response as per clause 8.9.2.3, after the successful ACR the T-EES updates the Session Context IE within the EEC Context in Table 8.2.8-1 by replacing Selected ACR scenario list with the Selected ACR Scenario list in the push context response. The T-EES may send the ACR Selection notification to the T-EAS if the T-EAS has subscribed to such a notification.

NOTE: If EES is not changed during ACR, the T-EES and S-EES are the same server.

8.8.3.9 ACR parameter information procedure

Figure 8.8.3.9-1 illustrates the procedure for sending ACR parameters from S-EES to the T-EES and T-EAS. The procedure may be used by the S-EES at the beginning of the ACR execution to provide ACR parameters, e.g. prediction expiration time, to the T-EES and T-EAS. The procedure may also be used during an ongoing ACR to update ACR parameters. This procedure is also applicable for the CES to send ACR parameter information to the T-EES.

Pre-condition:

1. The ACR has been launched to the S-EES.

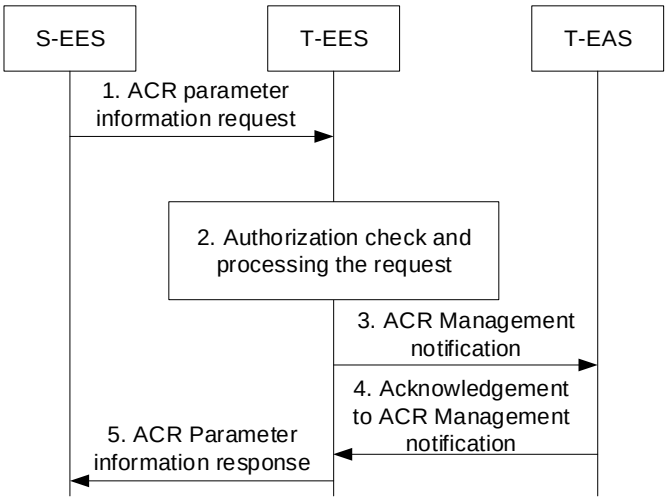

Figure 8.8.3.9-1: ACR parameter information procedure

1. The S-EES sends the ACR parameter information request to the T-EES.
2. The T-EES checks if the requestor is authorized for this operation. If authorized, the T-EES processes the request.
3. If the request is authorized and if the T-EAS has subscribed to receive ACR notifications, the EES shall notify the T-EAS by sending an ACR management notification, with "ACT start" event including ACR parameters from the request in step 1, e.g. Prediction expiration time.
4. In case of service continuity planning, if the T-EAS had included indication of EAS Acknowledgement within ACR management subscribe request, the T-EAS sends EAS Acknowledgement as a response to the ACR management notification. In the Acknowledgement, the T-EAS indicates the acceptance or rejection of the ACT considering ACR parameters (e.g. prediction expiration time).

NOTE: The T-EAS can use the ACR parameters to handle the ACR. For example, the T-EAS can consider prediction expiration time in deciding whether and for how long to wait for the AC of the UE to connect to it. If the ACT is performed, and the AC does not connect to the T-EAS by "Prediction expiration time", the EAS can send ACT failure with the appropriate cause to the EES. In that case, the T-EAS can delete the transferred application context.

5. The EES responds to the requestor's request with an ACR parameter information response message.

8.8.3.10 Selected EES declaration

The selected EES declaration request is triggered when an ACR is performed from EAS to CAS.

Figure 8.8.3.10-1 illustrates the interactions between the EES and the CAS for the selected EES declaration.

Pre-conditions:

1. A serving EES is selected for the EEC and the serving EES decides to inform CAS. The serving EES is the last EES serving the EEC during the ACR from EAS to CAS.
2. AC has requested and forwarded the UE ID as per clause 8.14.2.6 while performing ACR from EAS to CAS as described in clause 8.8.2A or the CAS knows UE ID using procedure defined in clause 8.6.5.

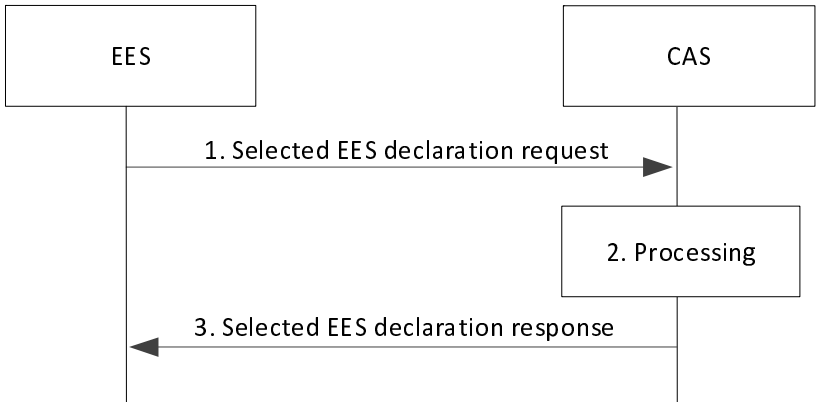

Figure 8.8.3.10-1: Selected EES declaration procedure

1. The EES sends Selected EES declaration request message to the CAS. The request includes the information of the selected EES and may include ACID to indicate which AC the EES is intended for.
2. The CAS checks whether the requesting EES is authorized to perform operation. If authorized, the CAS stores the received information.
3. The CAS responds the request with Selected EES notification declaration response message.

The CAS, after knowing the selected EES for the UE, may subscribe to receive ACT status notifications as described in clause 8.8.3.6.2.3 for EELManagedACR, or trigger service continuity procedures towards the selected EES.

8.8.4 Information flows

8.8.4.1 General

8.8.4.2 EAS discovery request

Table 8.5.3.2-1 describes information elements for the EAS discovery request from the EAS to the EES and from the S-EES to the T-EES. Table 8.5.3.2-2 provides further detail about the EAS Discovery Filter information element.

8.8.4.3 EAS discovery response

The information elements specified in the Table 8.5.3.3-1 is used for the EAS discovery response sent from the EES to the EAS with the following differences:

- The EAS available resources (e.g. memory) indicates the maximum resources available for the AC(s) connected to the S-EAS.

8.8.4.4 ACR request

Table 8.8.4.4-1 describes information elements for the ACR request sent either from the EEC to the S-EES or T-EES, or by the S-EAS to the S-EES. In the EAS bundle case, the ACR request is sent by the main S-EES to its associated S-EES(s).

Table 8.8.4.4-1: ACR request

Information element	Status	Description
Requestor Identifier	M	Identifier of the requestor (i.e. EECID or EASID).
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID	O	Identifier of the EAS
EAS bundle information	O	EAS bundle information.
> Bundle ID (NOTE 12)	O	Bundle ID as described in clause 7.2.10.
> List of EASIDs	O	A list of the EASIDs of the EASs in the bundle.

(NOTE 12)		
UE identifier	M	The identifier of the UE (i.e. GPSI).
Predicted/Expected UE location or Expected AC Geographical Service Area (NOTE 8)	O	The predicted/expected location information of the UE. The UE location is described in clause 7.3.2 or the predicted/expected AC Geographical Service Area as described in clause 7.3.3.3
ACID (NOTE 10)	O	The identifier of the AC.
> EASID	O	Identifier of the EAS
> EAS endpoint	M	Endpoint information of the T-EAS
ACR action (NOTE 3)	M	Indicates the ACR action (ACR initiation, ACR determination or ACR modification)
ACR initiation data (NOTE 2)	O	ACR initiation IEs to be included in an ACR request message when ACR action indicates it is ACR initiation request.
> T-EAS Endpoint	M	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the T-EAS. In case of ACR to cloud, Endpoint information is of CAS.
> Previous T-EAS Endpoint (NOTE 7)	O	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the T-EAS of the previous ACR.
> DNAI of the T-EAS	O	DNAI information associated with the T-EAS.
> N6 Traffic Routing requirements	O	The N6 traffic routing information and/or routing profile ID corresponding to the T-EAS DNAI.
> Simultaneous EAS connectivity information	O	Indicates if simultaneous EAS connectivity is needed and the inactive time guidance for keeping connectivity towards the S-EAS.
> EAS notification indication	M	Indicates whether to notify the EAS about the need of ACR.
> Previous EAS notification indication (NOTE 7)	O	Indicates whether to notify the EAS about the cancellation of a previous ACR.
> S-EAS endpoint (NOTE 1)	O	Endpoint information of the S-EAS
> Bundled T-EAS endpoint list (NOTE 11)	O	A list of associated EAS endpoints in a EAS bundle.
> ACR parameters (NOTE 9)	O	Parameters of the ACR
>> Prediction expiration time	O	The estimated time the UE may reach the Predicted/Expected UE location or EAS service area at the latest
> EEC context relocation details	O	Information required for EEC context relocation using the EEC context push or EEC context pull mechanisms.
>> EEC Context ID (NOTE 5)	O	Identifier of the EEC Context
>> S-EES ID (NOTE 5)	O	Identifier of the EES that provided EEC context ID.
>> S-EES endpoint (NOTE 5)	O	The endpoint address (e.g. URI, IP address) of the EES that provided EEC context ID.
>> T-EES ID (NOTE 6)	O	Identifier of the T-EES.
>> T-EES endpoint (NOTE 6)	O	The endpoint address (e.g. URI, IP address) of the T-EES.
ACR determination data (NOTE 2)	O	ACR determination IEs to be included in an ACR request message when ACR action indicates it is ACR determination request.
> S-EAS endpoint	M	Endpoint information of the S-EAS
ACR modification data (NOTE 2)	O	ACR modification IEs to be included in an ACR request message when ACR action indicates it is ACR modification request.
> S-EAS Endpoint	M	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the S-EAS.
> T-EAS Endpoint	M	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the T-EAS.
> ACR parameters	M	ACR parameters
>> Prediction expiration time	O	The estimated time the UE may reach the Predicted/Expected UE location or EAS service area at the latest

NOTE 1: This IE shall be present if the EAS notification indication or previous EAS notification indication indicates that the EAS needs to be informed.
NOTE 2: One of the ACR initiation, ACR determination or ACR modification shall be included corresponding to the ACR action.
NOTE 3: This IE shall indicate ACR determination if the request originates from the S-EAS.
NOTE 4: Void.
NOTE 5: This IE may be present only if the request originates from the EEC towards the T-EES.
NOTE 6: This IE may be present only if the request originates from the EEC towards the S-EES.
NOTE 7: These IEs shall be present when the EEC re-sends the ACR request as described in clause 8.8.1.3 to indicate a previous ACR is to be cancelled.
NOTE 8: This IE may be present if the ACR procedure is for service continuity planning.
NOTE 9: This IE may be included when the ACR is decided and executed for service continuity planning for a predicted/expected UE location.
NOTE 10: The IE shall be present when the action is ACR modification to identify the ACR to be modified.
NOTE 11: The IE is present when the EEC informs S-EES(s) with applicable bundled T-EAS(s) information for the direct bundle EAS case or when the main S-EES informs its associated S-EES(s) with applicable bundle T-EAS(s) information for the direct bundle EAS case.
NOTE 12: At least one of the IEs shall be present if EAS bundle information is provided.

8.8.4.5 ACR response

Table 8.8.4.5-1 describes the information elements for the ACR response sent either from the S-EES to the EEC or S-EAS, or by the T-EES to the EEC. In the EAS bundle case, the ACR response is sent by the associated S-EES(s) to the main S-EES.

Table 8.8.4.5-1: ACR response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the ACR request was successful.
Failure response (NOTE)	O	Indicates that the ACR request failed.
> Cause	O	Indicates the cause of ACR request failure
NOTE: One of these IEs shall be present in the message.		

8.8.4.6 Retrieve EES request

Table 8.8.4.6-1 describes the information elements to retrieve T-EES information from the ECS.

Table 8.8.4.6-1: Retrieve EES request

Information element	Status	Description
EESID	M	Identifier of the requesting EES or CES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID	M	The identifier of the EAS.
Application Group ID	O	Application group identifier as defined in 7.2.11. Indicates to the ECS that the request is to obtain EES list for the announcement of common EAS
Bundle ID (NOTE)	O	A bundle ID as described in clause 7.2.10.
List of EASIDs (NOTE 2)	O	List of EASIDs associated with the EAS bundle.
> Bundle type	O	Type of the EAS bundle as described in clause 7.2.10
Target DNAI	O	The target DNAI information which can be associated with potential T-EES(s) and/or T-EAS(s).
UE Identifier	O	The identifier of the UE (i.e., GPSI)
UE location	O	The location information of the UE. The UE location is described in clause 7.3.2.
EEC service continuity support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
AC service continuity support	O	Indicates if the AC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the AC.
ENS indication	O	Indicates whether edge node sharing is used.
NOTE: The bundle ID is provided only when bundle type indicates the proxy bundle.		

8.8.4.7 Retrieve EES response

The information elements specified in the Table 8.3.3.3.3-1 is used as response for T-EES information retrieval.

8.8.4.8 ACR information subscription request

Table 8.8.4.8-1 describes the information elements for ACR information subscription request from the EEC to the EES.

Table 8.8.4.8-1: ACR information subscription request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
UE Identifier	O	The identifier of the UE (i.e., GPSI)
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID(s)	M	The identifier of the EAS(s)
ACID(s)	O (NOTE)	The identifier of the AC(s)
Event ID(s)	M	Event ID: - Target information notification - ACR complete
Notification target address	M	Notification target address
Proposed expiration time	O	Proposed expiration time for the subscription
NOTE: If ACID(s) IE is not included, it implies that the subscription corresponds to all ACs that can be served by the EAS(s).		

8.8.4.9 ACR information subscription response

Table 8.8.4.9-1 describes the information elements for ACR information subscription response from the EES to the EEC.

Table 8.8.4.9-1: ACR information subscription response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (NOTE)	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
NOTE: One of these IEs shall be present in the message.		

8.8.4.10 ACR information notification

Table 8.8.4.10-1 describes the information elements for ACR information notification from the EES to the EEC.

Table 8.8.4.10-1: ACR information notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
EASID	M	The identifier of the EAS
ACID	O	The identifier of the AC corresponding to the Selected target EAS
Event ID	M	Either Target information notification or ACR complete
Target information (NOTE 1)	O	Details of the selected T-EAS and the T-EES.
> T-EAS information	M	Details of the selected T-EAS as described in 'Discovered EAS' IE of Table 8.5.3.3-1 or CAS information in case of ACR to cloud.
> Bundled T-EAS information list	O	A list of T-EASs in a EAS bundle, the T-EASs are selected by the network side and details are described in 'Discovered EAS' IE of Table 8.5.3.3-1.
> T-EES information (NOTE 4)	O	Details of the selected T-EES as described in 'EDN configuration information' IE of Table 8.3.3.3.3-1.
> EDN connection information	O	EDN connection information as described in Table 8.3.3.3.3-2.
ACR complete event information (NOTE 2)	O	Details of a completed ACR and its result.
Result of ACR (NOTE 2)	M	Indicates whether the ACR is successful or failure
> T-EAS endpoint	M	Endpoint address of the T-EAS to which an ACR has been performed.
> Bundled T-EAS endpoint list	O	A list of associated EAS endpoints in a EAS bundle.
EEC Context Relocation status (NOTE 5)	O	Indicates whether the EEC context relocation was successful or not.
> Registration Id (NOTE 6)	O	Identifier of the registration for the EEC.
> Expiration Time (NOTE 6)	O	Indicates the expiration time of the registration.
Cause information (NOTE 3)	O	Indicates the cause information for the failure
Selected ACR scenario list (NOTE 6)	O	List of selected ACR scenarios.
NOTE 1: This IE shall be included when Event ID indicates 'Target information notification' event NOTE 2: This IE shall be included when Event ID indicates 'ACR complete' event NOTE 3: This IE shall be included when the Result of ACR indicates failure. NOTE 4: This IE shall be included if the selected T-EES is different from the S-EES. Otherwise, it may be skipped. NOTE 5: This IE shall be included when Event ID indicates 'ACR complete' event and EEC context relocation was attempted. NOTE 6: This IE shall be included if S-EES has received it in EEC Context Push response.		

8.8.4.11 ACR information subscription update request

Table 8.8.4.11-1 describes the information elements for ACR information subscription update request from the EEC to the EES.

Table 8.8.4.11-1: ACR information subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID(s)	O	The identifier of the EAS(s)
Event ID(s)	O	Event ID: - Target information notification - ACR complete
Notification target address	O	Notification target address
Proposed expiration time	O	Proposed expiration time for the subscription

8.8.4.12 ACR information subscription update response

Table 8.8.4.12-1 describes the information elements for ACR information subscription update response from the EES to the EEC.

Table 8.8.4.12-1: ACR information subscription response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (NOTE)	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
NOTE: One of these IEs shall be present in the message.		

8.8.4.13 ACR information unsubscribe request

Table 8.8.4.13-1 describes the information elements for ACR information subscription unsubscribe request from the EEC to the EES.

Table 8.8.4.13-1: ACR information unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.

8.8.4.14 ACR information unsubscribe response

Table 8.8.4.14-1 describes the information elements for ACR information unsubscribe response from the EES to the EEC.

Table 8.8.4.14-1: ACR information unsubscribe response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the unsubscribe request was successful.
Failure response (NOTE)	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
NOTE: One of these IEs shall be present in the message.		

8.8.4.15 EELManagedACR service request

Table 8.8.4.15-1 describes information elements for the EELManagedACR service request from the Edge Application Server to the Edge Enabler Server.

Table 8.8.4.15-1: EELManagedACR service request

Information element	Status	Description
UE identifier	M	Identifies the UE for which ACR is requested
EAS characteristics for ACR	M	Set of characteristics to determine required Edge Application Servers, as detailed in Table 8.5.3.2-2.
Security credentials	M	Security credentials of the source Edge Application Server
Address for Application Context storage	O	The address information from where the Application Context can be accessed for ACT.

8.8.4.16 EELManagedACR service response

Table 8.8.4.16-1 describes information elements for the EELManagedACR service response from the Edge Enabler Server to the Edge Application Server.

Table 8.8.4.16-1: EELManagedACR service response

Information element	Status	Description
Successful response	O	Indicates that the ACR request was successful.
> Address for Application Context storage (NOTE)	O	The address information from where the Application Context can be accessed for ACT.
Failure response	O	Indicates that the EELManagedACR request failed.
> Cause	O	Indicates the cause of request failure
NOTE: This IE is included if "Address for Application Context storage" IE as specified in Table 8.8.4.15-1 is not included in ACR service request.		

8.8.4.17 Selected target EAS declaration request

Table 8.8.4.17-1 describes information elements for the selected target EAS declaration request sent from the S-EAS to the S-EES.

Table 8.8.4.17-1: Selected target EAS declaration request

Information element	Status	Description
UE ID	M	The identifier of the UE.
Security credentials	M	Security credentials.
Selected EAS ID	M	Selected EAS identifier.
ACID	O	The identifier of the AC
Selected EAS Endpoint	M	Endpoint of the selected EAS. In case of ACR to cloud, Endpoint information is of CAS.
EAS bundle information	O	EAS bundle information.
> Bundle ID	O	Bundle ID as described in clause 7.2.10.
> List of EASIDs (NOTE)	O	A list of the EASIDs of the EASs in the bundle.
> T-EAS endpoint list	M	A list of associated EAS endpoints in a EAS bundle, selected by the S-EAS.
Predicted/Expected UE location or Expected AC Geographical Service Area	O	The predicted/expected location information of the UE. The UE location is described in clause 7.3.2 or the predicted/expected AC Geographical Service Area as described in clause 7.3.3.3
NOTE: At least one of the IEs shall be present if EAS bundle information is provided.		

8.8.4.18 Selected target EAS declaration response

Table 8.8.4.18-1 describes information elements for the Selected target EAS declaration response sent from the S-EES to the S-EAS.

Table 8.8.4.18-1: Selected target EAS declaration response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the request was successful.
Failure response (NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the failure cause.
NOTE: One of these IEs shall be present in the message.		

8.8.4.19 ACR status update request

Table 8.8.4.19-1 describes the information elements for the ACR status update request from EAS to EES.

Table 8.8.4.19-1: ACR status update request

Information element	Status	Description
EASID	M	The identifier of the EAS providing the update
Security credentials	M	Security credentials of the EAS
ACID	O	The identifier of the AC
ACT result (NOTE 1, NOTE 3)	O	Indicates whether the ACT was successful or failed.
> UEID	M	The identifier of the UE
> EAS endpoint	M	Endpoint address of the other EAS to or from which the ACT has been performed.
List of EDGE-3 subscription ID(s) (NOTE 2, NOTE 3)	O	A list of the EDGE-3 subscription identifiers.
Notification Target Address for EDGE-3 subscription (NOTE 2, NOTE 3)	O	Notification Target Address of the EAS where the notification is to be sent by the EES for EDGE-3 subscription.
NOTE 1: This IE may be included by the S-EAS and T-EAS. In case of EELManagedACR, this IE is not included by the T-EAS. NOTE 2: This IE may be included only by the T-EAS. NOTE 3: At least one of these IEs shall be present in the message.		

8.8.4.20 ACR status update response

Table 8.8.4.20-1 describes the information elements for the ACR status update response from EES to EAS.

Table 8.8.4.20-1: ACR status update response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the request was successful.
> EDGE-3 subscription initialization result	O	The IE indicates if the EDGE-3 subscriptions were initialized successfully or if initialization failed.
> List of updated EDGE-3 subscription ID(s)	O	If the EDGE-3 subscription initialization result is successful, the EES provides the updated subscription identifier(s). The absence of an identifier implies no change for the subscription identifier.
Failure response (NOTE)	O	Indicates that the request failed
> Cause	O	Indicates the cause of request failure
NOTE: One of these IEs shall be present in the message.		

8.8.4.21 ACT status subscription request

Table 8.8.4.21-1 describes the information elements for the ACT status subscription request from EAS to EES.

Table 8.8.4.21-1: ACT status subscription request

Information element	Status	Description
EASID	M	The identifier of the EAS providing the update
Security credentials	M	Security credentials of the EAS
Notification Target Address	M	Notification Target Address of the EAS where the notification is to be sent by the EES

8.8.4.22 ACT status subscription response

Table 8.8.4.22-1 describes the information elements for the ACT status subscription response from EES to EAS.

Table 8.8.4.22-1: ACT status subscription response

Information element	Status	Description
Successful response	O	Indicates that the request was successful.
> Subscription ID	O	Identifier of the subscription
Failure response	O	Indicates that the request failed
> Cause	O	Indicates the cause of request failure

8.8.4.23 ACT status notification

Table 8.8.4.23-1 describes the information elements for an ACT status notification from the EES to the EAS.

Table 8.8.4.23-1: ACT status notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
ACT status	M	Status of the ACT between S-EES and the T-EES

8.8.4.24 ACR parameter information request

Table 8.8.4.24-1 describes information elements for the ACR parameter information request sent from the S-EES or CES to the T-EES.

Table 8.8.4.24-1: ACR parameter information request

Information element	Status	Description
EES ID	M	Unique identifier of the requesting S-EES or CES.
EECID (NOTE 1)	M	Unique identifier of the EEC.
ACID (NOTE 1)	M	The identifier of the AC.
S-EAS Endpoint (NOTE 1)	M	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the S-EAS.
T-EAS Endpoint (NOTE 1)	M	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the T-EAS or CAS.
ACR parameters	M	ACR parameters
> Prediction expiration time	O	The estimated time the UE may reach the Predicted/Expected UE location or EAS service area at the latest
NOTE 1: These IEs are used to identify the ACR.		

8.8.4.25 ACR parameter information response

Table 8.8.4.25-1 describes information elements for the ACR parameter information response sent from the T-EES to the S-EES or CES.

Table 8.8.4.25-1: ACR parameter information response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the ACR parameter information request was successful.
Failure response (NOTE)	O	Indicates that the ACR parameter information request failed.
> Cause	O	Indicates the cause of ACR parameter information request failure
NOTE: One of these IEs shall be present in the message.		

8.8.4.26 Selected EES declaration request

Table 8.8.4.26-1 describes information elements for the selected EES declaration request sent from the EES to the CAS.

Table 8.8.4.26-1: Selected EES declaration request

Information element	Status	Description
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
UE ID	M	The identifier of the UE.
Selected EES ID	M	Selected EES identifier.
Selected EES Endpoint	M	Endpoint of the selected EES.
EAS ID	M	The identifier of the EAS.
AC ID	O	The identifier of the AC.

8.8.4.27 Selected EES declaration response

Table 8.8.4.27-1 describes information elements for the selected EES declaration response sent from the CAS to the EES.

Table 8.8.4.27-1: Selected EES declaration response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the request was successful.
Failure response (NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the failure cause.
NOTE: One of these IEs shall be present in the message.		

8.8.5 APIs

8.8.5.1 General

Table 8.8.5.1-1 illustrates the APIs for ACR.

Table 8.8.5.1-1: ACR APIs

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_TargetEASDiscovery	Request	Request/Response	EAS, EES
Eees_SelectedTargetEAS	Declare	Request/Response	EAS
Eecs_TargetEESDiscovery	Request	Request/Response	EES, CES
Eees_AppContextRelocation	Request	Request/Response	EEC, EAS, EES
Eees_ACREvents	Subscribe	Subscribe/Notify	EEC
	Notify		
	UpdateSubscription		
	Unsubscribe		
Eees_EELManagedACR	Request	Request/Response	EAS
	Subscribe	Subscribe/Notify	EAS
	Notify		
Eees_ACRStatusUpdate	Request	Request/Response	EAS
Eees_ACRParameterInformation	Request	Request/Response	EES, CES
Ecas_SelectedEES	Declare	Request/Response	EES

8.8.5.2 Eees_TargetEASDiscovery API

8.8.5.2.1 General

This clause describes the Eees_TargetEASDiscovery API and its operations.

8.8.5.2.2 Eees_TargetEASDiscovery_Request operation

API operation name: Eees_TargetEASDiscovery_Request

Description: The consumer requests for the T-EAS information from the EES.

Inputs: See clause 8.8.4.2.

Outputs: See clause 8.8.4.3.

See clause 8.8.3.2 for details of usage of this operation.

8.8.5.3 Eees_AppContextRelocation API

8.8.5.3.1 General

This clause describes the Eees_AppContextRelocation API and its operations.

8.8.5.3.2 Eees_AppContextRelocation_Request operation

API operation name: Eees_AppContextRelocation_Request

Description: The EEC, the EAS or the EES requests to start the ACR launching procedure.

Inputs: See clause 8.8.4.4.

Outputs: See clause 8.8.4.5.

See clause 8.8.3.4 for details of usage of this operation.

8.8.5.4 Eecs_TargetEESDiscovery API

8.8.5.4.1 General

This clause describes the Eecs_TargetEESDiscovery API and its operations.

8.8.5.4.2 Eecs_TargetEESDiscovery_Request operation

API operation name: Eecs_TargetEESDiscovery_Request

Description: The consumer requests for the T-EES information from the ECS.

Inputs: See clause 8.8.4.6.

Outputs: See clause 8.8.4.7.

See clause 8.8.3.3 for details of usage of this operation.

8.8.5.5 Eees_ACREvents API

8.8.5.5.1 General

This clause describes the Eees_ACREvents API and its operations.

8.8.5.5.2 Eees_ACREvents_Subscribe operation

API operation name: Eees_ACREvents_Subscribe

Description: The consumer subscribes for ACR related events.

Inputs: See clause 8.8.4.8.

Outputs: See clause 8.8.4.9.

See clause 8.8.3.5.2 for details of usage of this operation.

8.8.5.5.3 Eees_ACREvents_Notify operation

API operation name: Eees_ACREvents_Notify

Description: The consumer is notified about ACR related events.

Inputs: See clause 8.8.4.10.

Outputs: None.

See clause 8.8.3.5.3 for details of usage of this operation.

8.8.5.5.4 Eees_ACREvents_UpdateSubscription operation

API operation name: Eees_ACREvents_UpdateSubscription

Description: The consumer updates an existing subscription for ACR related events.

Inputs: See clause 8.8.4.11.

Outputs: See clause 8.8.4.12.

See clause 8.8.3.5.4 for details of usage of this operation.

8.8.5.5.5 Eees_ACREvents_Unsubscribe operation

API operation name: Eees_ACREvents_Unsubscribe

Description: The consumer unsubscribes for the previously subscribed ACR related events.

Inputs: See clause 8.8.4.13.

Outputs See clause 8.8.4.14.

See clause 8.8.3.5.5 for details of usage of this operation.

8.8.5.6 Eees_EELManagedACR API

8.8.5.6.1 General

This clause describes the Eees_EELManagedACR API and its operations.

8.8.5.6.2 Eees_EELManagedACR_Request operation

API operation name: Eees_EELManagedACR_Request

Description: The consumer requests for the EELManagedACR handling by the Edge Enabler Server. To use this API, the ASP (EAS provider) and ECSP should have an agreement to use a shared Application Context storage which enables the EES to undertake the ACT in a transparent and secure way, maintaining end user privacy.

Inputs: See clause 8.8.4.15.

Outputs: See clause 8.8.4.16.

See clause 8.8.3.6.2.2 for details of usage of this operation.

8.8.5.6.3 Eees_EELManagedACR_Subscribe operation

API operation name: Eees_EELManagedACR_Subscribe

Description: The consumer requests for the ACT status notifications for EELManagedACR.

Inputs: See clause 8.8.4.21.

Outputs: See clause 8.8.4.22.

See clause 8.8.3.6.2.3 for details of usage of this operation.

8.8.5.6.4 Eees_EELManagedACR_Notify operation

API operation name: Eees_EELManagedACR_Notify

Description: The consumer is notified about the ACT status for EELManagedACR.

Inputs: See clause 8.8.4.23.

See clause 8.8.3.6.2.4 for details of usage of this operation.

8.8.5.7 Eees_SelectedTargetEAS API

8.8.5.7.1 General

This clause describes the Eees_SelectedTargetEAS API and its operations.

8.8.5.7.2 Eees_SelectedTargetEAS_Declare operation

API operation name: Eees_SelectedTargetEAS_Declare

Description: The consumer declares the selected T-EAS information to the EES.

Inputs: See clause 8.8.4.17.

Outputs: See clause 8.8.4.18.

See clause 8.8.3.7 for details of usage of this operation.

8.8.5.8 Eees_ACRStatusUpdate API

8.8.5.8.1 General

This clause describes the Eees_ACRStatusUpdate API and its operations.

8.8.5.8.2 Eees_ACRStatusUpdate_Request operation

API operation name: Eees_ACRStatusUpdate_Request

Description: The consumer updates the information related to ACR, e.g. ACT status.

Inputs: See clause 8.8.4.19.

Outputs: See clause 8.8.4.20.

See clause 8.8.3.8 for details of usage of this operation.

8.8.5.9 Eees_ACRParameterInformation API

8.8.5.9.1 General

This clause describes the Eees_ACRParameterInformation API and its operations.

8.8.5.9.2 Eees_ACRParameterInformation Request operation

API operation name: Eees_ACRParameterInformation_Request

Description: The consumer sends the ACRParameterInformation to another EES.

Inputs: See clause 8.8.4.24.

Outputs: See clause 8.8.4.25.

See clause 8.8.3.9 for details of usage of this operation.

8.8.5.10 Ecas_SelectedEES API

8.8.5.10.1 General

This clause describes the Ecas_SelectedEES API and its operations.

8.8.5.10.2 Ecas_SelectedEES_Declare operation

API operation name: Ecas_SelectedEES_Declare

Description: The consumer declares the selected EES information to the CAS.

Inputs: See clause 8.8.4.26.

Outputs: See clause 8.8.4.27.

See clause 8.8.3.10 for details of usage of this operation.

8.9 EEC Context and EEC Context relocation

8.9.1 General

EEC Context contains information related to an EEC which is used by EESs to provide the Edge Enabler Layer services. The EEC Context may include information about the EEC-hosting UE and the ACs to which the EEC provides services. The EEC Context information may be collected and maintained at the EES in an EDN while the respective ACs are connected to EASs in that EDN.

EEC Context relocation procedures allow the EEC Context information to be shared between EESs (via EDGE-9 interactions).

The EEC Context information may contain List of EDGE-1 subscriptions (i.e., list of subscription IDs for an EEC). The corresponding EDGE-1 subscription information includes EEC ID, Event ID, subscription ID, 3GPP CN subscription information (optional), notification target address (optional) and filter information (optional).

8.9.1.1 EEC Context handling at EEC registration

An EEC Context shall be created for each registered EEC, after a successful registration, by the receiver EES, as follows:

- If the EEC registration request does not include a previously assigned EEC Context ID value, the receiver EES creates an EEC Context as described in clause 8.2.8. The receiver EES shall assign an EEC context ID and set the source EES Endpoint to its own Endpoint. The EEC ID and UE Identifier shall be set based on the corresponding registration request parameters.
- If the EEC registration request contains an EEC context ID and source EES Endpoint, the receiver (i.e., target) EES performs an EEC Context Pull relocation (clause 8.9.2.2). After a successful EEC Context relocation, the target EES updates the source EES Endpoint with its own Endpoint. The target EES may preserve the EEC Context ID received in the request or assign a new EEC Context ID, subject to EES implementation and local policies.

  If the EEC Context relocation is not successful, the target EES creates an EEC Context as described in clause 8.2.8. The target EES shall assign an EEC context ID and set the source EES Endpoint to its own endpoint. The EEC ID and UE ID shall be set based on the corresponding registration request parameters.

  After a successful EEC Context Relocation procedure is performed at EEC (re-)registration to a target EES, the source EES shall determine to be stale the EEC Context identified by the EEC Context ID included in the request (i.e., relocated) and the EEC to be de-registered.

8.9.1.2 EEC Context handling at EEC registration update

An EEC Context shall be updated when EEC Registration update requests targeting the corresponding EEC ID are received.

8.9.1.3 EEC Context handling at EEC de-registration

An EEC Context, including the list of Service Session Context(s) information, shall be determined to be stale after a successful EEC de-registration procedure.

NOTE: Stale EEC Context(s) are subject to information persistence policies and privacy policies. Mechanisms for re-use of stale EEC Context(s) are not in scope of the current version of specification.

8.9.1.4 EEC Context handling at Application Context Relocation

The EEC Context provided to a target EES in an EEC Context Pull relocation or an EEC context Push relocation shall be stored at the target EES, as follows:

- If an EEC context with the same EEC ID, EEC Context ID and source Endpoint already exists at the target EES, the EEC Context is updated.

- If an EEC context with the same EEC ID, EEC Context ID and source Endpoint does not exist at the target EES, the EEC Context is stored.

After a successful EEC Context Relocation procedure is performed at ACR, the source EES shall determine to be stale the element(s) of the list of Service Session Context(s) information included in the request (i.e., relocated). If all Service Session Context(s) information in the EEC Context are stale, the EEC Context is determined to be stale and the EEC to be de-registered.

8.9.1.5 Other EEC Context handling

Elements of the list of Service Session Context(s) information shall be created by the EES when it determines that a registered EAS is providing services to an AC on the served EEC.

Elements of the list of Service Session Context(s) information shall be determined to be stale when the EES determines that a registered EAS is no longer providing services to an AC on the served EEC.

NOTE: In this version of specification, mechanisms used by EES to determine that a registered EAS is no longer providing services to an AC on a served EEC are implementation-dependent.

An EEC Context shall be updated as follows:

- When EEC Context(s) are created, either after a registration request or based on EEC Context relocation procedure, the EES shall check whether the UE Identifier corresponds to an existing EEC Context and update the EEC Context accordingly.
- When EEC subscription requests corresponding to the EEC ID are processed, the "List of EDGE-1 subscriptions" shall be updated accordingly

8.9.2 Procedures

8.9.2.1 General

The following procedures are supported for EEC Context relocation:

- EEC Context Push; and
- EEC Context Pull.

8.9.2.2 EEC Context Pull relocation

An EEC Context is relocated via an EEC Context Pull request initiated by the target EES.

Figure 8.9.2.2-1 illustrates the EEC Context Pull.

Pre-conditions:

1. The source EES has provided the EEC with an EEC Context ID; and
2. The target EES has received the EEC Context ID, source EES Endpoint.

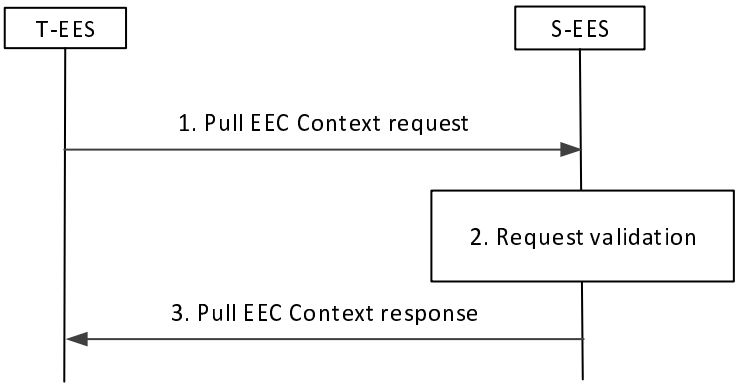

Figure 8.9.2.2-1: EEC Context Pull procedure

1. The target EES requests an EEC Context from the source EES. The request includes EEC Context ID.
2. Upon receiving the request from the target EES, the source EES validates the request and verifies the security credentials of the requester. The source EES uses the EEC Context ID provided to identify and authorize the EEC Context to be relocated.
3. The source EES sends a successful EEC Context response. The target EES stores the received EEC Context.

8.9.2.3 EEC Context Push relocation

An EEC Context is relocated via an EEC Context Push request initiated by the source EES. This procedure is also applicable for the CES to push EEC Context to the T-EES.

Pre-conditions:

1. The source EES has provided the EEC with an EEC Context ID.

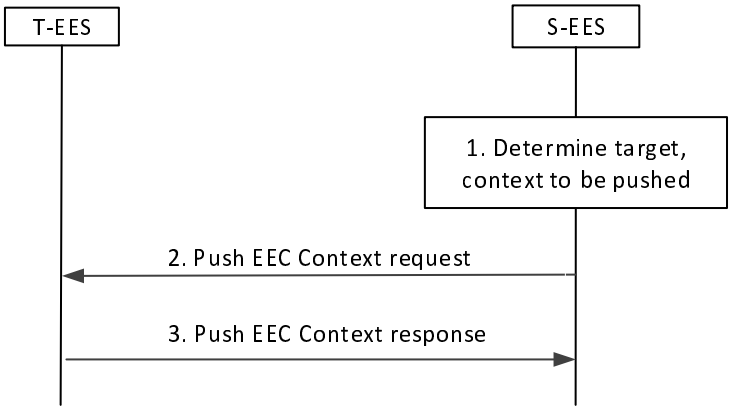

Figure 8.9.2.3-2: EEC Context relocation procedure initiated by source EES

1. The source EES determines to forward EEC Context for relocation to a target EES. The source EES determines the target and the EEC Context to be forwarded.
2. The source EES sends EEC Context Push request to the target EES including the EEC Context determined.
3. Upon receiving the request from the source EES, the target EES validates the request and verifies the security credentials. The target EES uses the EEC Context ID provided to authorize the EEC Context to be stored and managed. Then the target EES sends an EEC Context response indicating success. The T-EES performs implicit

registration and creates the registration ID for the registration and includes it in the EEC context push response message for S-EAS decided ACR or S-EES executed ACR scenarios. The S-EES stores the registration details, and when required, notifies the EEC about registration details while sending ACR information notification.

If the request in step 2 includes the list of selected ACR scenarios within the EEC context, and if the list cannot be supported by T-EES or T-EAS, new list of selected ACR scenarios needs to be selected based on the request from S-EES. The T-EES selects a list of selected ACR scenarios based on T-EES and T-EAS capabilities and "EEC Service Continuity Support" if the IE has been provided in the EEC context and includes it in the Push EEC context response.

NOTE: In this release, ACR scenario list transfer is not supported if EEC is not registered. The EEC can perform EEC Context establishment and ACR scenario selection with the target EES.

8.9.3 Information flows

8.9.3.1 General

The following information flows are specified for EEC Context relocation:

- EEC Context Pull request and response; and
- EEC Context Push request and response.

8.9.3.2 EEC Context Pull request

Table 8.9.3.2-1 describes information elements in the EEC Context Pull request between two EES.

Table 8.9.3.2-1: EEC Context Pull request

Information element	Status	Description
EES ID	M	Unique identifier of the requesting EES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EEC Context ID	M	Unique identifier of the EEC Context used to authorize the transfer.
List of Service Session Contexts requested	O	List of Service Session Context IEs requested to be pulled
> EAS ID	M	Identifier of the EAS providing the application services
> EAS Endpoint	M	Endpoint information of the EAS.
> EEC ID	O	Unique identifier of the EEC.

8.9.3.3 EEC Context Pull response

Table 8.9.3.3-1 describes information elements in the EEC Context Pull response between two EESs.

Table 8.9.3.3-1: EEC Context Pull response

Information element	Status	Description
Successful response	O	Indicates that the request was successful.
>EEC Context	O	EEC Context, mandatory if the request was successful
Failure response	O	Indicates that the request failed.
> Cause	O	Indicates the cause of request failure, mandatory if the request failed.

8.9.3.4 EEC Context Push request

Table 8.9.3.4-1 describes information elements in the EEC Context Push request between two EESs or between CES and EES.

Table 8.9.3.4-1: EEC Context Push request

Information element	Status	Description
EES ID	M	Unique identifier of the requesting EES or CES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EEC Context	M	EEC Context
T-EAS Endpoint	O	The endpoint of the selected T-EAS
ACR scenario selection request	O	Indicates T-EES to select the ACR scenario.

8.9.3.5 EEC Context Push response

Table 8.9.3.5-1 describes information elements in the EEC Context Push response between two EES or between CES and EES.

Table 8.9.3.5-1: EEC Context Push response

Information element	Status	Description
Successful response	O	Indicates that the request was successful.
> registration ID (NOTE)	O	Identifier of the registration for the EEC
> expiration time (NOTE)	O	Indicates the expiration time of the EEC registration.
> Selected ACR scenario list	O	The list of ACR scenarios selected by the T-EES
Failure response	O	Indicates that the request failed.
> Cause	O	Indicates the cause of request failure, mandatory if the request failed.
NOTE: This IE shall be included if implicit registration is performed by T-EES.		

8.9.4 APIs

8.9.4.1 General

Table 8.9.4.1-1 illustrates the EEC context management.

Table 8.9.4.1-1: EEC context management APIs

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EECContextPull	Request	Request/Response	EES
Eees_EECContextPush	Request	Request/Response	EES, CES

8.9.4.2 Eees_EECContextPull API

8.9.4.2.1 General

This clause describes the Eees_EECContextPull API and its operations.

8.9.4.2.2 Eees_EECContextPull_Request operation

API operation name: Eees_EECContextPull_Request

Description: The consumer requests for the EEC context from the EES.

Inputs: See clause 8.9.3.2.

Outputs: See clause 8.9.3.3.

See clause 8.9.2.2 for details of usage of this operation.

8.9.4.3 Eees_EECContextPush API

8.9.4.3.1 General

This clause describes the Eees_EECContextPush API and its operations.

8.9.4.3.2 Eees_EECContextPush_Request operation

API operation name: Eees_EECContextPush_Request

Description: The consumer pushes the EEC context to another EES.

Inputs: See clause 8.9.3.4.

Outputs: See clause 8.9.3.5.

See clause 8.9.2.3 for details of usage of this operation.

8.10 Utilizing 3GPP core network capabilities

8.10.1 General

The functional entities of the Edge Enabler Layer can utilize the 3GPP core network capabilities (i.e. 5GC, EPC) to fulfil the needs of the edge service operations. This clause specifies the details of the 3GPP core network capabilities consumed by each functional entity.

8.10.2 Capabilities utilized by ECS

When required, the ECS may utilize:

- user plane path management events by subscribing with the 3GPP core network for the user plane path management event notifications of the UE as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]; and
- the location information from the API exposed by 3GPP core network, e.g. SCEF/NEF/SCEF+NEF or LCS (Location Service) as specified in 3GPP TS 23.682 [17], 3GPP TS 23.502 [3], 3GPP TS 23.271 [7], 3GPP TS 36.305 [8], 3GPP TS 23.273 [9] and 3GPP TS 38.305 [10] to obtain the UE's location from the 3GPP Core Network.
- application triggering service as specified for Nnef_Trigger_Delivery service in clause 4.13.2 of TS 23.502 [3] or the device triggering procedure via T8 in clause 5.17 of TS 23.682 [17] for the EEC Triggering service described in clause 8.16.

8.10.3 Capabilities utilized by EES and CES

When required, the EES and CES may utilize:

- AF traffic influence functionality, including the user plane path management event notifications of the UE, from the 3GPP core network as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3];
- the location information from the API exposed by 3GPP core network, e.g. SCEF/NEF/SCEF+NEF or LCS (Location Service) as specified in 3GPP TS 23.682 [17], 3GPP TS 23.502 [3], 3GPP TS 23.271 [7], 3GPP TS 36.305 [8], 3GPP TS 23.273 [9] and 3GPP TS 38.305 [10] to obtain the UE's location from the 3GPP Core Network;
- capabilities exposed by the 3GPP core network, e.g. NEF or PCF, to establish an AF session with QoS, and QoS related event notifications subscribed with the 3GPP core network as specified in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [12];
- capabilities exposed by the 3GPP core network, e.g. NEF or NWDAF, to analyse UE expected behaviour as specified in 3GPP TS 23.288 [18]; and

- the monitoring capability exposed by the 3GPP core network as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

- application triggering service as specified for Nnef_Trigger_Delivery service in clause 4.13.2 of TS 23.502 [3] or the device triggering procedure via T8 in clause 5.17 of TS 23.682 [17] for the EEC Triggering service described in clause 8.16.

- AF specific UE ID retrieval as specified in clause 4.15.10 of TS 23.502 [3] to obtain an identifier that can be used when invoking further NEF provided services (e.g., location monitoring).

NOTE 1: While obtaining UE's location or analytics information using 3GPP core network capabilities for the request over EDGE-1 interface, if the EEC registration request from the UE indicates the UE mobility support requirement, the EES as per ECSP policy and EAS requirements may decide whether to subscribe to NEF or NWDAF for UE location information or its analytics.

NOTE 2: If required, EES can determine UE’s serving PLMN information through procedures described in clause 8.18. Further, as required, EES can use this information to utilize 3GPP capabilities provided by UE’s serving PLMN.

NOTE 3: When utilizing 3GPP core network capabilities, the EES, acting as an Application Function (AF) as defined in TS 23.503 [12], may use its EESID as the AF Identifier. Alternatively, when an EES is acting on behalf of an EAS that is also considered an AF, the EES may pass the EASID as the AF identifier in place of its EESID if it is authorized to do so.

8.11 EEC Authentication/Authorization

8.11.1 General

The architecture for enabling edge applications supports EEC authentication/authorization.

After the successful EEC authentication/authorization, the EEC acquires a valid security credential for EEC related procedures including service provisioning procedure, EEC registration procedure, EAS discovery procedure and ACR procedure. Detailed procedures are specified in 3GPP TS 33.558 [23].

8.12 Dynamic EAS instantiation triggering

8.12.1 General

The EES may trigger the EAS instantiation dynamically due to e.g., EAS discovery request, EAS discovery subscription request, UE mobility, upon receiving EEC Registration request containing AC profile or upon receiving an EAS information provisioning request.

Upon receiving the EAS discovery request with EAS discovery filter from the EEC or the S-EES during the procedures for EAS discovery or ACR, the EES may fail to discover and select the EAS that matches the UE location and the requesting application characteristics specified in table 8.5.3.2-2 due to no EAS is available or instantiated. The EES may trigger the ECSP management system (which is specified in TS 28.538 [22]) to instantiate the EAS serving the AC in the EDN corresponding to the EAS that can be instantiable before returning the EAS information to the EEC or S-EES, based on the information about instantiable EASs which can be dynamically instantiated at the associated EDN. If EAS selection is performed by the EES, the selected EAS is dynamically instantiated if applicable.

Based on the information about instantiable EASs, the EES may maintain the EAS instantiation status transition (e.g., among instantiated, instantiable but not instantiated yet, or instantiation in progress) via the EAS (de-)registration procedure or the dynamic EAS instantiation triggering procedure. The EAS instantiation status can be provided to the EEC using the Instantiable EAS Information IE of EAS discovery response and EAS discovery notification for the use of EAS selection by the EEC. If the EEC indicates EAS Instantiation Triggering Suppress in EAS discovery request and EAS discovery subscription request, then the EES does not trigger EAS instantiation.

Upon receiving EEC Registration request with bundle EAS information the EES may determine that only a subset of the EAS(s) in the bundle are registered and instantiated. If only a subset of bundle EASs is determined, the EES may

trigger the ECSP management system to instantiate the subset of remaining EASs corresponding to the bundle that can be instantiable before responding to the registration request.

Upon receiving one or more EAS discovery subscription request(s) for the availability of an EAS, EES may determine if there is a need for EAS instantiation based on the information about instantiable EASs. If such a need for EAS instantiation determined, EES may send a report for a need of the EAS instantiation to the ECSP management system to consider instantiating the requested EAS by invoking an MnS API of the ECSP management system. When the requested EAS has been instantiated, the EES may obtain the EAS profile during the EAS registration procedure and notify the availability change event of the requested EAS with the EAS profile to the corresponding EECs via the EAS discovery notification procedure as specified in the clause 8.5.2.3.

Upon receiving the EAS information provisioning request, the EES may trigger the ECSP management system to instantiate the EAS in the EDN before returning the EAS information to the EEC.

NOTE 1: The ECSP management system is responsible for the authorization of the dynamic EAS instantiation.

NOTE 2: The ECSP management system can provide the information about instantiable EASs to the EES. Such a mechanism is out of scope of this release of the present document.

NOTE 3: When determining a need for EAS instantiation, EES can further consider the requested service characteristics (e.g. location, latency) by EEC or service load/capacity (e.g. number of service sessions) of EAS, which is upon implementation and out the scope of this specification.

NOTE 4: The details for EAS instantiation provided by the ECSP management system is specified in clause 7.1.2 of 3GPP TS 28.538 [22].

8.13 Charging

The charging procedures are specified in 3GPP TS 32.257 [25].

8.14 EDGE-5 APIs

8.14.1 General

EEC exposes EDGE-5 APIs corresponding to EEC's capabilities, for the AC to request EEC's services for edge enablement. Using these APIs, ACs request the EEC for EEL services. EDGE-5 APIs include one-time request/response operations for EAS discovery, retrieval of UE ID and ACR operations. Additionally, the AC can request for an AC subscription. The EEC creates the subscription and when required, performs necessary operations such as EAS discovery, ACR etc., delivering notifications to the AC as required.

NOTE 1: EEC can initiate any EDGE-1 or EDGE-4 operation without receiving a request or without receiving AC related information from the AC.

NOTE 2: It is outside the scope of this release of this specification how to ensure of user's authorization as well as AC’s authorization in invoking functions exposed by EEC (to AC) which in turn relies on functions exposed by the network (e.g. Location) via EES/NEF.

8.14.2 Procedures

8.14.2.1 General

Following procedures are specified for EDGE-5:

- Registration;
- EAS discovery;
- ACR trigger request;
- EEC services subscription; and

- UE ID request.

8.14.2.2 Registration

8.14.2.2.1 General

Following are supported for AC registration:

- AC registration procedure;
- AC registration update procedure; and
- AC de-registration procedure.

8.14.2.2.2 AC registration

Figure 8.14.2.2.2-1 illustrates AC registration procedure.

Pre-conditions:

1. AC can communicate with the EEC.

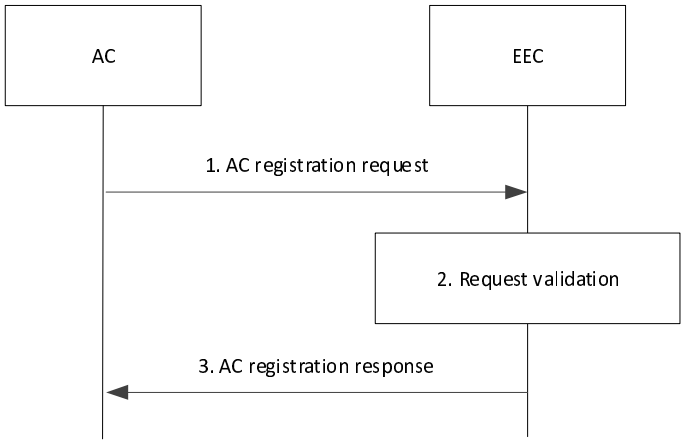

Figure 8.14.2.2.2-1: AC registration procedure

1. The AC sends an AC registration request to the EEC. The request includes the AC profile, AC's security credentials and optionally the EAS characteristics. The request may also include a list of EEC's services that AC requires the EEC to handle. The request additionally includes ECS configuration information if the AC is edge-aware and configured with the ECS configuration information.

NOTE 1: The ASP providing the AC and the ECSP providing the ECS can have edge computing service provider service agreement as described in Annex B. The ECS configuration information configured in the AC is based on the service agreement.

2. The EEC checks AC's security credentials and validates the request.
3. If the request is successfully validated, the EEC registers the information provided in the request and responds back to the AC with AC registration response. The AC registration response includes the list of EEC's services that AC is authorized for.

NOTE 2: The mechanisms used for authentication and authorization between AC and EEC is out of scope of this specification. EEC can use local policies, user preferences, ASP services agreement(s) (see Annex B) to authorize the request from the AC.

NOTE 3: When the ECS configuration information is provided from an AC, the EEC can use the ECS configuration for initial service provisioning for the AC that provided the ECS configuration information if there is no ECS configuration information is provided from the 5GC.

8.14.2.2.3 AC registration update

Figure 8.14.2.2.3-1 illustrates AC registration update procedure.

Pre-conditions:

1. AC is registered with the EEC.

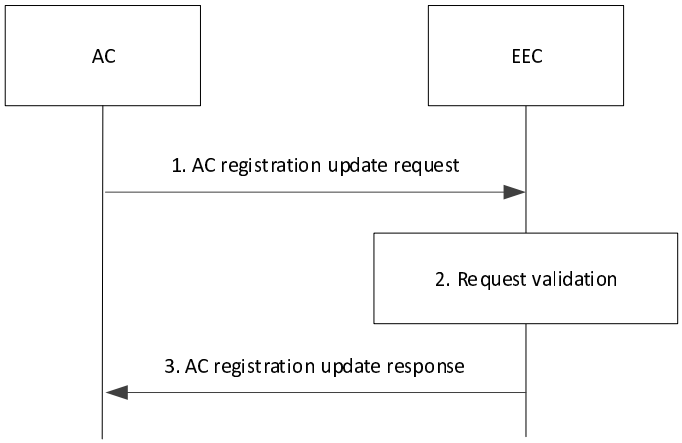

Figure 8.14.2.2.3-1: AC registration update procedure

1. The AC sends an AC registration update request to the EEC. The request includes the registration ID, AC's security credentials, and may include the updated AC profile, EAS discovery filters, list of requested EEC services and list of ECS information.
2. The EEC checks AC's security credentials and validates the request.
3. If the request is successfully validated, the EEC sends a successful registration update response, which includes an updated list of EEC services that AC is authorized for.

8.14.2.2.4 AC deregistration

Figure 8.14.2.2.4-1 illustrates AC deregistration procedure.

Pre-conditions:

1. AC is registered with the EEC.

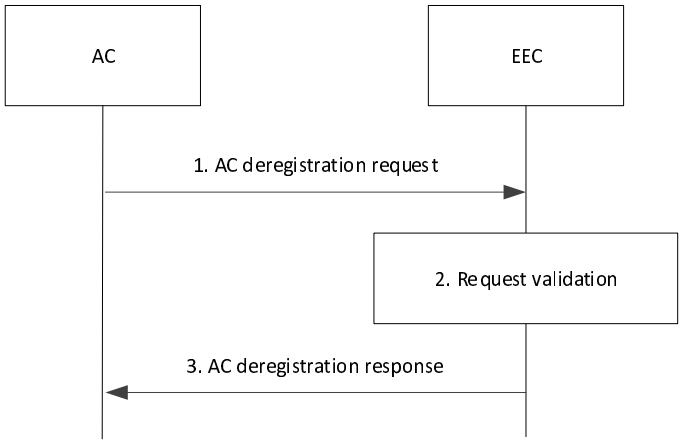

Figure 8.14.2.2.4-1: AC deregistration procedure

1. The AC sends an AC deregistration request to the EEC. The request includes the registration ID and AC's security credentials.
2. The EEC checks AC's security credentials and validates the request.
3. Upon successful authorization, the EEC deregisters the AC and sends a successful de-registration response.

8.14.2.3 EAS discovery

Pre-conditions:

1. The AC can communicate with the EEC.

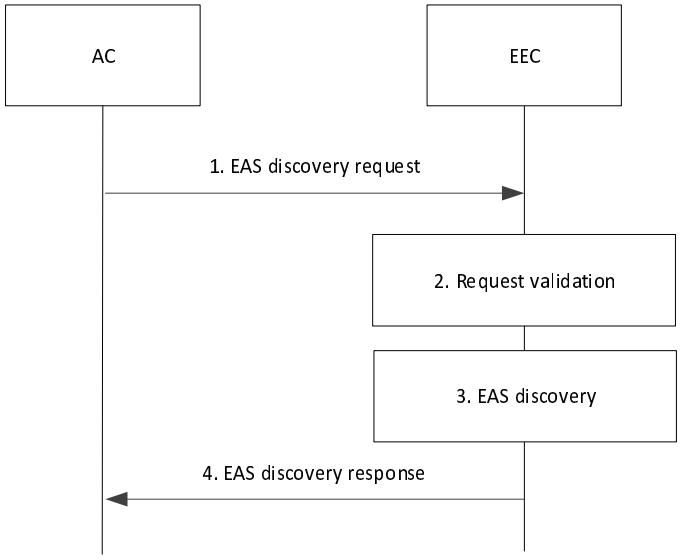

Figure 8.14.2.3-1: EAS discovery request procedure

1. The AC sends an EAS discovery request to the EEC. The request includes AC profile and AC's security credentials and may include EAS discovery filters.
2. The EEC checks AC's security credentials and validates the request.

3. If the request is successfully validated, the EEC determines if the required EAS is available or not. The EEC may use information cached or preconfigured at the EEC or may use the EAS discovery procedures to query the EES. If step 1 includes the AC profile or EAS discovery filters, then the EEC may utilize the provided AC profile and filters, to form the EAS discovery request towards EES. If step 1 does not include any of the optional IEs of the AC profile and EAS discovery filters, and AC registration was performed, the EEC may utilize the AC profile provided by the AC during AC registration. The EEC also needs to take user privacy requirements, e.g., regarding the disclosure of location information towards the network into account. If required, e.g., when EAS discovery procedures returns a list of EASs, the EEC performs EAS selection based on the information received in step 1 and the AC profile. The EEC can perform EAS discovery with different EESs before selecting an EAS.

NOTE 1: If required, the EEC can perform service provisioning procedure, or EEC registration procedure or both, before performing the EAS discovery procedures. EEC may already have captured EESs and EASs availability for present location; so that the AC's request (step 1) can be replied to quickly and efficiently.

NOTE 2: The EEC can include AC profiles of more than one AC in the EAS discovery request sent to the EES.

NOTE 3: It is outside the scope of this release of this specification how the user or the AC can consent, e.g., to the disclosure of location information and the use of the AC ID in the signalling towards the network.

4. The EEC responds back to the AC with the EAS discovery response. The response includes the EAS profile(s) of the available EAS(s).

8.14.2.4 ACR trigger request

Pre-conditions:

1. AC has subscribed for "ACR notifications" as specified in clause 8.14.2.5.2.

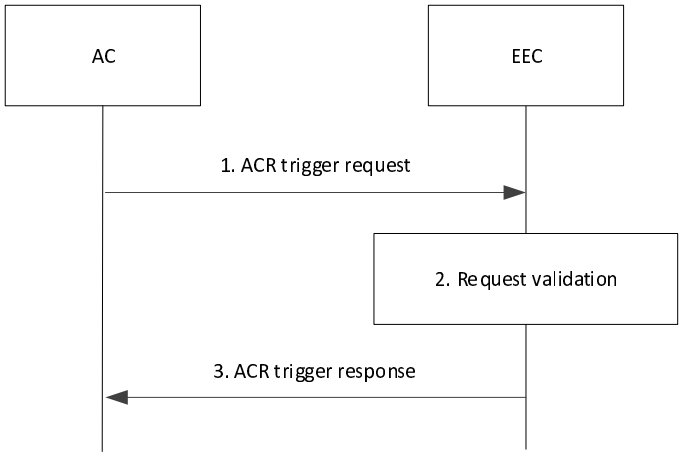

Figure 8.14.2.4-1: ACR trigger request procedure

1. The AC sends an ACR trigger request to the EEC. The request includes AC profile, AC's security credentials, type of requested operation (i.e., ACR detection, ACR initiation) and S-EAS information as described in clause 8.14.3.10. If the request is to initiate the ACR, the request may also include the target EAS information.

2. The EEC checks AC's security credentials and validates the request.

3. If the request is successfully validated, the EEC sends an ACR trigger response to the AC indicating if the request was successful as described in 8.14.3.11. The EEC process the request from the AC. If the type of requested operation in the request received in step 1 is:

   - ACR detection, then the EEC determines if ACR is required or not. If it is required, the EEC uses one of the EEC initiated ACR scenarios or launches ACR with action "determination", leading to S-EES executed ACR;

- ACR initiation, then the EEC uses one of the EEC initiated ACR scenarios and initiate ACR. If the request in step 1 also includes target information, the EEC uses it to select the ACR targets;

NOTE: EEC notifies the AC to trigger ACT as required, or EEC notifies ACR execution result as specified in clause 8.14.2.5.3.

8.14.2.5 EEC services subscription

8.14.2.5.1 General

Following are supported for EEC services subscription:

- Subscribe;
- Notify;
- Subscription update; and
- Unsubscribe.

8.14.2.5.2 Subscribe

Pre-conditions:

1. The AC can communicate with the EEC.

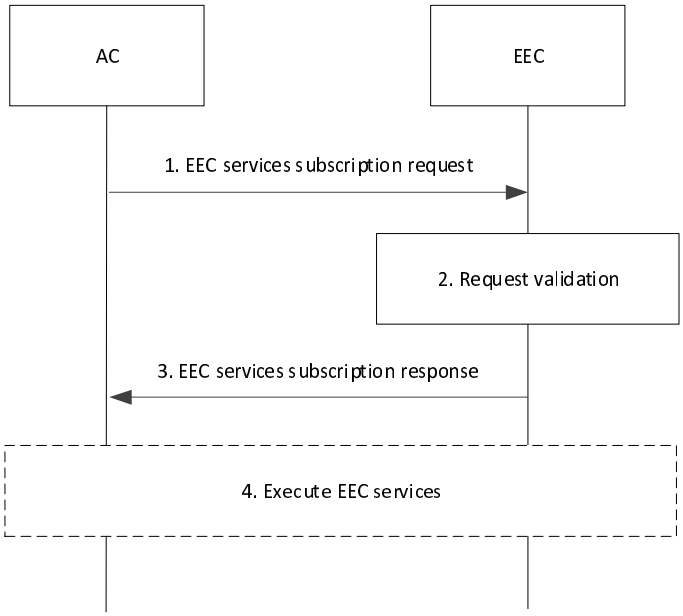

Figure 8.14.2.5.2-1: EEC services subscription procedure

1. The AC sends an EEC services subscription request to the EEC. The request includes AC profile, AC's security credentials, a list of EEC's services that AC requires the EEC to handle, and related parameters as described in 8.14.3.12. If the subscription request includes:

- EAS discovery or EAS dynamic information subscription, then the request may include a list of EAS characteristics and a list of EAS dynamic information filters respectively;
- ACR, then the request includes a list of S-EAS information and corresponding type of ACR operations:
  - ACR notifications, where the EEC notifies the AC with respect to the "ACR detection" and "ACR initiation" requests as specified in clause 8.14.2.5.3;

- ACR monitoring, where the EEC monitors the need for ACR and notifies the AC as and when required e.g., on receiving ACR related notifications on EDGE-1 interface; and

- EEC managed ACR, where the EEC monitors the need for ACR. If need for ACR is detected, then the EEC decides and initiates ACR using one of the EEC initiated ACR scenarios. The EEC notifies the AC about the imminent ACR and may include the target information.

2. The EEC checks AC's security credentials and validates the request.

3. If the request is successfully validated, the EEC creates the subscription and sends an EEC services subscription response message to the AC. The response includes the list of services that the EEC will handle and related details.

4. The EEC executes the services e.g., EAS discovery, ACR, and notifies the AC with information as necessary. The EEC may use locally cached information or configurations while providing services to the AC.

8.14.2.5.3 EEC services notification

Pre-conditions:

1. The AC has subscribed to the EEC.

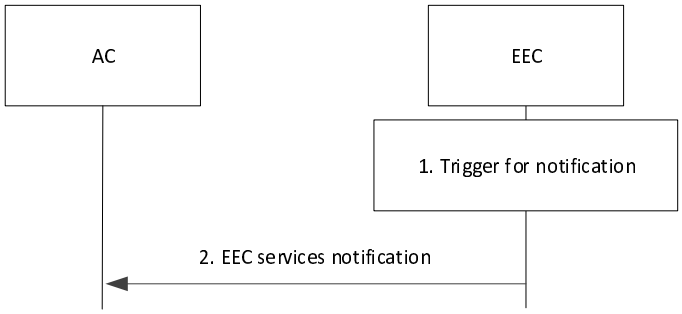

Figure 8.14.2.5.3-1: EEC services notification procedure

1. An event occurs at the EEC that satisfies the trigger conditions for notifying a AC e.g., EEC detects a need for Application Context Relocation, unavailability of suitable T-EES and/or unavailability of suitable T-EAS.

NOTE: Upon receiving a EEC services notification indicating no suitable T-EES/T-EAS was available, the AC may decide to initiate DNS query to obtain CAS information to prepare and move the application context to the CAS.

2. The EEC sends an EEC services notification to the AC with relevant information related to the event triggered in step 1.

8.14.2.5.4 EEC services subscription update

Figure 8.14.2.5.4-1 illustrates EEC services subscription update procedure.

Pre-conditions:

1. The AC has subscribed to the EEC.

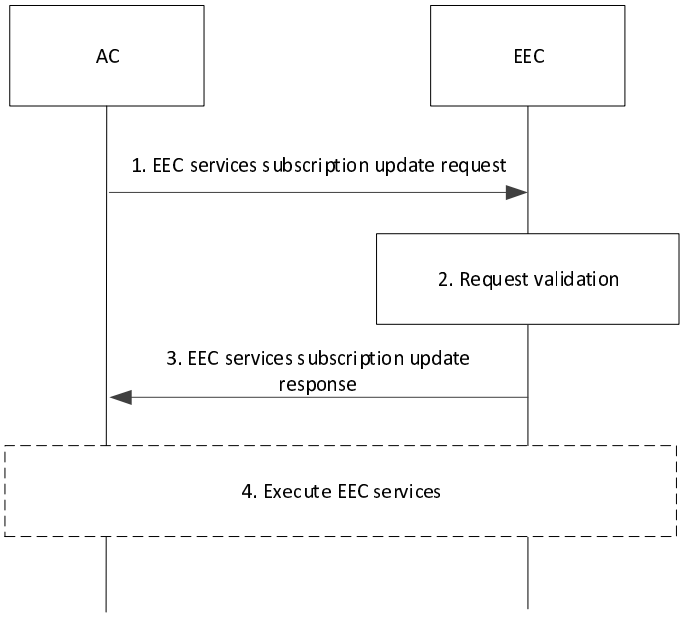

Figure 8.14.2.5.4-1: EEC services subscription update procedure

1. The AC sends an EEC services subscription update request to the EEC. The request includes the subscription ID, AC's security credentials, and may include updated notification related details or updated list of required EEC services.
2. The EEC checks AC's security credentials and validates the request.
3. If the request is successfully validated, the EEC updates the subscription and sends a successful subscription update response.
4. The EEC executes the services e.g., EAS discovery, ACR, and notifies the AC with information as necessary. The EEC may use locally cached information or configurations while providing services to the AC.

8.14.2.5.5 Unsubscribe

Figure 8.14.2.5.5-1 illustrates the unsubscribe procedure.

Pre-conditions:

1. The AC has subscribed to the EEC.

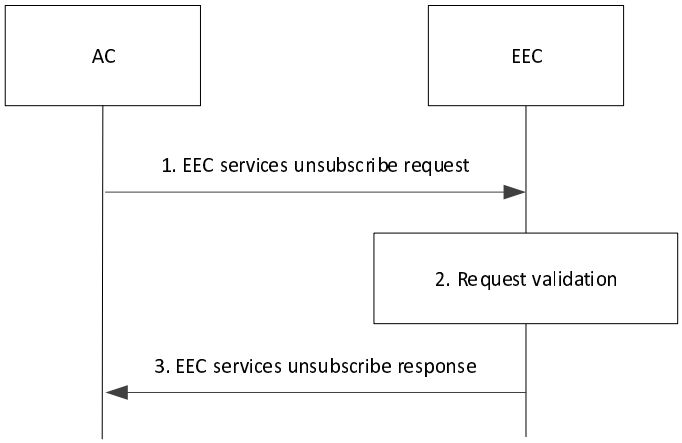

Figure 8.14.2.5.5-1: EEC services unsubscribe procedure

1. The AC sends EEC services unsubscribe request to the EEC. The request includes the subscription ID and AC's security credentials.
2. The EEC checks AC's security credentials and validates the request.
3. Upon successful authorization, the EEC sends a successful de-registration response.

8.14.2.6 UE ID request

Pre-conditions:

1. The AC can communicate with the EEC.

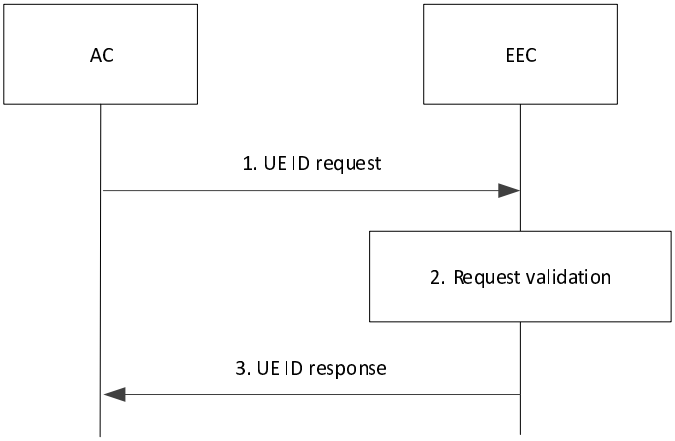

Figure 8.14.2.6-1: UE ID request procedure

1. The AC sends an UE ID request to the EEC. The request includes AC's security credentials and the EAS ID list for which the AC needs to know the associated Edge UE ID or AF-specific UE ID(s).
2. The EEC checks AC's security credentials and validates the request.
3. If the request is successfully validated, the EEC process the request from the AC. The EEC uses the UE Identifier API procedure (see clause 8.6.5) to query the EES.

NOTE: This procedure may be used to support the retrieval of the UE ID for AC's (and EAS's) dealing with IPv4 NATed IP address issue (i.e. EAS's direct invocation of UE Identifier API procedure due to NATed IP address fails to identify the UE). Under such a scenario then it is understood that, the AC through application signalling which is outside the scope of this document, would pass on the UE ID (received in step 3) to the EAS so that it can be used to invoke capability APIs over EDGE-3 or EDGE-7.

8.14.3 Information flows

8.14.3.1 General

8.14.3.2 AC registration request

Table 8.14.3.2-1 describes information elements of the AC registration request sent by the AC to the EEC.

Table 8.14.3.2-1: AC registration request

Information element	Status	Description
AC profile	M	AC profile of the AC sending the registration request.
Security credentials	M	Security credentials of the AC sending the registration request.
List of EAS characteristics	O	List of EAS characteristics as described in EAS discovery filters (see Table 8.5.3.2-2).
List of requested EEC services	O	One or more EEC services requested by the AC e.g., EAS discovery, ACR.
List of ECS information	O	One or more ECS configuration information

8.14.3.3 AC registration response

Table 8.14.3.3-1 describes information elements of the AC registration response sent by the EEC to the AC.

Table 8.14.3.3-1: AC registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the AC registration.
> List of allowed EEC services	M	List of all the EEC services AC is authorized to use.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time.
Failure response	O	Indicates that the registration request failed.
> Cause	M	Provides the cause for registration request failure.

8.14.3.4 AC registration update request

Table 8.14.3.4-1 describes information elements in the AC registration update request sent by the AC to the EEC.

Table 8.14.3.4-1: AC registration update request

Information element	Status	Description
Registration ID	M	AC registration identifier provided by the EEC during AC registration.
Security credentials	M	Security credentials of the AC sending the registration update request.
AC profile	O	AC profile of the AC sending the registration update request.
List of EAS characteristics	O	List of EAS characteristics as described in EAS discovery filters (see Table 8.5.3.2-2).
List of requested EEC services	O	One or more EEC services requested by the AC e.g., EAS discovery, ACR.
List of ECS information	O	One or more ECS configuration information

8.14.3.5 AC registration update response

Table 8.14.3.5-1 describes information elements in the AC registration update response sent by the EEC to the AC.

Table 8.14.3.5-1: AC registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> List of allowed EEC services	M	List of all the EEC services AC is authorized to use.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time.
Failure response	O	Indicates that the registration request failed.
> Cause	M	Provides the cause for registration request failure.

8.14.3.6 AC deregistration request

Table 8.14.3.6-1 describes information elements in the AC deregistration request sent by the AC to the EEC.

Table 8.14.3.6-1: AC deregistration request

Information element	Status	Description
Registration ID	M	AC registration identifier provided by the EEC during AC registration.
Security credentials	M	Security credentials of the AC sending the deregistration request.

8.14.3.7 AC deregistration response

Table 8.14.3.7-1 describes information elements in the AC deregistration response sent by the EEC to the AC.

Table 8.14.3.7-1: AC deregistration response

Information element	Status	Description
Successful response	O	Indicates that the deregistration request was successful.
Failure response	O	Indicates that the deregistration request failed.
> Cause	M	Provides the cause for deregistration request failure.

8.14.3.8 EAS discovery request

Table 8.14.3.8-1 describes information elements for the EAS discovery request sent by the AC to the EEC.

Table 8.14.3.8-1: EAS discovery request

Information element	Status	Description
AC profile	M	AC profile of the AC sending the registration request.
Security credentials	M	Security credentials of the AC.
List of EAS characteristics	O	List of EAS characteristics as described in EAS discovery filters (see Table 8.5.3.2-2).

8.14.3.9 EAS discovery response

Table 8.14.3.9-1 describes information elements for the EAS discovery response sent by the EEC to the AC.

Table 8.14.3.9-1: EAS discovery response

Information element	Status	Description
Successful response	O	Indicates that the EAS discovery request was successful.
> Discovered EAS list	O	List of discovered EAS(s). Each element includes the information described below.
>> EAS profile	M	Profile of the EAS. Each element is described in clause 8.2.4
>> Lifetime	O	Time interval or duration during which the information elements in the EAS profile is valid and supposed to be cached in the AC (e.g. time-to-live value for an EAS Endpoint)
Failure response	O	Indicates that the EAS discovery request failed.
> Cause	O	Indicates the cause of EAS discovery request failure.

8.14.3.10 ACR trigger request

Table 8.14.3.10-1 describes information elements of the ACR trigger request sent by the AC to the EEC.

Table 8.14.3.10-1: ACR trigger request

Information element	Status	Description
AC profile	M	AC profile for EEC to determine the target EAS.
Security credentials	M	Security credentials of the AC
Requested ACR action	M	One of ACR detection or ACR initiation request actions
S-EAS information	M	ID of the EAS to which the ACR request relates.
T-EAS information (NOTE)	O	AC provided target EAS information.
NOTE: This IE may be included if the request is to initiate the ACR.		

8.14.3.11 ACR trigger response

Table 8.14.3.11-1 describes information elements of the ACR trigger response sent by the EEC to the AC.

Table 8.14.3.11-1: ACR trigger response

Information element	Status	Description
Successful response	O	Indicates that the ACR request was successful and EEC is processing the requested ACR operation.
Failure response	O	Indicates that the ACR request failed.
> Cause	O	Indicates the cause of ACR request failure.

8.14.3.12 EEC services subscription request

Table 8.14.3.12-1 describes information elements for the EEC services subscription request sent by the AC to the EEC.

Table 8.14.3.12-1: EEC services subscription request

Information element	Status	Description
AC profile	M	AC profile of the AC requesting subscription
Security credentials	M	Security credentials of the AC.
Notification details	M	Details on how the EEC can notify the AC.
Required EEC services	M	EEC handled services required by the AC
> EAS discovery	O	Indicates that AC requires EEC to handle EAS discovery.
>> List of EAS characteristics	O	List of EAS characteristics as described in EAS discovery filters (see Table 8.5.3.2-2).
> EAS dynamic information	O	Indicates that the AC requires EAS dynamic information subscription
>> List of EAS dynamic information filters	M	List of EAS dynamic information filters as described in Table 8.5.3.4-2.
> ACR	O	Indicates that the AC requires ACR related services for the following EASs
>> List of S-EAS information	M	S-EAS information corresponding to the ACR operation
>>> EASID	M	Identifier of the S-EAS to which the subscription relates.
>>> EAS endpoint	M	Endpoint of the S-EAS to which the subscription relates.
>>> ACR operation	O	Indicates if AC requires ACR monitoring or EEC managed ACR corresponding to each S-EAS
>>> CAS information	O	AC provided target CAS information.

8.14.3.13 EEC services subscription response

Table 8.14.3.13-1 describes information elements for the EEC services subscription response sent by the EEC to the AC.

Table 8.14.3.13-1: EEC services subscription response

Information element	Status	Description
Successful response	O	Indicates that the EEC services subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
> Confirmed EEC services	M	List of services EEC confirms to handle
>> EAS discovery	O	Indicates that the EEC will handle EAS discovery
>> EAS dynamic information	O	Indicates that the EEC will handle EAS dynamic information subscription
>> ACR	O	Indicates that the EEC will handle ACR.
>>> List of S-EAS information	M	Information of the S-EASs EEC will handle.
>>>> EASID	M	Identifier of the S-EAS to which the subscription relates.
>>>> EAS endpoint	M	Endpoint of the S-EAS to which the subscription relates.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.14.3.14 EEC services notification

Table 8.14.3.14-1 describes information elements for the EEC services notification sent by the EEC to the AC.

Table 8.14.3.14-1: EEC services notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the notification.
Notification details	M	Information related to the notification
> EAS discovery	O	Indicates that the notification relates to EAS discovery
>> List of EAS profiles	M	EAS profiles associated with the notification. Each element is described in clause 8.2.4
>>> Lifetime	O	Time interval or duration during which the information in the EAS profile is valid and supposed to be cached in the AC (e.g. time-to-live value for an EAS Endpoint)
> EAS dynamic information	O	Indicates that the notification relates to EAS dynamic information subscription
>> List of EAS profile	M	EAS profiles associated with the notification. Each element is described in clause 8.2.4
>>> Lifetime	O	Time interval or duration during which the information in the EAS profile is valid and supposed to be cached in the AC (e.g. time-to-live value for an EAS Endpoint)
> ACR	O	Indicates that the notification relates to ACR
>> List of S-EAS information	M	ACR operation information and information of the EAS to which the notification relates.
>>> EASID	M	Identifier of the S-EAS to which the subscription relates.
>>> EAS endpoint	M	Endpoint of the S-EAS to which the subscription relates.
>>> ACR detection	O	Indicates that the EEC detected a need for ACR
>>> ACR decision	O	EEC's decision information related to an ACR detection
>>> ACR execution status	O	Indicates the status of ACR execution
>>>> Status	M	ACR status such as initiated, in-progress, complete, failed
>>>> T-EAS information	O (NOTE)	Information of the T-EAS corresponding to the S-EAS
>>>>> EASID	M	Identifier of the T-EAS to which an ACR has been performed.
>>>>> EAS endpoint	M	Endpoint address of the T-EAS to which an ACR has been performed.
>>>> Failure cause	O (NOTE)	ACR failure reason e.g. due to unavailability of suitable T-EES or T-EAS
NOTE: "T-EAS information" IE shall be present only when the value of "Status" IE is other than failed. And "Failure cause" IE shall be present only when the value of "Status" is failed.		

8.14.3.15 EEC services subscription update request

Table 8.14.3.15-1 describes information elements for the EEC services subscription update request sent by the AC to the EEC.

Table 8.14.3.15-1: EEC services subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the update request.
Security credentials	M	Security credentials of the AC.
Notification details	O	Details on how the EEC can notify the AC.
Required EEC services	O	EEC handled services required by the AC
> EAS discovery	O	Indicates that AC requires EEC to handle EAS discovery.
>> List of EAS discovery filters	M	List of EAS discovery filters as described in Table 8.5.3.2-2.
>>> Preferred ECSP list	O	Preferred ECSP list corresponding to each set of EAS discovery filters.
> EAS dynamic information	O	Indicates that the AC requires EAS dynamic information subscription
>> List of EAS dynamic information filters	M	List of EAS dynamic information filters as described in Table 8.5.3.4-2.
> ACR	O	Indicates that the AC requires ACR related services for the following EASs
>> List of S-EAS information	M	S-EAS information corresponding to the ACR operation
>>> EASID	M	Identifier of the S-EAS to which the subscription relates.
>>> EAS endpoint	M	Endpoint of the S-EAS to which the subscription relates.
>>> ACR operation	O	Indicates if AC requires ACR monitoring or EEC managed ACR corresponding to each S-EAS
>>> CAS information	O	AC provided target CAS information.

8.14.3.16 EEC services subscription update response

Table 8.14.3.16-1 describes information elements for the EEC services subscription update response sent by the EEC to the AC.

Table 8.14.3.16-1: EEC services subscription update response

Information element	Status	Description
Successful response	O	Indicates that the EEC services subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
> Confirmed EEC services	M	List of services EEC confirms to handle
>> EAS discovery	O	Indicates that the EEC will handle EAS discovery
>> EAS dynamic information	O	Indicates that the EEC will handle EAS dynamic information subscription
>> ACR	O	Indicates that the EEC will handle ACR
>>> List of S-EAS information	M	Information of the S-EASs EEC will handle.
>>> EASID	M	Identifier of the S-EAS to which the subscription relates.
>>> EAS endpoint	M	Endpoint of the S-EAS to which the subscription relates.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.14.3.17 EEC services unsubscribe request

Table 8.14.3.17-1 describes information elements for the EEC services unsubscribe request sent by the AC to the EEC.

Table 8.14.3.17-1: EEC services unsubscribe request

Information element	Status	Description
Subscription ID	M	EEC services subscription identifier provided by the EEC during subscription.
Security credentials	M	Security credentials of the AC sending the EEC services unsubscribe request.

8.14.3.18 EEC services unsubscribe response

Table 8.14.3.18-1 describes information elements for the EEC services unsubscribe response sent by the EEC to the AC.

Table 8.14.3.18-1: EEC services unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the EEC services unsubscribe request was successful.
Failure response	O	Indicates that the EEC services unsubscribe request failed.
> Cause	M	Provides the cause for EEC services unsubscribe request failure.

8.14.3.19 UE ID request

Table 8.14.3.19-1 describes information elements of the UE ID request sent by the AC to the EEC.

Table 8.14.3.19-1: UE ID request

Information element	Status	Description
EAS ID list	M	List of EAS ID(s) the AC requires to know the associated AF-specific UEID(s) for.
Security credentials	M	Security credentials of the AC sending the UE ID request.

NOTE: It is out of scope of this release of this specification how to ensure EAS ID list IE only contains the EAS IDs that are associated with the AC requesting the UE ID(s).

8.14.3.20 UE ID response

Table 8.14.3.20-1 describes information elements of the UE ID response sent by the EEC to the AC.

Table 8.14.3.20-1: UE ID response

Information element	Status	Description
Successful response	O	Indicates that the UE ID request was successful.
> UE ID list	M	List of all the Edge UE IDs or AF-specific UE IDs the AC asked for in the request and is authorized to use as per EAS ID(s).
>> UE ID	M	Edge UE ID or AF-specific UE ID
>> UE ID type	M	Indication whether the UE ID is CN assigned AF-specific UE ID or Edge UE ID.
>> EAS ID	M	Associated EAS ID
Failure response	O	Indicates that the UE ID request failed.
> Cause	M	Provides the cause for UE ID request failure.

8.14.4 APIs

8.14.4.1 General

Table 8.14.4.1-1 illustrates the API exposed by EEC.

Table 8.14.4.1-1: EEC API

API Name	API Operations	Operation Semantics	Consumer(s)
Eeec_ACRegistration	Request	Request/Response	AC
	Update		
	Deregister		
Eeec_EASDiscovery	Request	Request/Response	AC
Eeec_ACRTrigger	Request	Request/Response	AC
Eeec_Services	Subscribe	Subscribe/Notify	AC
	Notify		
	UpdateSubscription		
	Unsubscribe		
Eeec_UEId	Request	Request/Response	AC

8.14.4.2 Eeec_ACRegistration API

8.14.4.2.1 Eeec_ACRegistration_Request operation

API operation name: Eeec_ACRegistration_Request

Description: The consumer requests to register the AC on the EEC.

Inputs: See clause 8.14.3.2.

Outputs: See clause 8.14.3.3.

See clause 8.14.2.2.2 for details of usage of this operation.

8.14.4.2.2 Eeec_ACRegistration_Update operation

API operation name: Eeec_ACRegistration_Update

Description: The consumer requests to update the registered information of the AC on the EEC.

Inputs: See clause 8.14.3.4.

Outputs: See clause 8.14.3.5.

See clause 8.14.2.2.3 for details of usage of this operation.

8.14.4.2.3 Eeec_ACRegistration_Deregister operation

API operation name: Eeec_ACRegistration_Deregister

Description: The consumer requests to de-register the AC from the EEC.

Inputs: See clause 8.14.3.6.

Outputs: See clause 8.14.3.7.

See clause 8.14.2.2.4 for details of usage of this operation.

8.14.4.3 Eeec_EASDiscovery API

8.14.4.3.1 Eeec_EASDiscovery_Request operation

API operation name: Eeec_EASDiscovery_Request

Description: The consumer requests for one time EAS discovery information.

Inputs: See clause 8.14.3.8.

Outputs: See clause 8.14.3.9.

See clause 8.14.2.3 for details of usage of this operation.

8.14.4.4 Eeec_ACRTrigger API

8.14.4.4.1 Eeec_ACRTrigger_Request operation

API operation name: Eeec_EASDiscovery_Request

Description: The consumer requests to trigger ACR.

Inputs: See clause 8.14.3.10.

Outputs: See clause 8.14.3.11.

See clause 8.14.2.4 for details of usage of this operation.

8.14.4.5 Eeec_Services API

8.14.4.5.1 Eeec_Services_Subscribe operation

API operation name: Eeec_Services_Subscribe

Description: The consumer subscribes for EEC Services related events.

Inputs: See clause 8.14.3.12.

Outputs: See clause 8.14.3.13.

See clause 8.14.2.5.2 for details of usage of this operation.

8.14.4.5.2 Eeec_Services_Notify operation

API operation name: Eeec_Services_Notify

Description: The consumer is notified about EEC Services related events.

Inputs: See clause 8.14.3.14.

Outputs: None.

See clause 8.14.2.5.3 for details of usage of this operation.

8.14.4.5.3 Eeec_Services_UpdateSubscription operation

API operation name: Eeec_Services_UpdateSubscription

Description: The consumer updates an existing subscription for EEC Services related events.

Inputs: See clause 8.14.3.15.

Outputs: See clause 8.14.3.16.

See clause 8.14.2.5.4 for details of usage of this operation.

8.14.4.5.4 Eeec_Services_Unsubscribe operation

API operation name: Eeec_Services_Unsubscribe

Description: The consumer unsubscribes for the previously subscribed EEC Services related events.

Inputs: See clause 8.14.3.17.

Outputs See clause 8.14.3.18.

See clause 8.14.2.5.5 for details of usage of this operation.

8.14.4.6 Eeec_UEId API

8.14.4.6.1 Eeec_UEId_Request operation

API operation name: Eeec_UEId_Request

Description: The consumer requests for EAS specific UE ID.

Inputs: See clause 8.14.3.19.

Outputs: See clause 8.14.3.20.

See clause 8.14.2.6 for details of usage of this operation.

8.15 EAS Information provisioning

8.15.1 General

EAS information provisioning procedure allows the EEC to exchange information with the EES about selected EAS and/or ACR scenario selection.

When service continuity is required, ACR scenarios may be combined to perform ACR detection in one or more of the EEC, the EES and the EAS; the related procedures are specified in clauses 8.15.2, 8.6.3 and referred to in clause 8.8.2. The selection of ACR scenario(s) may be performed by the EEC or the EES for a given AC and the selected EAS from the common supported ACR scenarios of AC, EEC, selected EES and selected EAS. The selection of ACR scenario(s) for each EAS in EAS bundles may be performed separately by the EEC or the EES (or the main EES in case of bundle EAS served by multiple EESs, which is the EES registering the main EAS) for a given AC and the selected EAS(s) in a bundle, based on the service continuity support by AC, EEC, EES(s) and EAS(s) when the coordinated ACR need to be performed for the bundle EAS. In addition, the EEC or EES can further determine the one or more ACR scenario(s) for the selected EAS based on the AC service KPI.

NOTE: How to select ACR scenario(s) at the EEC or EES considering AC service KPI is implementation specific.

Instantiable EAS Information may be provided to the EEC in EAS discovery response and EAS discovery notification, as specified in clause 8.5.3.3 and 8.5.3.6. Triggering the instantiation of an EAS by the EEC may be announced to the EES by including the selected EASID in the EAS information provisioning request without including the selected EAS endpoint.

The EAS information provisioning request types supported are:

- "ACR scenario selection announcement". Inform the EES about the EAS that has been selected by the EEC and may provide the selected ACR scenario list to the EES. For the EAS bundles scenario, the selected bundled EAS(s) and the selected ACR scenario list for EAS bundles by EEC are included and notified to the EES.
- "ACR scenario selection request". Inform the EES to perform ACR scenario selection. For the EAS bundles scenario, the request may inform the EES to determine the ACR scenario list for EAS bundles.
- "EAS selection request". Inform the EES of EAS selection, e.g. for Application Group.

8.15.2 Procedure

8.15.2.1 General

8.15.2.2 EAS Information provisioning

Pre-conditions:

1. The EEC has performed service provisioning procedure
2. The EEC has performed the EAS discovery procedure

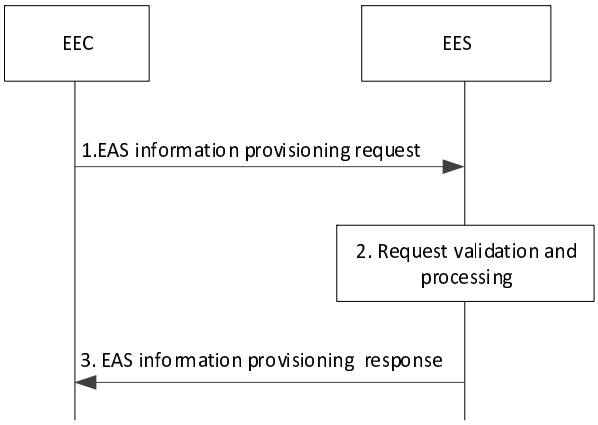

Figure 8.15.2.2-1: EAS information provisioning

1. The EEC sends the EAS information provisioning request to the EES:

   a- "ACR scenario selection announcement". The request may include ACR scenario list selected by the EEC, EEC security credentials, selected EASID, selected EAS endpoint, EECID and ACID. For the EAS bundles scenario, the request may include the ACR scenario list for EAS bundles selected by the EEC.

   b- "ACR scenario selection request". The request may include AC profile, EEC service continuity support, EEC security credentials, EECID and ACID.

   c- " EAS selection". Informs the EES of EAS selection. When Application Group information is included in the request, the EAS provided is considered Common EAS for Application Group.

   The EAS information provisioning request may include associated EES(s) endpoint and the DNAIs and service area of the selected EAS(s).

   NOTE 1: It is up to implementation how it is determined that EES no longer serves the application group.

If the EEC has selected an EAS which is instantiable but not yet instantiated, the EEC includes the selected EASID without including the selected EAS endpoint in the request.

The request may contain the associated EES(s) information along with the bundle EAS information (i.e. list of EASID) and the bundle EAS type indicating direct bundle, each associated EES(s) is along with part of or all the list of EASID, when EEC determines the associated EES(s) based on the EDN configuration information and bundle EAS information (e.g. list of EASID and direct bundle type).

2. Upon receiving the request from the EEC, the EES validates the EEC information request and verifies if the EEC is authorized for this operation.

   a- "ACR scenario selection announcement". The EES may send the ACR Selection notification to the selected EAS if the EAS has subscribed and if EES allows EEC based ACR scenario selection. Otherwise, EES may respond with status failure and include appropriate reason. For the EAS bundles scenario, the EES may send the ACR selection notification to the bundled EAS(s).

   b- "ACR scenario selection request". The EES selects the ACR scenario list and may send the ACR Selection notification to the selected EAS if the EAS has subscribed. The EES may include the ACR scenario list in the EAS information provisioning response. For the EAS bundles scenario, the EES selects the ACR scenario list for EAS bundles based on the AC/EEC/EES(s)/EAS(s) service continuity support, and sends the ACR scenario list to the bundled EAS(s).

   c- "EAS selection". When Application Group information is not provided, the EES determines that the EAS in the request is providing services to the AC with the indicated ACID e.g. for EEC Context handling purposes as described in clause 8.9. When Application Group information is included in the request, the EAS provided is considered Common EAS for the Application Group.

NOTE 2: Further clarification for EAS selection may be needed.

If the EEC or EES selected ACR scenario list for EAS bundle includes EAS executed ACR scenario (as described in 8.8.2.8), the EES also sends DNAIs and service area of the selected EAS(s) to the main EAS in the ACR selection notification.

The request may contain the associated EES(s) information along with the bundle EAS information (i.e. list of EASID) and the bundle EAS type indicating direct bundle, each associated EES(s) is along with part of or all the list of EASID, when EEC determines the associated EES(s) based on the EDN configuration information and bundle EAS information (e.g. list of EASID and direct bundle type).

If the request contains selected EAS ID and selected EAS Endpoint, the EES may apply the EAS traffic influence with the N6 routing information of the EAS in the 3GPP Core Network, based on application KPIs and if the EAS traffic influence was not done before (e.g. neither in EAS discovery procedure nor the EAS perform traffic influence).

When the selection is that of a common EAS for application group, the request message may contain the list of EESs for a certain Application Group ID, received from the ECS in the service provisioning response message. This application group related information may be used for further common EAS announcement(s) between EES(s). In the case of no ECS-ER, if the request message does not contain the list of EESs for a certain Application Group ID, then the EES determines the other EESs to which announce common EAS request needs to be sent as described in clause 8.8.3.3. If there is ECS-ER, the EEC selected EAS is used in interaction between the EES and ECS-ER, as described in clause 8.20.2.3 to store the common EAS information., If the ECS-ER provides a different common EAS information in the response it is forwarded to the EEC in the EAS information provisioning response. If the ECS-ER-provided common EAS is registered to another EES, then the EES endpoint of the EES where the common EAS is registered is also included in the EAS information provisioning response.

If the request contains the selected EASID and the selected EAS endpoint is not included, the EES verifies if instantiation of EAS is needed and may trigger the ECSP management system to instantiate the EAS as in clause 8.12.

When the request contains EEC Service Continuity Support IE and the EEC context has been established, the EES includes the IE into the EEC context described in Table 8.2.8-1.

NOTE 2: EES can also influence the EAS traffic in advance.

NOTE 3: It is up to the AC to decide when to connect to the selected EAS (either immediately or wait for a while) once the AC knows the selected EAS.

3. If the processing of the request was successful, the EES sends an EAS information provisioning response to the EEC indicating a successful status. If an EEC context has been established, the response also includes the list of selected ACR scenario(s) into the session context IE within EEC context as described in Table 8.2.8-2; otherwise, the EES shall indicate a failure status and include appropriate reasons. If the EES has triggered EAS instantiation based on the EAS information provisioning request and obtained the newly instantiated EAS information, the response contains information about the newly instantiated EAS, including the EAS endpoint information.

The EEC, EES and EAS (or the bundled EAS(s)) use the selected ACR scenario list to determine if they should perform ACR detection and/or ACR decision.

Upon receiving the EAS information provisioning response, if the response includes instantiated EAS information, the EEC uses the endpoint information to subscribe to ACR event notification, as needed, and provides necessary notifications to the AC.

NOTE 4: Other ACR selection criteria are out of scope of the current specification.

NOTE 5: The common supported ACR scenarios is decided as part of the EAS discovery and selection procedure.

For the "EAS selection" case, in the case of no ECS-ER, the selected common EAS shall be announced to other relevant EES(s) as per procedure in clause 8.19.

8.15.3 Information flows

8.15.3.1 General

The information flows are specified for EAS information provisioning request and response.

8.15.3.2 EAS information provisioning request

Table 8.15.3.2-1 describes the information elements for EAS information provisioning request from the EEC to the EES.

Table 8.15.3.2-1: EAS information provisioning request

Information element	Status	Description
EECID	M	The identifier of the EEC.
ACID	M	The identifier of the AC.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Selected EAS ID(s)	O	The identifier(s) of the selected EAS or the selected EAS(s) for EAS bundles, which is either instantiated or instantiable.
Application Group ID (NOTE 4)	O	Application group identifier as defined in 7.2.11.
List of EES(s) (NOTE 4)	O	List of EES information (e.g. address information) corresponding to the Application group ID which is used for the common EAS announcement between these EESs as provided by ECS during service provisioning.
Selected EAS Endpoint(s)	O	The endpoint(s) of the selected EAS or the selected EAS(s) for EAS bundles
DNAIs and service area of the selected EAS(s)	O	For each selected EAS ID, it includes the DNAIs and/or service area for EAS bundles, as described in "EAS Geographical Service Area" IE, "EAS Topological Service Area" IE and "List of EAS DNAI(s)" IE of Table 8.2.4-1.
Request type	O	Request types: - ACR scenario selection announcement - ACR scenario selection request - EAS selection
Selected ACR scenario list (NOTE 1)	O	The list of ACR scenarios (or the list of ACR scenarios for EAS bundles) selected by the EEC
AC Profile (NOTE 2, NOTE 3)	O	AC Profile as described in Table 8.2.2-1
EEC Service Continuity Support (NOTE 2, NOTE 5)	O	Indicates if the EEC supports service continuity or not. The IE indicates which ACR scenarios are supported by the EEC, also indicates the EEC ability (e.g. EAS bundle information) of handling bundled EAS ACR.
Associated EES(s) endpoint	O	EES information of the other EES(s) which support the direct bundled EAS, within the same EDN, and associated with the EASID list.
CAS information	O	Target CAS information received from AC.
NOTE 1: The IE may be present only if Selected EASID(s) and Selected EAS Endpoint(s) are present and Request type is "ACR scenario selection announcement" NOTE 2: The IEs are present only if request type is “ACR scenario selection request” NOTE 3: The IE is present if AC Profile is not shared to EES previously NOTE 4: This IE may be present only if the request type is "EAS selection". NOTE 5: The EAS bundle information is not applicable for proxy type of EAS bundle.		

8.15.3.3 EAS information provisioning response

Table 8.15.3.2-1 describes the information elements for EAS information provisioning response from the EES to the EEC.

Table 8.15.3.3-1: EAS information provisioning response

Information element	Status	Description
Successful response (NOTE 1)	O	Indicates that the request was successful.
> Selected ACR scenario list (NOTE 2)	O	The list of ACR scenarios (or the list of ACR scenarios for EAS bundles) selected by the EES
> Instantiated EAS Information (NOTE 3)	O	Instantiated EAS information. Each element includes the information described below.
>> EAS Profile	M	The profile of the instantiated EAS.Each element is described in clause 8.2.4.
>> EES Endpoint	O	The endpoint address (e.g. URI, IP address) of the EES
>> Lifetime	O	Time interval or duration during which the information elements in the EAS profile is valid and supposed to be cached in the EEC (e.g. time-to-live value for an EAS Endpoint)
> Common EAS endpoint (NOTE 4)	O	This IE includes common EAS endpoint. This IE shall be provided only when the EEC indicates EAS selection for an application group in the request and if the EES determines a different common EAS (e.g. from ECS-ER).
> Common EES endpoint (NOTE 4)	O	This IE includes common EES endpoint. It shall be provided when common EAS endpoint IE is included and the common EAS is registered to a different EES than the EES responding to the EEC.
Failure response (NOTE 1)	O	Indicates that the request failed.
> Cause	O	Indicates the failure cause.
NOTE 1: One of these IEs shall be present in the message. NOTE 2: Only if request type is "ACR scenario selection request". NOTE 3: Only if request does not include selected EAS endpoint. NOTE 4: Only if request type is "EAS selection".		

8.15.4 APIs

8.15.4.1 General

Table 8.15.4.1-1 illustrates the API for EAS Information provisioning.

Table 8.15.4.1-1: Eees_EASInformationProvisioning API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EASInformationProvisioning	Declare	Request/Response	EEC

8.15.4.2 Eees_EASInformationProvisioning_Declare operation

API operation name: Eees_EASInformationProvisioning_Declare

Description: The consumer declares EAS information to the EES.

Inputs: See clause 8.15.3.2.

Outputs: See clause 8.15.3.3.

See clause 8.15.2.2 for details of usage of this operation.

8.16 EEC triggering service to initiate procedures over EDGE-1 or EDGE-4

8.16.1 General

The functional entities of the Edge Enabler Layer can utilize the Application Triggering services (or Device Triggering) provided by the 3GPP core network via NEF or SCEF (see clause 4.4.5 in 3GPP TS 23.501 [2], clause 4.13.2, 5.2.6.5.2 in TS 23.502 [3], and clause 4.5.1 TS 23.682 [17]) to enable for ECS or EES to perform EEC Triggering, i.e., to trigger EEC to perform the procedures over EDGE-1 or EDGE-4 (e.g., service provisioning or EAS discovery).

If application triggering is supported and required by the EEC, the EEC may indicate to the ECS or EES that the EEC triggering service is needed.

The triggering mechanism is used by the ECS and EES for messaging to EEC by invoking application triggering service as specified for Nnef_Trigger_Delivery service in clause 4.13.2 of TS 23.502 [3] or the device triggering procedure via T8 in clause 5.17 of TS 23.682 [17]. The ECS can use it to trigger the EEC to initiate service provisioning request (as per clause 8.3.3.2.2) when the EDN configuration information in the ECS is updated. The EES can use it to trigger the EEC to initiate EAS discovery request (as per clause 8.5.2.2) when the EAS profile in the EES is updated.

NOTE: In this release, the ECS and EES can determine the port ID for EEC triggering service based on implementation.

After receiving the EEC triggering indication in the Service Provisioning subscription or EAS discovery subscription request as described in clause 8.3.3 and 8.5.2, when ECS or EES performs EEC triggering service by invoking the application triggering service, the ECS or EES includes, in the Trigger Payload, Triggering Entity Information (identifier and endpoint address of the triggering EES or ECS) and optionally Trigger Description, which indicates the procedure (e.g., service provisioning or EAS discovery) to be initiated by the EEC. Upon receiving the Trigger Payload, the EEC selects which procedure needs to be performed according to the received Trigger Description and initiates the selected procedure towards either EES or ECS indicated by the Triggering Entity Information in the Trigger Payload.

NOTE: If the Trigger Description is not given, application port information can be used by the EEC to select the procedure to be triggered.

8.17 Support for roaming and federation

8.17.1 General

This clause describes procedures to support roaming and federation. In this document, roaming and federation are distinguished as follows.

Roaming is a scenario where a UE is served by a visited PLMN. The UE may be served by ECS connected with the VPLMN (i.e., V-ECS). The UE may also be served by ECS connected with the HPLMN (i.e., H-ECS) via local breakout (see clause 6.2a.2) or via home-routed session (see clause 6.2a.3).

Federation is a scenario where a UE consumes edge services involving two or more ECSPs. The architecture for federation support is described in clause 6.2b. Different ECSP's ECSs are connected by EDGE-10 and exchange ECS configuration information and EDN configuration information. A UE may consume federation services while non-roaming or roaming.

8.17.2 Procedures

8.17.2.1 General

Following sets of procedures are defined to support roaming and federation:

- Registration;
- ECS discovery via ECS-ER; and

- Service provisioning information retrieval.

8.17.2.2 Registration

8.17.2.2.1 General

Following procedures are defined for ECS registration:

- ECS registration procedure;
- ECS registration update procedure; and
- ECS de-registration.

8.17.2.2.2 ECS registration

ECS registers with the ECS-ER and provides the information included in the ECS profile. Figure 8.17.2.2.2-1 illustrates the procedure.

Pre-conditions:

1. The ECS has the address (e.g. URI) of the ECS-ER.

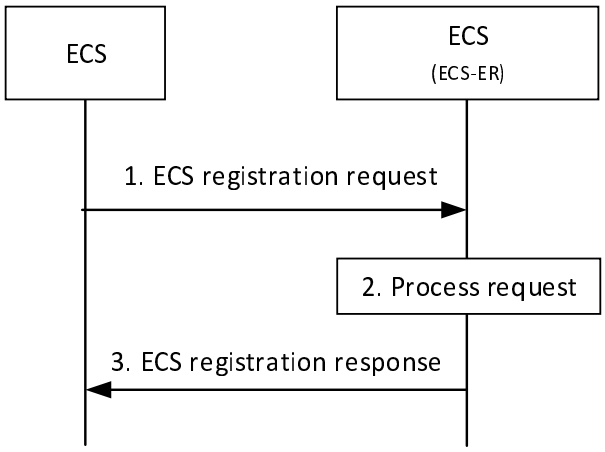

Figure 8.17.2.2.2-1: ECS registration procedure

1. The ECS sends the ECS registration request to the ECS-ER. The request from the ECS includes ECS profile and security credentials. The request may include a proposed expiration time for the registration, and may include list of partner ECSPs that are allowed to receive its information. The request may also include DNN and S-NSSAI information for roaming UEs to establish a PDU session towards the ECS as specified in 3GPP TS 23.548 [20].
2. Upon receiving the request from the ECS, the ECS-ER verifies the security credentials of the ECS and stores the ECS registration information received in step 1.
3. The ECS-ER sends an ECS registration response indicating success or failure of the registration operation. The ECS-ER may provide an expiration time to indicate to the ECS when the registration will automatically expire. To maintain the registration, the ECS sends a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the ECS-ER treats the ECS as implicitly de-registered.

8.17.2.2.3 ECS registration update

Figure 8.17.2.2.3-1 illustrates the ECS registration update procedure.

Pre-conditions:

1. The ECS is registered with the ECS-ER.

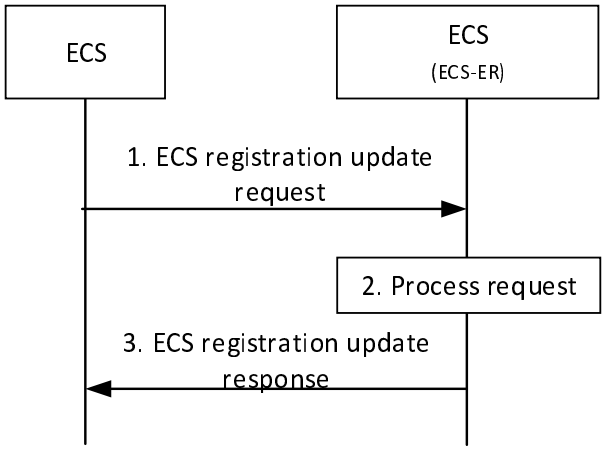

Figure 8.17.2.2.3-1: ECS registration update procedure

1. The ECS sends the ECS registration update request to the ECS-ER. The request from the ECS includes security credentials and may include updated ECS profile that may include updated DNN and S-NSSAI information, and an updated list of partner ECSPs that are allowed to receive its information. The request may also include a proposed expiration time for the updated registration.
2. Upon receiving the request from the ECS, the ECS-ER verifies the security credentials of the ECS and updates the stored the ECS registration information as received in step 1.
3. The ECS-ER sends an ECS registration update response indicating success or failure of the registration update operation. The ECS-ER may provide an updated expiration time to indicate to the ECS when the updated registration will automatically expire. To maintain the registration, the ECS sends another registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the ECS-ER treats the ECS as implicitly de-registered.

8.17.2.2.4 ECS de-registration

Figure 8.17.2.2.4-1 illustrates the ECS de-registration procedure.

Pre-conditions:

1. The ECS is registered with the ECS-ER.

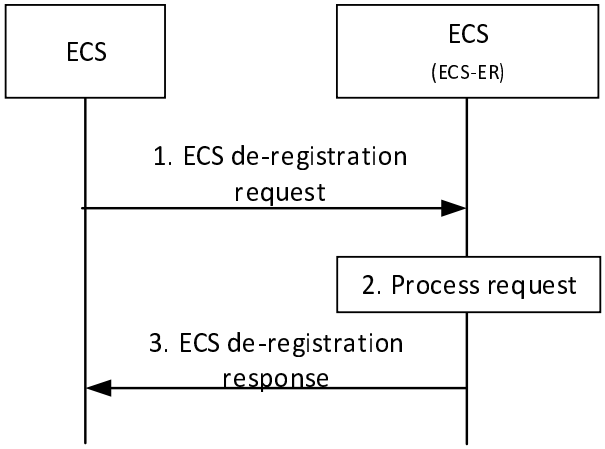

Figure 8.17.2.2.4-1: ECS de-registration procedure

1. The ECS sends the ECS de-registration request to the ECS-ER. The request from the ECS includes its security credentials.
2. Upon receiving the request from the ECS, the ECS-ER verifies the security credentials of the ECS and de-registers the ECS.
3. The ECS-ER sends an ECS de-registration response indicating success or failure of the de-registration operation.

8.17.2.3 ECS discovery via ECS-ER

8.17.2.3.1 General

Following procedures are supported for ECS discovery via ECS-ER:

- Request-response procedure;
- Subscribe-notify procedures, including:
  - Subscription procedure;
  - Notification procedure;
  - Subscription update procedure; and
  - Unsubscribe procedure.

8.17.2.3.2 Request-response model

When required to find a suitable partner ECS, the ECS queries the ECS-ER by providing information such as the location of the UE, applications required by the UE etc. In response the ECS-ER provides ECS profile of partner ECS(s) providing the required application at the location indicated by the ECS. Figure 8.17.2.3.2-1 illustrates the procedure.

Pre-conditions:

1. The ECS has the address (e.g. URI) of the ECS-ER.

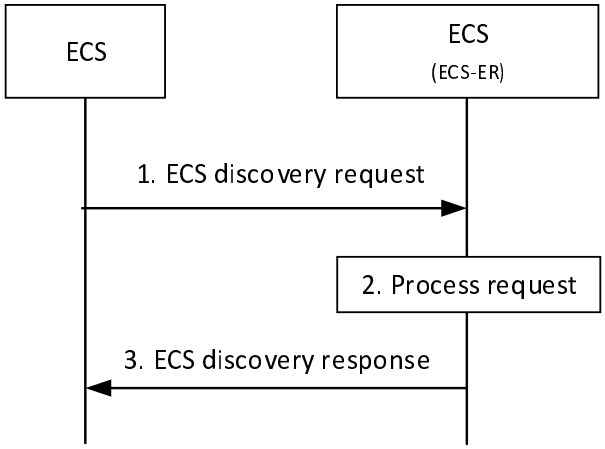

Figure 8.17.2.3.2-1: ECS querying ECS-ER

1. The ECS sends a ECS discovery request to the ECS-ER. The request contains security information of the ECS, and optionally AC profile(s) and UE's current location to filter ECS. If the UE hosting the EEC is roaming in a V-PLMN (determined using the serving PLMN information in the received service provisioning request, or by interacting with the H-PLMN), then the ECS discovery request includes the information of the serving PLMN i.e. the V-PLMN.
2. The ECS-ER authorizes the received request. If authorized, the ECS-ER processes the request and gathers the information of partner ECS(s) that can satisfy the query parameters received in step 1.
3. The ECS-ER sends a ECS discovery response to the ECS. The response includes ECS profile of the Partner ECS(s) available in the H-PLMN and/or the V-PLMN, depending on the serving PLMN of the UE as indicated in step 1 and may include DNN and S-NSSAI information for roaming UEs to establish a PDU session to the Partner ECS as specified in 3GPP TS 23.548 [20]. The ECS caches the received information for further use.

NOTE: The ECS sending the ECS discovery request can also be an ECS-ER.

8.17.2.3.3 Subscribe-notify model

8.17.2.3.3.1 General

8.17.2.3.3.2 Subscribe

Figure 8.17.2.3.3.2-1 illustrates the procedure.

Pre-conditions:

1. The ECS has the address (e.g. URI) of the ECS-ER.

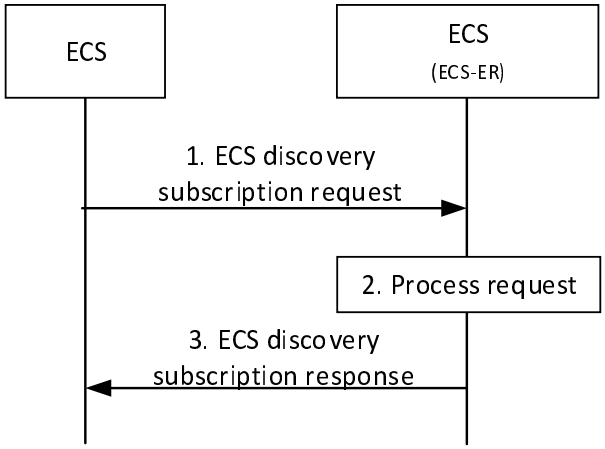

Figure 8.17.2.3.3.2-1: ECS discovery subscription procedure

1. The ECS sends a ECS discovery subscription request to the ECS-ER. The request contains security information of the ECS. The request optionally contains AC profile(s), UE's location information and the PLMN information.
2. The ECS-ER authorizes the received request. If authorized, the ECS-ER creates and stores the subscription.
3. The ECS-ER sends a ECS discovery subscription response to the ECS which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EEC shall send a ECS discovery subscription update request prior to the expiration time. If a ECS discovery subscription update request is not received prior to the expiration time, the ECS-ER shall treat the ECS as implicitly unsubscribed.

8.17.2.3.3.3 Notify

Figure 8.17.2.3.3.3-1 illustrates the procedure.

Pre-conditions:

1. The ECS has subscribed for ECS discovery.

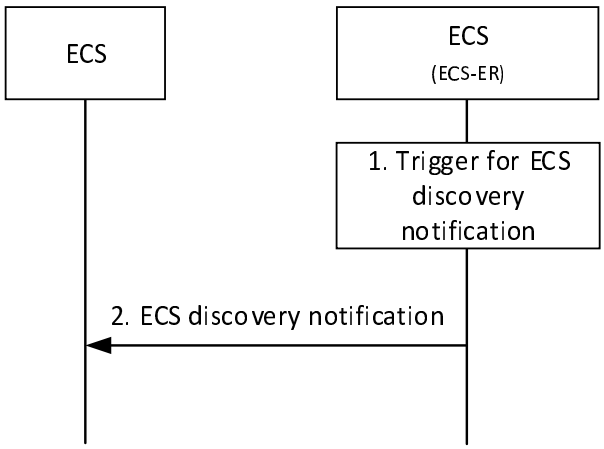

Figure 8.17.2.3.3.3-1: ECS discovery notification

1. An event occurs at the ECS-ER that satisfies trigger conditions for ECS discovery notification, e.g. after new ECS registration.

2. The ECS-ER sends a ECS discovery notification to the ECS. The notification includes the ECS profile of the Partner ECS(s) as requested in the subscription and may include information for roaming UEs to establish a PDU session to the Partner ECS as specified in 3GPP TS 23.548 [20]. The ECS caches the information for further use.

8.17.2.3.3.4 Subscription update

Figure 8.17.2.3.3.4-1 illustrates the procedure.

Pre-conditions:

1. The ECS has subscribed for ECS discovery.

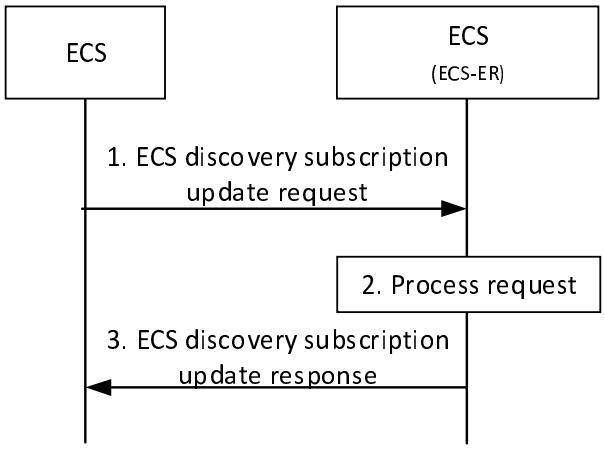

Figure 8.17.2.3.3.4-1: ECS discovery subscription update procedure

1. The ECS sends a ECS discovery subscription update request to the ECS-ER. The request contains security information of the ECS and may include an AC profile(s), UE's location information and the PLMN information.
2. The ECS-ER authorizes the received request. If authorized, the ECS-ER updates the stored subscription.
3. The ECS-ER sends an ECS discovery subscription update response indicating success or failure of the subscription update operation. The ECS-ER may provide an updated expiration time to indicate to the ECS when the updated subscription will automatically expire. To maintain the subscription, the ECS needs to send another subscription update request prior to the expiration time. If a subscription update request is not received prior to the expiration time, the ECS-ER treats the ECS as implicitly unsubscribed.

8.17.2.3.3.5 Unsubscribe

Figure 8.17.2.3.3.5-1 illustrates the procedure.

Pre-conditions:

1. The ECS has subscribed for ECS discovery.

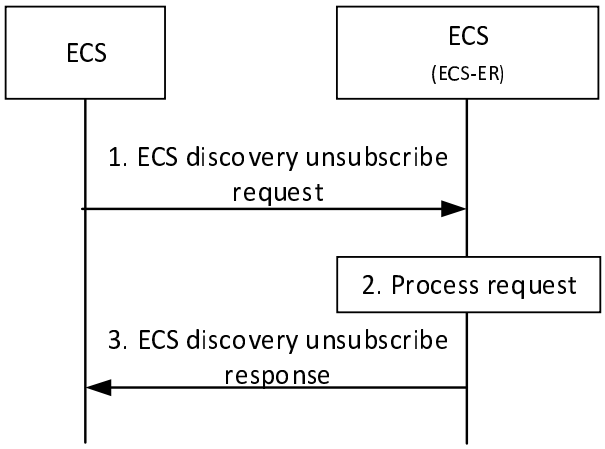

Figure 8.17.2.3.3.5-1: ECS discovery unsubscribe procedure

1. The ECS sends a ECS discovery unsubscribe request to the ECS-ER. The request contains security information of the ECS and the subscription identifier.
2. The ECS-ER authorizes the received request. If authorized, the ECS-ER cancels the stored subscription.
3. The ECS-ER sends an ECS unsubscribe response indicating success or failure of the subscription update operation.

8.17.2.4 Service provisioning information retrieval

8.17.2.4.1 General

When required to retrieve Service provisioning information from a partner ECS, the ECS queries the partner ECS by providing information such as required applications, location, service continuity support information and connectivity information. In response the partner ECS provides Service provisioning information of EDNs satisfying the requirements.

The following clauses specify procedures, information flows and APIs for service provisioning information retrieval.

In the following procedures, ECS sending the request can be an ECS-ER of an ECSP and Partner ECS receiving the request can be the ECS-ER of the partner ECSP.

NOTE: Partner ECS can also be a V-ECS based on the roaming status of the UE for which the service provisioning information is being retrieved.

8.17.2.4.2 Procedures

8.17.2.4.2.1 General

Following procedures are supported for service provisioning:

- Request-response model; and
- Subscribe-notify model.

8.17.2.4.2.2 Request-response model

Figure 8.17.2.4.2.2-1 illustrates service provisioning procedure based on request/response model.

Pre-condition(s):

1. ECS has received a service provisioning request from an EEC or T-EES discovery request from an EES.

2. The ECS has the ECS profile of the partner ECS (e.g. through pre-configuration, OAM configuration or ECS discovery).

3. Required federation agreement exists between the ECSPs.

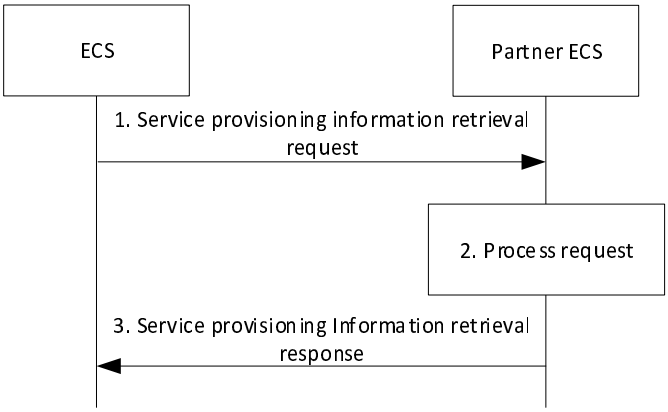

Figure 8.17.2.4.2.2-1: Service provisioning information retrieval – Request/Response

1. The ECS sends a service provisioning information retrieval request to the partner ECS. The request contains security information of the ECS, and optionally AC profile(s) and UE's current location. If the UE hosting the EEC is roaming in a V-PLMN (determined using the serving PLMN information in the received service provisioning request, or by interacting with the H-PLMN), then the service provisioning information retrieval request includes the information of the serving PLMN i.e. the V-PLMN.

2. The partner ECS authorizes the received request. If authorized, the partner ECS processes the request and gathers the provisioning information of the EDNs that can satisfy the query parameters received in step 1.

3. The partner ECS sends a service provisioning information retrieval response to the ECS. The response includes provisioning information of the EDNs that can satisfy the query parameters received in step 1 and may include lifetime information. The ECS caches the received information for further use. If the Lifetime IE is included, then the ECS may reuse the retrieved information only for the duration specified by the Lifetime IE, without the need to repeat step 1.

NOTE: Only the information allowed by the federation agreement is included in the service provisioning information response.

8.17.2.4.2.3 Subscribe-notify model

8.17.2.4.2.3.1 General

8.17.2.4.2.3.2 Subscribe

Figure 8.17.2.4.2.3.2-1 illustrates service provisioning information subscription request between an ECS and its partner ECS.

Pre-condition(s):

1. The ECS has the ECS configuration information of the partner ECS (e.g. through pre-configuration, OAM configuration or ECS discovery).

2. Required federation agreement exists between the ECSPs.

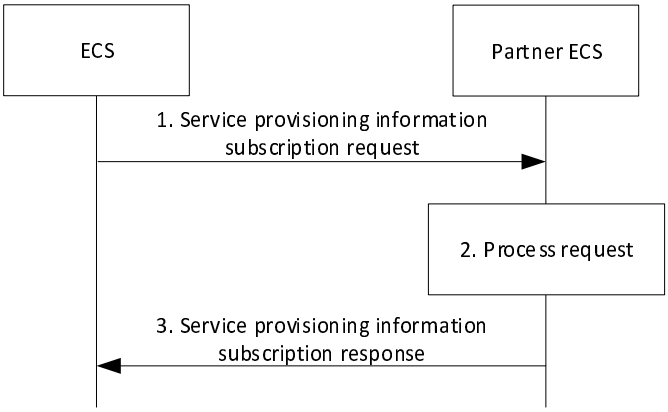

Figure 8.17.2.4.2.3.2-1: Service provisioning information retrieval – Subscribe

1. The ECS sends a service provisioning information subscription request to the partner ECS. The request contains security information of the ECS, Notification Target Address (e.g. URL), federation information, Service Provisioning filters.
2. The partner ECS authorizes the received request. If authorized, the partner ECS creates a subscription and stores the subscription.
3. The partner ECS sends a service provisioning information subscription response to the ECS. The response includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the ECS shall send a service provisioning information subscription update request prior to the expiration time. If a service provisioning information subscription update request is not received prior to the expiration time, the partner ECS shall treat the ECS as implicitly unsubscribed.

8.17.2.4.2.3.3 Notify

Figure 8.17.2.4.2.3.3-1 illustrates the service provisioning information notification procedure between an ECS and its partner ECS.

Pre-conditions:

1. ECS has subscribed for service provisioning information from the partner ECS as specified in clause 8.17.2.4.2.3.2.

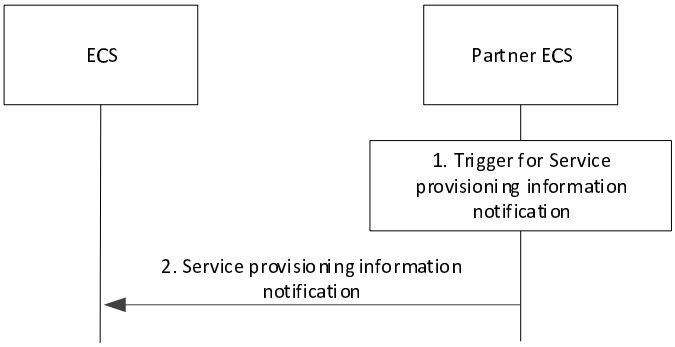

Figure 8.17.2.4.2.3.3-1: Service provisioning information notification

1. An event occurs at the partner ECS that satisfies trigger conditions for notifying (e.g. to provide a change in information about available EASs) a subscribed ECS.
2. The Partner ECS sends a service provisioning information notification to the ECS. The notification includes updated provisioning information of the EDNs that can satisfy the query parameters received during subscription

and may include lifetime information. The ECS caches the received information for further use. If the Lifetime IE is included, then the ECS may reuse the received information only for the duration specified by the Lifetime IE.

NOTE: Only the information allowed by the federation agreement is included in the service provisioning information notification.

8.17.2.4.2.3.4 Subscription update

Figure 8.17.2.4.2.3.4-1 illustrates service provisioning information subscription update request between an ECS and its partner ECS.

Pre-condition(s):

1. ECS has subscribed for service provisioning information from the partner ECS as specified in clause 8.17.2.4.2.3.2.

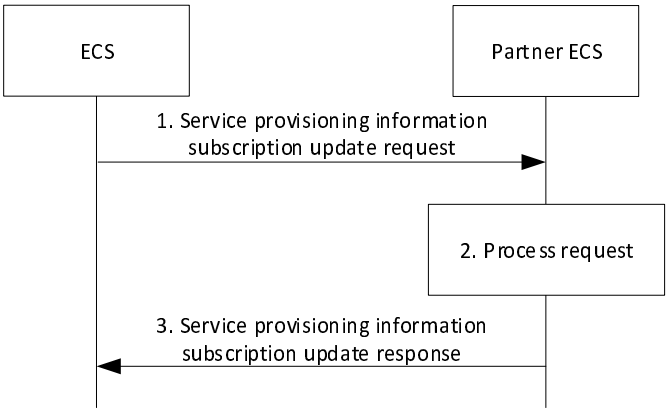

Figure 8.17.2.4.2.3.4-1: Service provisioning information retrieval – Subscription update

1. The ECS sends a service provisioning information subscription update request to the partner ECS. The request contains security information of the ECS and subscription identifier, and may include updated Notification Target Address (e.g. URL), federation information, Service Provisioning filters, location information and PLMN information.
2. The partner ECS authorizes the received request. If authorized, the partner ECS updates the stored subscription.
3. The partner ECS sends a service provisioning information subscription update response to the ECS. The response may include updated expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the ECS shall send a service provisioning information subscription update request prior to the expiration time. If a service provisioning information subscription update request is not received prior to the expiration time, the partner ECS shall treat the ECS as implicitly unsubscribed.

8.17.2.4.2.3.5 Unsubscribe

Figure 8.17.2.4.2.3.5-1 illustrates service provisioning subscription update request between an ECS and its partner ECS.

Pre-condition(s):

1. ECS has subscribed for service provisioning information from the partner ECS as specified in clause 8.17.2.4.2.3.2.

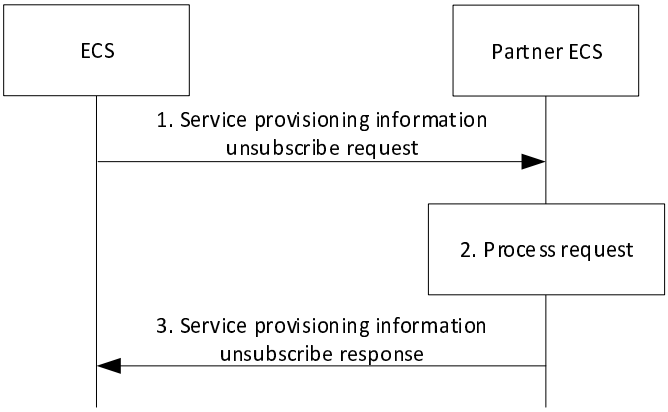

Figure 8.17.2.4.2.3.5-1: Service provisioning information retrieval – Unsubscribe

1. The ECS sends a service provisioning information unsubscribe request to the partner ECS. The request contains security information of the ECS and the subscription identifier.
2. The partner ECS authorizes the received request. If authorized, the partner ECS cancels the subscription.
3. The partner ECS sends a service provisioning information unsubscribe response to the ECS.

8.17.3 Information flows

8.17.3.1 General

Following information flows are specified for support of federation and roaming:

- ECS registration request and response;
- ECS registration update request and response;
- ECS registration de-registration request and response;
- ECS discovery request and response;
- ECS discovery subscription request and response;
- ECS discovery subscription update request and response;
- ECS discovery unsubscribe request and response;
- Service provisioning information retrieval request and response;
- Service provisioning information subscription request and response;
- Service provisioning information subscription update request and response; and
- Service provisioning information unsubscribe request and response.

8.17.3.2 ECS registration request

Table 8.17.3.2-1 describes the information elements for ECS registration request from the ECS to the ECS-ER.

Table 8.17.3.2-1: ECS registration request

Information element	Status	Description
ECS profile	M	Profile of the ECS as specified in clause 8.2.12
Security credentials	M	Security credentials of the ECS
Proposed expiration time	O	Proposed expiration time for the registration

8.17.3.3 ECS registration response

Table 8.17.3.3-1 describes the information elements for ECS registration response from the ECS-ER to the ECS.

Table 8.17.3.3-1: ECS registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the registration.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the registration never expires.
Failure response	O	Indicates that the registration request failed.
> Cause	O	Indicates the cause of registration request failure

8.17.3.4 ECS registration update request

Table 8.17.3.4-1 describes the information elements for ECS registration update request from the ECS to the ECS-ER.

Table 8.17.3.4-1: ECS registration update request

Information element	Status	Description
Updated ECS profile	O	Profile of the ECS as specified in clause 8.2.12
Security credentials	M	Security credentials of the ECS
Registration ID	M	Identifier of the registration to be updated
Proposed expiration time	O	Proposed expiration time for the registration

8.17.3.5 ECS registration update response

Table 8.17.3.5-1 describes the information elements for ECS registration update response from the ECS-ER to the ECS.

Table 8.17.3.5-1: ECS registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration update request was successful.
> Expiration time	O	Indicates the expiration time of the updated registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the updated registration never expires.
Failure response	O	Indicates that the registration update request failed.
> Cause	O	Indicates the cause of registration update request failure

8.17.3.6 ECS de-registration request

Table 8.17.3.6-1 describes the information elements for ECS de-registration request from the ECS to the ECS-ER.

Table 8.17.3.6-1: ECS de-registration request

Information element	Status	Description
Registration ID	M	Identifier of the registration.
Security credentials	M	Security credentials of the EES

8.17.3.7 ECS de-registration response

Table 8.17.3.7-1 describes the information elements for ECS de-registration response from the ECS-ER to the ECS.

Table 8.17.3.7-1: ECS de-registration response

Information element	Status	Description
Successful response	O	Indicates that the de-registration request was successful.
Failure response	O	Indicates that the de-registration request failed.
> Cause	O	Indicates the cause of de-registration request failure

8.17.3.8 ECS discovery request

Table 8.17.3.8-1 describes the information elements for ECS discovery request; from the ECS to the ECS-ER.

Table 8.17.3.8-1: ECS discovery request

Information element	Status	Description
ECS address	M	Endpoint information of ECS (e.g. URI, FQDN, IP address)
Security credentials	M	Security credentials of the ECS.
Federation information	O	List of information for different federation agreements related to the ECS
> ECSP identifiers	O	The list of ECSPs preferred by the ECS. This information is used by the ECS-ER to filter the discovered partner ECS information.
AC Profile(s)	O	Filter information about required services as described in Table 8.2.2-1.
Connectivity information	O	Connectivity information such as serving PLMN information where the services are required.
UE location	O	Location of the UE for which the services are required.

8.17.3.9 ECS discovery response

Table 8.17.3.9-1 describes the information elements for ECS discovery response from the ECS-ER to the ECS.

Table 8.17.3.9-1: ECS discovery response

Information element	Status	Description
Successful response	O	Indicates that the ECS discovery request was successful.
> List of ECS profiles	M	List of ECS profiles as described in clause 8.2.12.
> Lifetime	O	Time duration for which the ECS profiles are valid and supposed to be cached by the ECS.
Failure response	O	Indicates that the ECS discovery request failed.
> Cause	O	Indicates the cause of ECS discovery request failure.

8.17.3.10 ECS discovery subscription request

Table 8.17.3.10-1 describes the information elements for ECS discovery subscription request; from the ECS to the ECS-ER.

Table 8.17.3.10-1: ECS discovery subscription request;

Information element	Status	Description
ECS address	M	Endpoint information of ECS (e.g. URI, FQDN, IP address)
Security credentials	M	Security credentials of the ECS.
Notification Target Address	O	The Notification Target Address (e.g. URL) where the notifications destined for the ECS should be sent to.
Federation information	O	List of information for different federation agreements related to the ECS
> ECSP identifiers	O	The list of ECSPs preferred by the ECS. This information is used by the ECS-ER to filter the discovered partner ECS information.
AC Profile(s)	O	Filter information about required services as described in Table 8.2.2-1.
Connectivity information	O	Connectivity information such as serving PLMN information where the services are required.
UE location	O	Location of the UE for which the services are required.
Proposed expiration time	O	Proposed expiration time for the subscription

8.17.3.11 ECS discovery subscription response

Table 8.17.3.11-1 describes the information elements for ECS discovery subscription response from the ECS-ER to the ECS.

Table 8.17.3.11-1: ECS discovery subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.17.3.12 ECS discovery notification

Table 8.17.3.12-1 describes the information elements for ECS discovery notification request from the ECS-ER to the ECSR.

Table 8.17.3.12-1: ECS discovery notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the ECS-ER
List of ECS profiles	M	List of ECS profiles as described in clause 8.2.12.
Lifetime	O	Time duration for which the ECS profiles are valid and supposed to be cached by the ECS.

8.17.3.13 ECS discovery subscription update request

Table 8.17.3.13-1 describes the information elements for ECS discovery subscription update request from the ECS to the ECS-ER.

Table 8.17.3.13-1: ECS discovery subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials of the ECS.
Notification Target Address	O	The Notification Target Address (e.g. URL) where the notifications destined for the ECS should be sent to.
Federation information	O	List of information for different federation agreements related to the ECS
> ECSP identifiers	O	The list of ECSPs preferred by the ECS. This information is used by the ECS-ER to filter the discovered partner ECS information.
AC Profile(s)	O	Filter information about required services as described in Table 8.2.2-1.
Connectivity information	O	Connectivity information such as serving PLMN information where the services are required.
UE location	O	Location of the UE for which the services are required.
Proposed expiration time	O	Proposed expiration time for the subscription

8.17.3.14 ECS discovery subscription update response

Table 8.17.3.14-1 describes the information elements for ECS discovery subscription update response from the ECS-ER to the ECS.

Table 8.17.3.14-1: ECS discovery subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.17.3.15 ECS discovery unsubscribe request

Table 8.17.3.15-1 describes the information elements for ECS discovery unsubscribe request from the ECS to the ECS-ER.

Table 8.17.3.15-1: ECS discovery unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be unsubscribed
Security credentials	M	Security credentials of the ECS.

8.17.3.16 ECS discovery unsubscribe response

Table 8.17.3.16-1 describes the information elements for ECS discovery unsubscribe response from the ECS-ER to the ECS.

Table 8.17.3.16-1: ECS discovery unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.17.3.17 Service provisioning information retrieval request

Table 8.17.3.17-1 describes the information elements for Service provisioning information retrieval request from the ECS to a partner ECS.

Table 8.17.3.17-1: Service provisioning information retrieval request

Information element	Status	Description
ECS address	M	Endpoint information of ECS (e.g. URI, FQDN, IP address)
Security credentials	M	Security credentials of the ECS.
Federation information	O	List of information for different federation agreements related to the ECS
> Federation identifier	O	Identifier of the federation
> ECSP identifiers	O	The list of ECSPs preferred by the ECS. This information is used by the ECS-ER to filter the discovered partner ECS information.
AC Profile(s)	O	Filter information about required services as described in Table 8.2.2-1.
Connectivity information	O	Connectivity information such as serving PLMN information where the services are required.
UE location	O	Location of the UE for which the services are required.

8.17.3.18 Service provisioning information retrieval response

Table 8.17.3.18-1 describes the information elements for Service provisioning information retrieval response from the partner ECS to the ECS.

Table 8.17.3.18-1: Service provisioning information retrieval response

Information element	Status	Description
Successful response	O	Indicates that the Service provisioning information retrieval request was successful.
> List of EDN configuration information	M	List of EDN configuration information as defined in Table 8.3.3.3.3-2.
> Lifetime	O	Time duration for which the EDN configuration information is valid and supposed to be cached by the ECS.
Failure response	O	Indicates that the Service provisioning information retrieval request failed.
> Cause	O	Indicates the cause of Service provisioning information retrieval request failure.

8.17.3.19 Service provisioning information subscription request

Table 8.17.3.19-1 describes the information elements for Service provisioning information subscription request from the ECS to a partner ECS.

Table 8.17.3.19-1: Service provisioning information subscription request

Information element	Status	Description
ECS address	M	Endpoint information of ECS (e.g. URI, FQDN, IP address)
Security credentials	M	Security credentials of the ECS.
Notification Target Address	O	The Notification Target Address (e.g. URL) where the notifications destined for the ECS should be sent to.
Federation information	O	List of information for different federation agreements related to the ECS
> Federation identifier	O	Identifier of the federation
> ECSP identifiers	O	The list of ECSPs preferred by the ECS. This information is used by the ECS-ER to filter the discovered partner ECS information.
AC Profile(s)	O	Filter information about required services as described in Table 8.2.2-1.
Connectivity information	O	Connectivity information such as serving PLMN information where the services are required.
UE location	O	Location of the UE for which the services are required.
Proposed expiration time	O	Proposed expiration time for the subscription

8.17.3.20 Service provisioning information subscription response

Table 8.17.3.20-1 describes the information elements for Service provisioning information subscription response from the partner ECS to the ECS.

Table 8.17.3.20-1: Service provisioning information subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.17.3.21 Service provisioning information notification

Table 8.17.3.21-1 describes the information elements for Service provisioning information notification from the partner ECS to the ECS.

Table 8.17.3.21-1: Service provisioning information notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the ECS-ER
List of EDN configuration information	M	List of EDN configuration information as defined in Table 8.3.3.3.3-2.
Lifetime	O	Time duration for which the EDN configuration is valid and supposed to be cached by the ECS.

8.17.3.22 Service provisioning information subscription update request

Table 8.17.3.22-1 describes the information elements for Service provisioning information subscription update request from the ECS to a partner ECS.

Table 8.17.3.22-1: Service provisioning information subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials of the ECS.
Notification Target Address	O	The Notification Target Address (e.g. URL) where the notifications destined for the ECS should be sent to.
Federation information	O	List of information for different federation agreements related to the ECS
> Federation identifier	O	Identifier of the federation
> ECSP identifiers	O	The list of ECSPs preferred by the ECS. This information is used by the ECS-ER to filter the discovered partner ECS information.
AC Profile(s)	O	Filter information about required services as described in Table 8.2.2-1.
Connectivity information	O	Connectivity information such as serving PLMN information where the services are required.
UE location	O	Location of the UE for which the services are required.
Proposed expiration time	O	Proposed expiration time for the subscription

8.17.3.23 Service provisioning information subscription update response

Table 8.17.3.23-1 describes the information elements for Service provisioning information subscription update response from the partner ECS to the ECS.

Table 8.17.3.23-1: Service provisioning information subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.17.3.24 Service provisioning information unsubscribe request

Table 8.17.3.24-1 describes the information elements for Service provisioning information unsubscribe request from the ECS to a partner ECS.

Table 8.17.3.24-1: Service provisioning information unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be unsubscribed
Security credentials	M	Security credentials of the ECS.

8.17.3.25 Service provisioning information unsubscribe response

Table 8.17.3.25-1 describes the information elements for Service provisioning information unsubscribe response from the partner ECS to the ECS

Table 8.17.3.25-1: Service provisioning information unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.17.4 APIs

8.17.4.1 General

Table 8.17.4.1-1 illustrates the APIs for roaming and federation.

Table 8.17.4.1-1: Roaming and federation APIs

API Name	API Operations	Operation Semantics	Consumer(s)
Eecs_ECSRegistration	Request	Request/Response	ECS
	Update		
	Deregister		
Eecs_ECSDiscovery	Request	Request/Response	ECS
	Subscribe	Subscribe/Notify	ECS
	Notify		
	UpdateSubscription		
	Unsubscribe		
Eecs_ECSServiceProvisioning	Request	Request/Response	ECS
	Subscribe	Subscribe/Notify	ECS
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.17.4.2 Eecs_ECSRegistration API

8.17.4.2.1 General

This clause describes the Eecs_ECSRegistration API and its operations.

8.17.4.2.2 Eecs_ECSRegistration_Request operation

API operation name: Eecs_ECSRegistration_Request

Description: The consumer requests to register the ECS on the ECS-ER.

Inputs: See clause 8.17.3.2.

Outputs: See clause 8.17.3.3.

See clause 8.17.2.2.2 for details of usage of this operation.

8.17.4.2.3 Eecs_ECSRegistration_Update operation

API operation name: Eecs_ECSRegistration_Update

Description: The consumer requests to update the registered information of the ECS on the ECS-ER.

Inputs: See clause 8.17.3.4.

Outputs: See clause 8.17.3.5.

See clause 8.17.2.2.3 for details of usage of this operation.

8.17.4.2.4 Eecs_ECSRegistration_Deregister operation

API operation name: Eecs_ECSRegistration_Deregister

Description: The consumer requests to deregister the ECS from the ECS-ER.

Inputs: See clause 8.17.3.6.

Outputs: See clause 8.17.3.7.

See clause 8.17.2.2.4 for details of usage of this operation.

8.17.4.3 Eecs_ECSDiscovery API

8.17.4.3.1 General

This clause describes the Eecs_ECSDiscovery API and its operations.

8.17.4.3.2 Eecs_ECSDiscovery_Request operation

API operation name: Eecs_ECSDiscovery_Request

Description: The consumer requests for one time ECS discovery information.

Inputs: See clause 8.17.3.8.

Outputs: See clause 8.17.3.9.

See clause 8.17.2.3.2 for details of usage of this operation.

8.17.4.3.3 Eecs_ECSDiscovery_Subscribe operation

API operation name: Eecs_ECSDiscovery_Subscribe

Description: The consumer subscribes for ECS discovery information.

Inputs: See clause 8.17.3.10.

Outputs: See clause 8.17.3.11.

See clause 8.17.2.3.3.2 for details of usage of this operation.

8.17.4.3.4 Eecs_ECSDiscovery_Notify operation

API operation name: Eecs_ECSDiscovery_Notify

Description: The consumer is notified with ECS discovery information.

Inputs: See clause 8.17.3.12.

Outputs: None.

See clause 8.17.2.3.3.3 for details of usage of this operation.

8.17.4.3.5 Eecs_ECSDiscovery_UpdateSubscription operation

API operation name: Eecs_ECSDiscovery_UpdateSubscription

Description: The consumer updates an existing subscription for ECS discovery information.

Inputs: See clause 8.17.3.13.

Outputs: See clause 8.17.3.14.

See clause 8.17.2.3.3.4 for details of usage of this operation.

8.17.4.3.6 Eecs_ECSDiscovery_Unsubscribe operation

API operation name: Eecs_ECSDiscovery_Unsubscribe

Description: The consumer cancels an existing subscription for ECS discovery information.

Inputs: See clause 8.17.3.15.

Outputs: See clause 8.17.3.16.

See clause 8.17.2.3.3.5 for details of usage of this operation.

8.17.4.4 Eecs_ECSServiceProvisioning API

8.17.4.4.1 General

This clause describes the Eecs_ECSServiceProvisioning API and its operations.

8.17.4.4.2 Eecs_ECSServiceProvisioning_Request operation

API operation name: Eecs_ECSServiceProvisioning_Request

Description: The consumer requests for one time ECS service provisioning information.

Inputs: See clause 8.17.3.17.

Outputs: See clause 8.17.3.18.

See clause 8.17.2.4.2.2 for details of usage of this operation.

8.17.4.4.3 Eecs_ECSServiceProvisioning_Subscribe operation

API operation name: Eecs_ECSServiceProvisioning_Subscribe

Description: The consumer subscribes for ECS service provisioning information.

Inputs: See clause 8.17.3.19.

Outputs: See clause 8.17.3.20.

See clause 8.17.2.4.2.3.2 for details of usage of this operation.

8.17.4.4.4 Eecs_ECSServiceProvisioning_Notify operation

API operation name: Eecs_ECSServiceProvisioning_Notify

Description: The consumer is notified with ECS service provisioning information.

Inputs: See clause 8.17.3.21.

Outputs: None.

See clause 8.17.2.4.2.3.3 for details of usage of this operation.

8.17.4.4.5 Eecs_ECSServiceProvisioning_UpdateSubscription operation

API operation name: Eecs_ECSServiceProvisioning_UpdateSubscription

Description: The consumer updates an existing subscription for ECS service provisioning information.

Inputs: See clause 8.17.3.22.

Outputs: See clause 8.17.3.23.

See clause 8.17.2.4.2.3.4 for details of usage of this operation.

8.17.4.4.6 Eecs_ECSServiceProvisioning_Unsubscribe operation

API operation name: Eecs_ECSServiceProvisioning_Unsubscribe

Description: The consumer cancels an existing subscription for ECS service provisioning information.

Inputs: See clause 8.17.3.24.

Outputs: See clause 8.17.3.25.

See clause 8.17.2.4.2.3.5 for details of usage of this operation.

8.18 Edge Node Sharing

8.18.1 General

In the following clauses, ECSP-A is an ECSP partner of ECSP-B and ECSP-B is the leading ECSP which is serving the UE.

NOTE: An operator platform (OP) as described in GSMA PRD OPG.02 [19] is provided by an ECSP.

8.18.2 Procedures

8.18.2.1 General

Following procedures are defined to support ENS:

- Application information sharing between ECSPs; and
- EAS discovery for ENS.

NOTE: Service continuity in the current release is restricted to be provided via the Partner ECSP.

8.18.2.2 Application information sharing between ECSPs

NOTE: The security aspect of application information sharing between ECS-ER (ECSP-B) and ECS-ER (ECSP-A) is outside the scope of this release of this specification.

8.18.2.2.1 General

To exchange EES and application information between ECSPs, allowed by the federation agreement for the purpose of ENS, the procedures defined in clause 8.17 are used.

When the ECS determines to query a partner ECSP for the purpose of ENS, e.g., upon receiving a service provisioning request from the EEC as specified in clause 8.3 or periodically, the ECS uses -

- the procedures defined in clause 8.17.2.3, if it needs to obtain or subscribe for ECS information of partner ECSP; and
- the procedures defined in clause 8.17.2.4, to obtain or subscribe for the EES information from the partner ECS.

To obtain EES and application information using

- a request-response model the procedures defined in clause 8.17.2.4.2.2.
- a subscribe-notify model the procedures defined in clause 8.17.2.4.2.3.

If the query was initiated as a result of a service provisioning request from the EEC as specified in clause 8.3.3.2.2, the service provisioning response to the EEC includes EES information of the partner ECSP along with the EES information of the ECSP serving the UE. The EES of the ECSP serving the UE is determined based on SLA(s) between the ECSPs such that it can be authorized by the EES of the partner ECSP. The endpoint of EES of partner ECSP is provided by the ECS in a way that is transparent to EEC.

8.18.2.3 EAS discovery for ENS

8.18.2.3.1 General

Following procedures are defined for EAS discovery with respect to ENS:

- EAS discovery via leading ECSP;
- EEC triggered EAS discovery via partner ECSP; and
- EES triggered EAS discovery via partner ECSP.

8.18.2.3.2 EAS discovery via leading ECSP

Pre-conditions:

1. ECSP-1 and ECSP-2 have a service level agreement to share edge services.

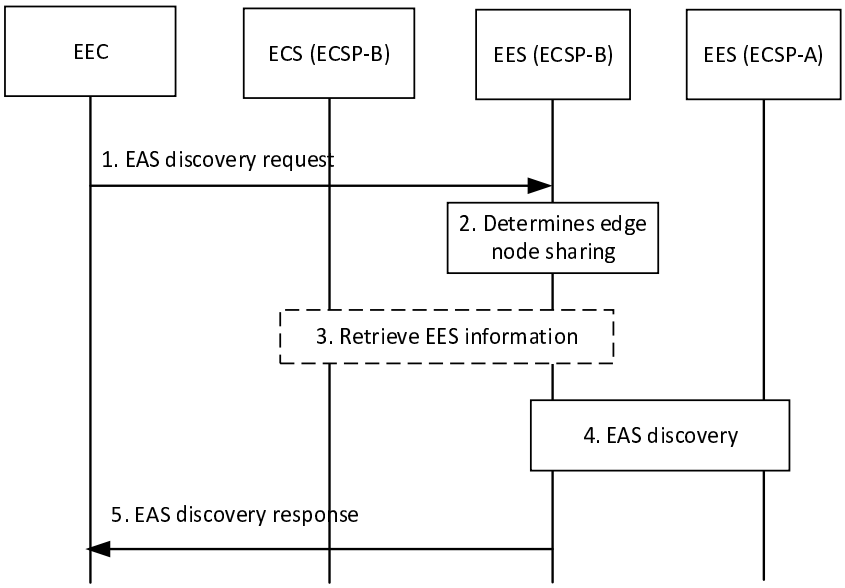

Figure 8.18.2.3.2-1: EAS discovery for ENS

1. The EEC sends EAS discovery request to EES (ECSP-B) as specified in clause 8.5 and may include the endpoint of EES (ECSP-A) in the request, if provided by the ECS as specified in clause 8.18.2.2.1.
2. If the EAS discovery request contains EES information of a partner ECSP (ECSP-A) or the required EAS is not available with the EES the EES may determine to use ENS. If the EAS discovery request contains EES information of a partner ECSP, the EES can use it after validating the information.

NOTE 1: To validate the information of partner ECSPs, EES (ECSP-B) can use the federation agreement between ECSPs.

3. If the EAS discovery request does not contain EES information of a partner ECSP, the EES may use the EES retrieval procedures as specified in clause 8.8.3.3 to obtain EES information of a partner ECSP. The Retrieve EES request may include an ENS indication so that the ECS (ECSP-B) can skip checking T-EES(s) locally registered in the ECS (ECSP-B).
4. Once EES information of the partner ECSP is available, the EES (ECSP-B) sends the EAS discovery request to the EES (ECSP-A) as described in step 3 of clause 8.8.3.2. The EAS discovery request includes the information of the MNO serving the UE (e.g. MNO name, PLMN ID).

The EES (ECSP-A) validates the request and returns EAS discovery response including the discovered candidate EAS(s) to the EES (ECSP-B). In addition to step 4 of clause 8.8.3.2, the candidate EAS(s) are discovered based on the serving MNO information received from the EES (ECSP-B) and allowed MNO information registered by the EAS.

NOTE 2: To validate the EAS discovery request, EES (ECSP-A) can use the federation agreement between ECSPs.

5. EES (ECSP-B) provides the discovered information to the EEC as part of the EAS discovery response as specified in clause 8.5.

8.18.2.3.3 EAS discovery via Partner ECSP, EEC triggered

If the EEC has the EES information of the partner ECSP and the required security credentials to communicate with the partner ECSP, the EEC can use the EAS discovery procedures specified in clause 8.5 to directly obtain the EAS information from the EES of the partner ECSP. Upon receiving the request from the EEC, the EES of the partner ECSP identifies the EAS(s) considering the allowed MNO information of the registered EASs and UE's serving MNO information.

8.18.2.3.4 EAS discovery via Partner ECSP, EES triggered

When service continuity is required, the EES can trigger the T-EAS discovery procedures as defined in clause 8.8.3.2 with the EES of the partner ECSP to find an EAS with respect to ENS. The EAS discovery request includes UE''s serving MNO information (e.g. MNO name, PLMN ID). Upon receiving the request from the S-EES, the T-EES of the partner ECSP identifies the EAS(s) considering the allowed MNO information of the registered EASs and UE's serving MNO information.

8.18.3 APIs

8.18.3.1 General

The APIs as defined in clause 8.5.4 are used to perform EAS discovery in partner ECSP.

See clause 8.18.2.3.2, clause 8.18.2.3.3 and clause 8.18.2.3.4 for details of usage of this operation.

8.19 Common EAS announcement

8.19.1 General

Common EAS announcement procedure enables an EES to exchange selected common EAS information with other EES(s).

8.19.2 Procedure

Pre-conditions:

1. The announcing EES may be pre-configured with the EES information of other receiving EES(s), which belongs to the same EDN; or

2. The announcing EES may receive the list of receiving EES(s) information (e.g. address information) from the EEC during the EAS information provisioning procedure.

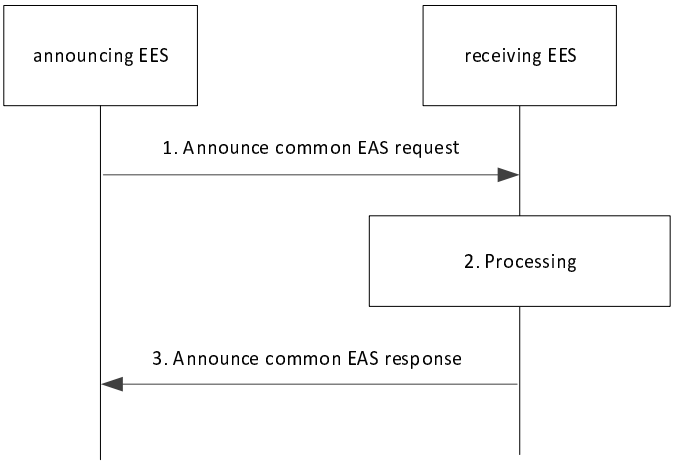

Figure 8.19.2-1: Announce common EAS procedure

1. The announcing EES sends Announce common EAS request message to the receiving EES. The request message includes the requestor identifier [EESID], the security credentials, the selected common EAS information, the announcing EES endpoint, and the Application group ID.

2. Upon receiving the request from the announcing EES, the receiving EES checks if the announcing EES is authorized to provide the selected common EAS. The receiving EES stores the received selected EAS information and announcing EES endpoint along with the Application group ID.

3. If the processing of the request was successful, the receiving EES sends Announce common EAS response to the announcing EES indicating a successful status; otherwise, the receiving EES shall indicate a failure status and include appropriate reasons.

8.19.3 Information flows

8.19.3.1 General

The information flows are specified for Announce common EAS request and response.

8.19.3.2 Announce common EAS request

Table 8.19.3.2-1 describes the information elements for Announce common EAS request from the announcing EES to the receiving EES.

Table 8.19.3.2-1: Announce common EAS request

Information element	Status	Description
Requestor identifier	M	The identifier of the announcing EES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Selected common EAS ID	M	The identifier of the Selected Common EAS
Selected common EAS endpoint	M	The endpoint of the Selected Common EAS
EES endpoint	O	The endpoint address (e.g., URI, IP address) of the announcing EES.
Application Group ID	M	Application group identifier as defined in 7.2.11.

8.19.3.3 Announce common EAS response

Table 8.19.3.2-1 describes the information elements for Announce common EAS response from the receiving EES to the announcing EES.

Table 8.19.3.2-1: Announce common EAS response

Information element	Status	Description
Successful response	O	Indicates that the request was successful.
Failure response	O	Indicates that the request has failed.
Cause	O	Indicates the failure cause. Only included when Failure Response is included.

8.19.4 APIs

8.19.4.1 General

Table 8.19.4.1-1 illustrates the API for common EAS announcement.

Table 8.19.4.1-1: Eees_CommonEASAnnouncement API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_CommonEasAnnouncement	Declare	Request/Response	EES

8.19.4.2 Eees_CommonEasAnnouncement_Declare operation

API operation name: Eees_CommonEasAnnouncement_Declare

Description: The consumer declares common EAS information to the EES.

Inputs: See clause 8.19.3.2.

Outputs: See clause 8.19.3.3.

See clause 8.19.2 for details of usage of this operation.

8.20 Interaction with ECS with Repository function

8.20.1 General

This clause describes procedures and services provided by the ECS with Repository function (ECS-ER) for obtaining and storing common EAS information, which is applicable when the ECS-ER is available. Removal of common EAS information stored at the ECS-ER is not specified in this release.

NOTE: ECS can support repository function as ECS-ER.

8.20.2 Procedure

8.20.2.1 General

Clause 8.20.2.2, clause 8.20.2.3 and clause 8.20.2.4 illustrate the application group specific EAS information retrieval procedures.

8.20.2.2 Obtain EAS information

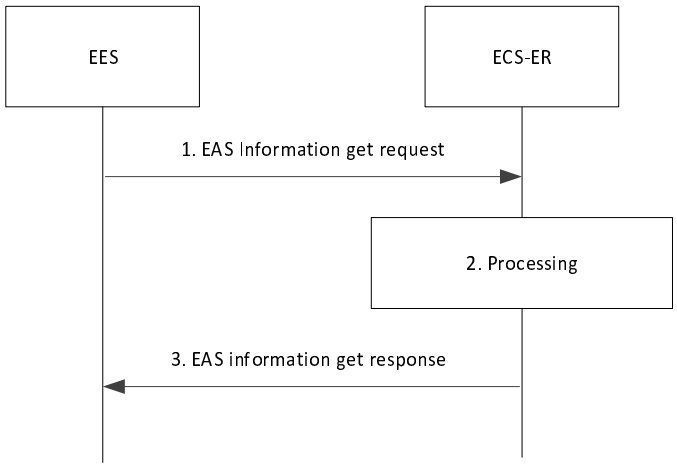

Figure 8.20.2.2-1: Obtain EAS information

1. The EES sends EAS information get request message to the ECS-ER. The request message includes EAS ID and Application Group ID.
2. Upon receiving the request, the ECS-ER checks if there are any stored EAS(s) serving the application group for the EAS ID.
3. If the processing of the request was successful, the ECS-ER responds the EES with EAS information identified in step 2.

8.20.2.3 Common EAS information storage

Pre-condition:

1. The EES is registered in the ECS supporting repository function.

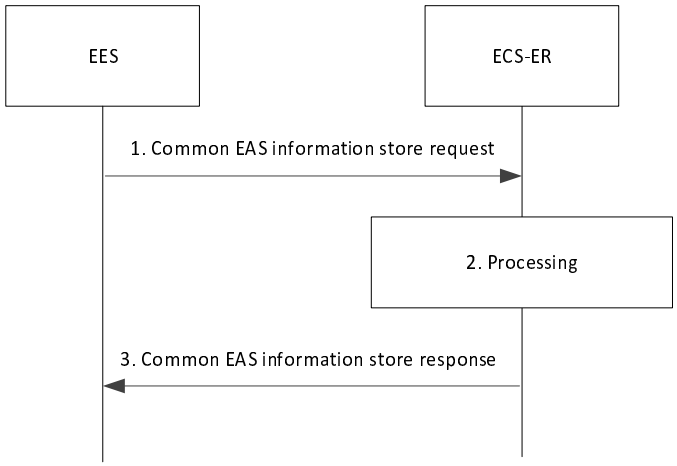

Figure 8.20.2.3-1: Common EAS information storage

1. The EES sends Common EAS information store request message to the ECS-ER. The request message includes EDN information, EES ID, EAS ID, EAS endpoint and Application Group ID.

2. Upon receiving the request, the ECS-ER checks if there is any stored EAS serving the application group for the EAS ID within the same EDN. If no common EAS is identified, the ECS-ER stores the received information for subsequent binding requests.

3. The ECS-ER responds the EES with Common EAS information store response message. The ECS-ER may reject the request with common EAS information identified in step 2 or accept the request. For enabling the EEC to further communicate with common EES, the common EES endpoint is also provided with common EAS information.

8.20.3 Information flows

8.20.3.1 General

The information flows are specified for EAS information service.

8.20.3.2 EAS information get request

Table 8.20.3.2-1 describes the information elements for EAS information get request from the EES to the ECS-ER.

Table 8.20.3.2-1: EAS information get request

Information element	Status	Description
Requestor identifier	M	The identifier of the EES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EAS ID	M	The identifier of the EAS.
Application Group ID	M	Application group identifier as defined in 7.2.11.

8.20.3.3 EAS information get response

Table 8.20.3.3-1 describes the information elements for EAS information get response from the ECS-ER to the EES.

Table 8.20.3.3-1: EAS information get response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the request was successful.
> EAS information	M	This IE includes a list of EAS endpoints.
Failure response (NOTE)	O	Indicates that the request has failed.
> Cause	O	Indicates the failure cause. Only included when Failure response is included.
NOTE: One of these IEs shall be present in the message.		

8.20.3.4 Common EAS information store request

Table 8.20.3.4-1 describes the information elements for common EAS information store request from the EES to the ECS-ER.

Table 8.20.3.4-1: Common EAS information store request

Information element	Status	Description
Requestor identifier	M	The identifier of the EES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EAS ID	M	The identifier of the EAS.
EAS endpoint	M	Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EAS.
Application Group ID	M	Application group identifier as defined in 7.2.11.
EDN information	M	Information of EDN where the EAS resides.
> DNN	M	Data network name to identify the EDN.
> DNAI(s)	O	DNAI(s) associated with the EDN.

8.20.3.5 Common EAS information store response

Table 8.20.3.5-1 describes the information elements for common EAS information store response from the ECS-ER to the EES.

Table 8.20.3.5-1: Common EAS information store response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the request was successful.
Failure response (NOTE)	O	Indicates that the request has failed.
> Cause	O	Indicates the failure cause. Only included when Failure response is included.
> Common EAS information	O	This IE includes common EAS endpoint.
> Common EES endpoint	O	This IE includes common EES endpoint address. It shall be provided when common EAS information is provided.
NOTE: One of these IEs shall be present in the message.		

8.20.4 APIs

8.20.4.1 General

Table 8.20.4.1-1 illustrates the API for EAS information management.

Table 8.20.4.1-1: EAS information management APIs

API Name	API Operations	Operation Semantics	Consumer(s)
Eecs_EASInfoManagement	Store	Request/Response	EES
	Get	Request/Response	EES

8.20.4.2 Eecs_EASInfoManagement_Store operation

API operation name: Eecs_EASInfoManagement_Store

Description: The consumer requests EAS information storage service from the ECS.

Inputs: See clause 8.20.3.4.

Outputs: See clause 8.20.3.5.

See clause 8.20.2.3 for details of usage of this operation.

8.20.4.3 Eecs_EASInfoManagement_Get operation

API operation name: Eecs_EASInfoManagement_Get

Description: The consumer obtains EAS information from the ECS.

Inputs: See clause 8.20.3.2.

Outputs: See clause 8.20.3.3.

See clause 8.20.2.2 for details of usage of this operation.

9 Usage of SEAL services

9.1 Notification management service

9.1.1 General

The notification management is a SEAL service that offers the notification functionality. This service enables EEC to subscribe and receive notifications from the EES and ECS, and thereby offloading the complexity of delivery and reception of notifications to the edge enabler layer.

9.1.2 Information flows

The following information flows of notification management service of SEAL as specified in 3GPP TS 23.434 [13] are applicable for the EEL:

- Create notification channel request specified in clause 17.3.2.1;
- Create notification channel response specified in clause 17.3.2.2;
- Open notification channel specified in clause 17.3.2.3;
- Notification message specified in clause 17.3.2.4.

The usage of the above information flows are clarified as below:

- The Callback URL is the address (e.g. Notification Target Address) where the notifications destined for the EEC;
- VAL Application ID is EECID;
- VAL Service ID is ECS ID or EES ID;
- VAL client is the EEC;
- VAL server is the EES or ECS.

9.1.3 Procedures

The following procedures of notification management service of SEAL as specified in 3GPP TS 23.434 [13] are applicable for the edge enabler layer:

- Procedure for creating notification channel to receive notifications, specified in clause 17.3.3.

Annex A (Informative): Deployment models

A.1 General

The following clauses illustrate different aspects of some possible deployment options

- Clause A.2 describes some deployment models for different DN implementations;
- Clause A.3 describes some options for how ECS is deployed in relation to the UE;
- Clause A.4 describes deployment of EES in relation with SEAL services and Application Enabler Services; and
- Clause A.5 describes deployments in relation with CAPIF.

A.2 Deployment models for different DN implementations

A.2.1 General

This clause describes examples of deployment models with respect to different DN implementations as follows:

- option 1. use of non-dedicated DN;
- option 2. use of Edge-dedicated DN; and
- option 3. use of LADN.

The PLMN supporting edge computing services provides connection to one or multiple DNs.

The following clauses describes the detailed deployment models including relationships between EAS service areas, EES service areas, LADN service areas, and PLMN area.

A.2.2 Option 1. Use of non-dedicated DN

There is no Edge-dedicated DN for support of edge computing service. A DN common to other services (e.g. internet access) is used to connect to the EASs.

The PLMN supporting edge computing services provides connection to EASs located in EDNs that respectively corresponds to one or more DNAI(s), and each EDN is identified by DNN and one or more DNAI. UEs establishing PDU sessions for the EASs identify the DN using the same DNN and slice information as for PDU sessions for non-Edge services.

Each EAS and EES can have a topological service area or a geographical service area that the EAS and EES serves, respectively. Within this service area, UEs can access an EAS or an EES regardless of their location within the PLMN area via local breakout.

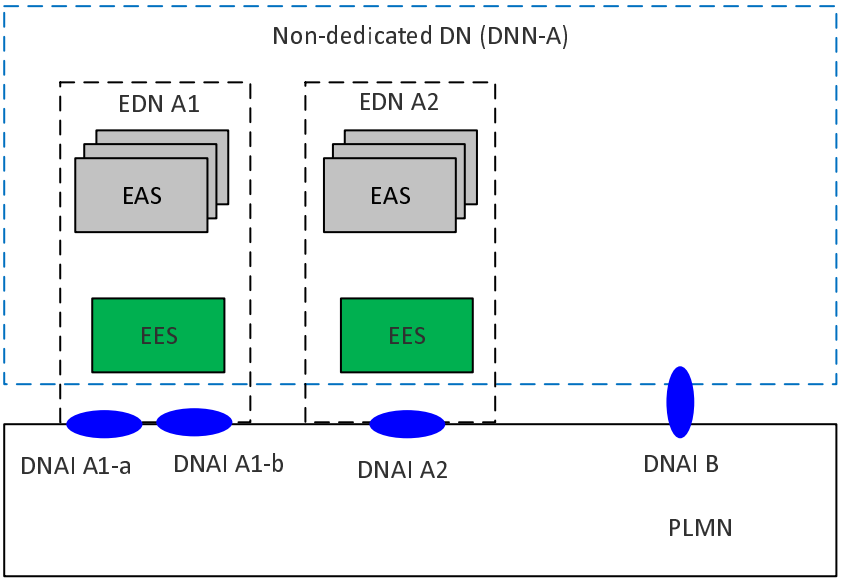

Figure A.2.2-1: Option 1: Use of non-dedicated DN

A.2.3 Option 2. Use of Edge-dedicated DN

The deployment uses Edge-dedicated DNs for support of edge computing service. Each Edge-dedicated DN is configured with unique DNNs.

The PLMN supporting edge computing services provides connection to several EDNs that correspond to one or more DNAI(s), and each EDN is identified by DNN of the Edge-dedicated DN and one or more DNAI.

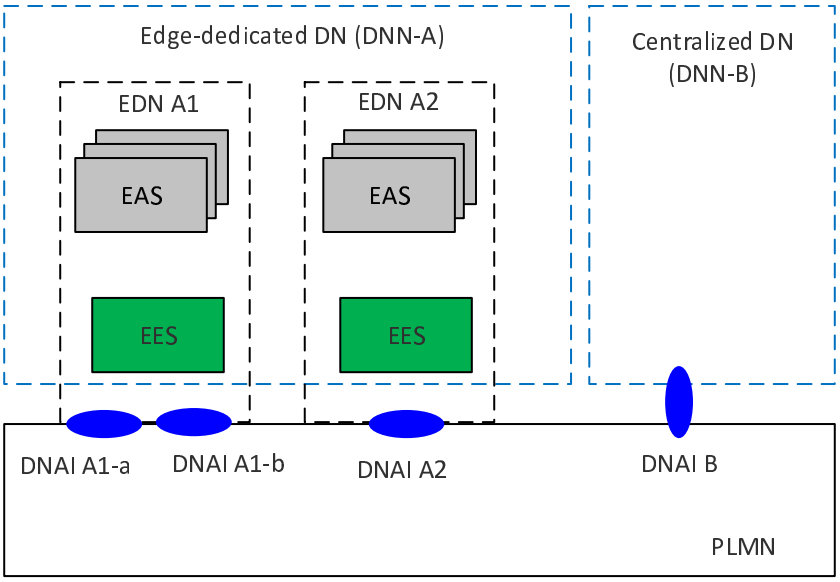

Figure A.2.3-1: Option 2: Use of Edge-dedicated DN

A.2.4 Option 3. Use of LADN

Edge computing services can be provided via Edge-dedicated Data Networks deployed as LADNs. With this option, the PLMN supports edge computing services in the EDN service areas which is equal to the LADN service area. The LADN service area is the service area that the Edge Computing is supported. Each individual EAS in the LADN can support the same or smaller service area than the LADN.

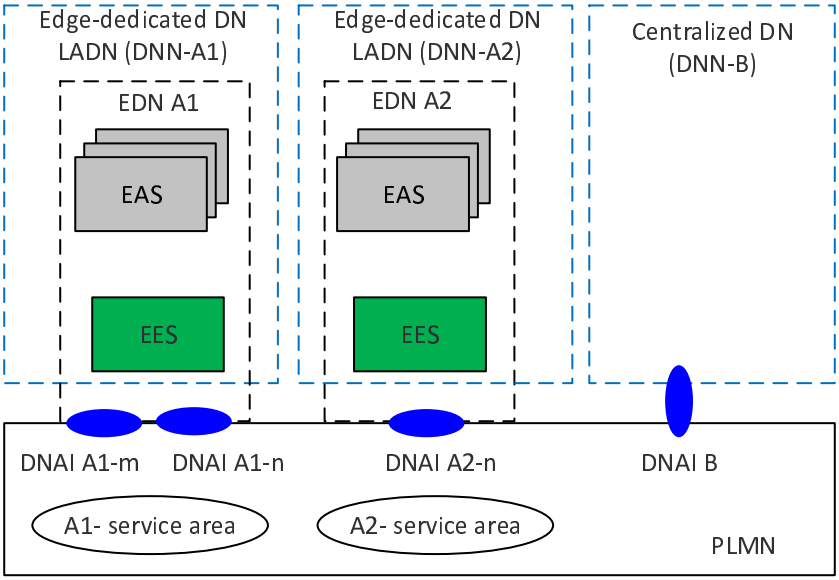

Figure A.2.4-1: Option 3: Use of LADN(s)

A.3 ECS deployments in relation to the UE

A.3.1 General

This clause shows some examples for how the ECS can be deployed in relation to the UE

A.3.2 UE (EEC) served by a single ECS

In this scenario the UE can contain a single AC or multiple ACs, however the UE contains a single EEC which is configured with the address of a single ECS. This could for example be an IoT device that only supports a single AC or a smartphone device which contains many ACs which are served by a single ECS.

A.3.3 UE (EECs) served by multiple ECSs

In this scenario the user is allowed to install multiple ACs in the UE where each AC can be served by an EAS which in turn served by a different ECSP's EES/ECS.

One example is that multiple ACs are installed on a smartphone and the associated EASs are on-boarded onto different ECSP's EESs which are registered with different ECSs.

Another example is a UE that supports Dual SIM. In this scenario the UE can support concurrent connection to two PLMNs.

A.4 Deployment of EES in relation with SEAL services and Application Enabler Services

A.4.1 General

The illustration of layered application architecture with the generic SEAL and Application Enabler server functions available in the cloud is shown in Figure A.4.1-1.

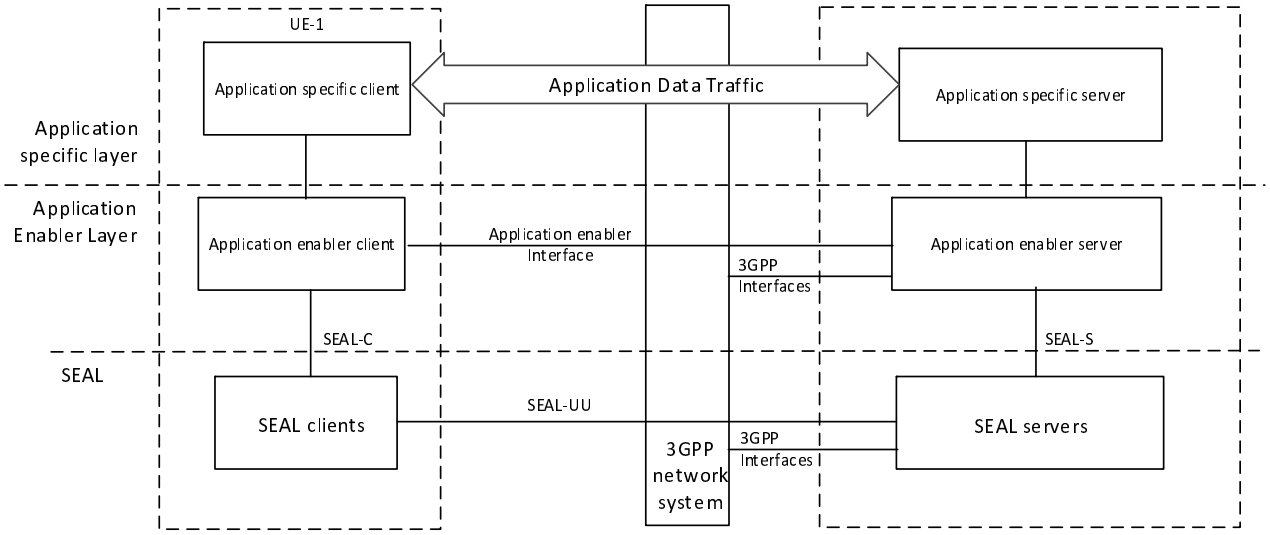

Figure A.4.1-1: Illustration of a layered application architecture with generic SEAL and Application Enabler server functions available in the cloud

The examples of application specific client are V2X application specific client, FF application specific client, UAS application specific client or other vertical application specific client residing on the UE. Similarly, the application specific server could be e.g. V2X application specific server, FF application specific server, UAS application specific server or other vertical application specific server.

The UE may consist of an application enabler client. The examples of application enabler client include V2X application enabler client, FF application enabler client, UAS application enabler client or other vertical application enabler client residing on the UE. Similarly, the application enabler server could be V2X application enabler server, FF application enabler Server, UAS application enabler server or other vertical application enabler server.

The illustration of layered application architecture with generic SEAL and Application Enabler server functions available in the edge is shown in Figure A.4.1-2.

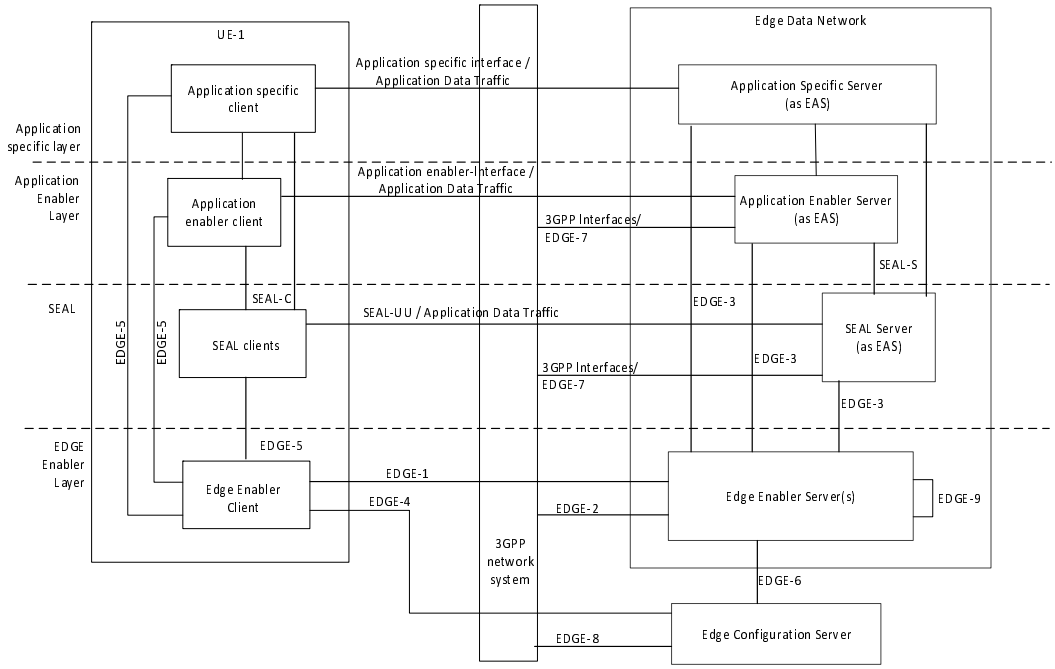

Figure A.4.1-2: Illustration of layered application architecture with generic SEAL and Application Enabler server functions available in the edge

While the server functions of an application specific server can be made available only as an EAS, it is also possible that certain application specific server functions are available both at the edge and in the cloud. Similarly, the server functions of an application enabler server can be made available only as an EAS, it is also possible that certain application enabler server functions are available both at the edge and in the cloud. When the server functions of an application are both available at the edge and the cloud, there may be a need for interaction between the two corresponding application servers, which is out of scope of this specification.

NOTE 1: The details of a specific vertical application architecture based on the generic layered application architecture with server functions of an application available in the edge and the cloud is out of scope of this specification.

NOTE 2: When UE is in the coverage of the EDN due to which certain server functions are available both at the edge and in the cloud, then whether UE connects to the server functions available at the edge or directly to the cloud is out of scope of the present document.

A.4.2 Deployment of SEAL services

There are several options to support SEAL service APIs to be exposed to the EAS.

The EES can act as the CAPIF core function, and the SEAL servers acting the AEF and publish the SEAL service API to the EES. Further, the SEAL service APIs is discovered by the EASs acting as the API invoker during the service API discover procedure as specified in 3GPP TS 23.222 [6].

The EES can act as the API topology hiding entry and re-expose SEAL service APIs as specified in 3GPP TS 23.434 [13] to EAS via EDGE-3 which utilizes the CAPIF-2/2e reference point as specified in 3GPP TS 23.222 [6].

A.4.3 Deployment of Application Enabler services

There are several options to support vertical application enabler server (e.g., V2X application enabler server) APIs to be exposed to the EAS.

The EES can act as the CAPIF core function, and the vertical application enabler server acting the AEF and publish the vertical application enabler server APIs to the EES. Further, the vertical application enabler server APIs is discovered by the EASs acting as the API invoker during the service API discover procedure as specified in 3GPP TS 23.222 [6].

The EES can act as the API topology hiding entry and re-exposes vertical application enabler server APIs, e.g., VAE server APIs as specified in 3GPP TS 23.286 [14] to EAS via EDGE-3 which utilizes the CAPIF-2/2e reference point as specified in 3GPP TS 23.222 [6].

A.5 Deployments in relation with CAPIF

A.5.1 General

A.5.2 Distributed CAPIF core functions

The EES can support EAS's access to northbound APIs exposed by SCEF/NEF by providing distributed CAPIF core functions as shown in Figure A.5.2-1.

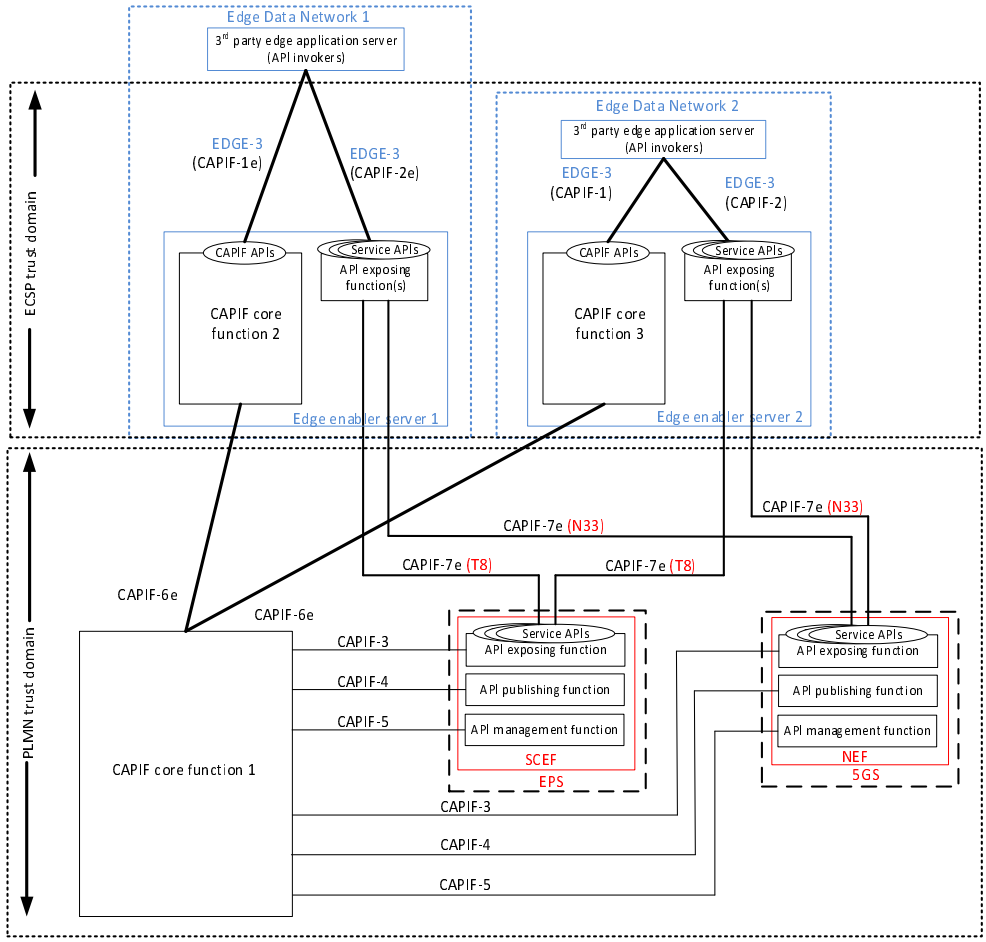

Figure A.5.2-1: EES supporting distributed CAPIF core functions

The EDNs reside outside the PLMN trust domain as shown in Figure A.5.2-1. In EDN 2, the EAS and EES are within the same ECSP trust domain. While in EDN 1, the EES and the EAS are in the different ECSP trust domain.

The EES of an EDN provides the following functions for network capability exposure:

- the CAPIF core function as specified in 3GPP TS 23.222 [6] to support onboarding of EASs (API invokers), publish of service APIs, discovery of service APIs and charging of service APIs invocations; and
- the API exposing function as specified in 3GPP TS 23.222 [6] to expose the service APIs from SCEF/NEF to the EASs via proxy or gateway function.

The following procedures are performed as specified in 3GPP TS 23.222 [6]:

- The SCEF and NEF act as API exposing function and the service APIs from SCEF (T8) and NEF (Nnef) are published to the CAPIF core function 1. The service APIs are published to the EESs (CAPIF core function 2 and CAPIF core function 3) from the CAPIF core function 1.
- The EAS acts as an API invoker and is onboarded to the EES (CAPIF core function 2 or CAPIF core function 3) within the EDN.
- The EASs (API invokers) are authenticated with EES (CAPIF core function 2 or CAPIF core function 3).

NOTE: The trusted EASs can utilize the services of a centralized CAPIF core function deployed by the PLMN operator instead of the CAPIF core function of EES deployed within the EDN.

- The EAS discovers the service APIs published by the SCEF and NEF via the EES (CAPIF core function 2 or CAPIF core function 3) within the EDN including the end point address of the API exposing function where the service API invocation is to be performed.

- The EAS obtains authorization to invoke the service APIs of the SCEF and NEF from the EES (CAPIF core function 2 or CAPIF core function 3).

- The EAS invokes the service APIs of the SCEF and NEF after authorization by the EES (API exposing function) and obtaining the UE identifier as specified in clause 8.6.5. The EES (API exposing function) further invokes the service APIs of the SCEF or NEF in the 3GPP core network. EDGE-2 supports CAPIF-7e interactions corresponding to T8 (for SCEF) and N33 (for NEF).

A.5.3 Centralized CAPIF core function

The EES can support EAS (owned by 3rd party or by PLMN operator) access to northbound APIs exposed by SCEF/NEF by using centralized CAPIF core functions as shown in Figure A.5.3-1.

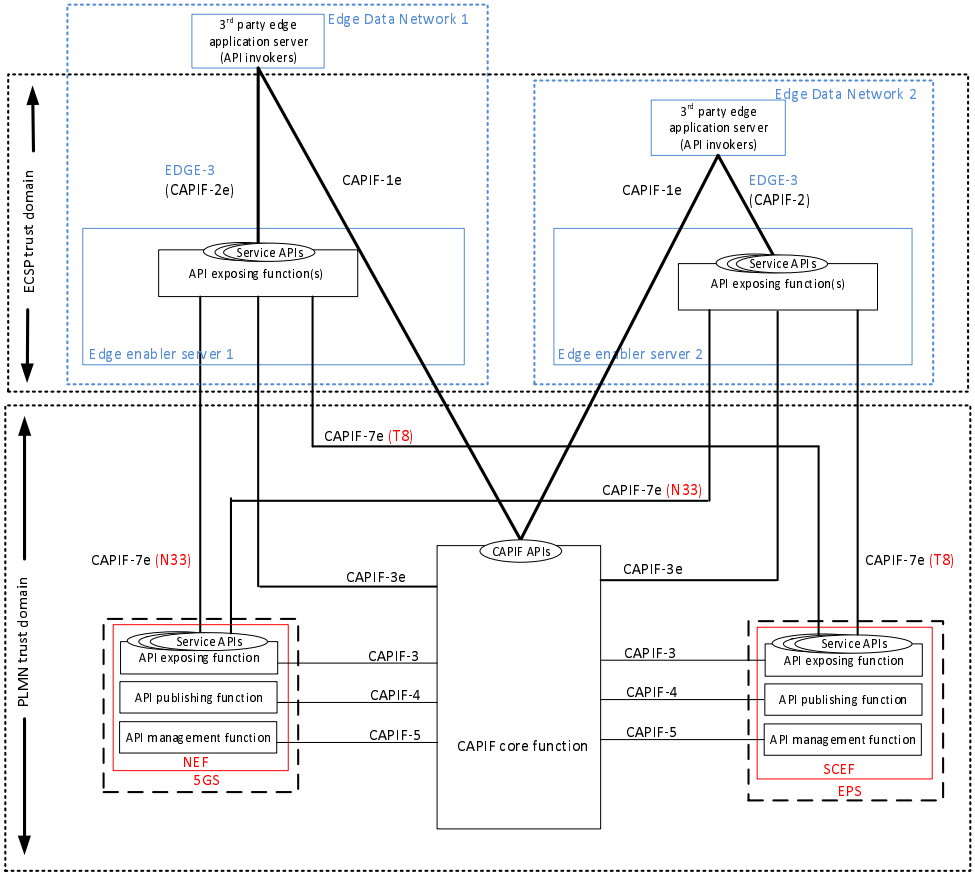

Figure A.5.3-1: EES supporting centralized CAPIF core functions

The EDNs reside outside the PLMN trust domain as shown in Figure A.5.3-1. In EDN 2, the EAS and EES are within the same ECSP trust domain. While in EDN 1, the EES and the EAS are in the different ECSP trust domain.

The EES of an EDN provides the following functions for network capability exposure:

- the API exposing function as specified in 3GPP TS 23.222 [6] to expose the service APIs from SCEF/NEF to the EASs via proxy or gateway function.

The following procedures are performed as specified in 3GPP TS 23.222 [6]:

- The SCEF and NEF act as API exposing function and the service APIs from SCEF (T8) and NEF (Nnef) are published to the centralized CAPIF core function. The service APIs exposed by the EESs are published to the centralized CAPIF core function.

- The EAS acts as an API invoker and is onboarded to the centralized CAPIF core function residing outside of the EDN.

- The EASs (API invokers) are authenticated with the centralized CAPIF core function.
- The EAS discovers the service APIs published by the SCEF and NEF via the centralized CAPIF core function including the end point address of the API exposing function where the service API invocation is to be performed.
- The EAS obtains authorization to invoke the service APIs of the SCEF and NEF from the centralized CAPIF core function.
- The EAS invokes the service APIs of the SCEF and NEF after authorization by the EES (API exposing function) and obtaining the UE identifier as specified in clause 8.6.5. The EES (API exposing function) further invokes the service APIs of the SCEF or NEF in the 3GPP core network. EDGE-2 supports CAPIF-7e interactions corresponding to T8 (for SCEF) and N33 (for NEF).

A.5.4 Supporting Exposure of EAS Service APIs using CAPIF

The EES provides support for an EAS to expose its Service APIs (i.e., EAS Service APIs) for consumption by the other EASs by providing CAPIF functions as shown in Figure A.5.4-1.

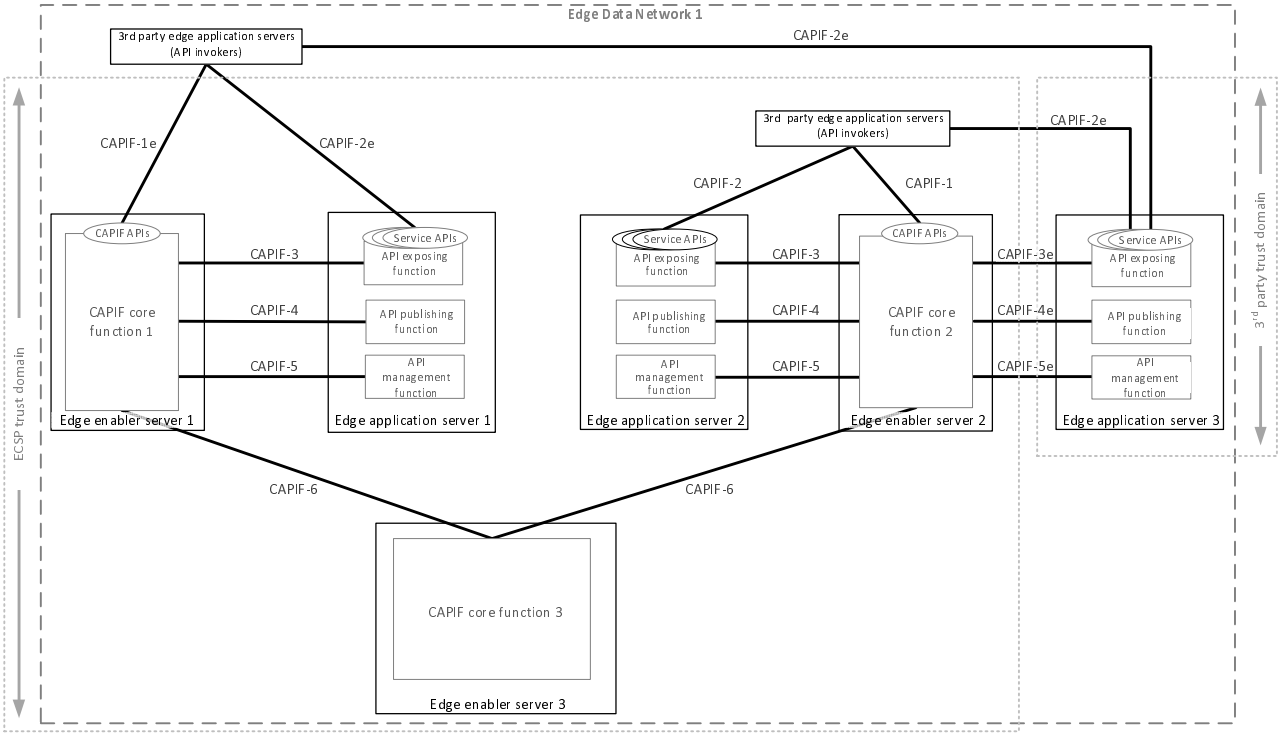

Figure A.5.4-1: EES supporting CAPIF functions for exposure of EAS Service APIs

In EDN 1, all the EESs are within the same ECSP trust domain. The EASs (EAS 1 and EAS 2 as API providers) are within the same ECSP trust domain and EAS 3 (API provider) is within the 3rd-party trust domain. The 3rd party EASs (API invoker) connected to EES 2 (CCF 2) are within the same ECSP trust domain, whereas the 3rd party EASs (API invoker) connected to EES 1 (CCF 1) are outside the ECSP trust domain.

The EES of an EDN provides the following functions for exposure of EAS Service APIs:

- The CAPIF core function as specified in 3GPP TS 23.222 [6] to support onboarding of EASs (API invokers), publish of EAS Service APIs, discovery of EAS Service APIs, and charging of EAS Service APIs invocations.

The following procedures are performed as specified in 3GPP TS 23.222 [6]:

- The EAS (API provider) acts as an API provider by supporting API provider domain functions (i.e., API exposing function, API publishing function, and API management function), and its Service APIs are published to the EES (CAPIF core function 1 or CAPIF core function 2).

- The EESs (CAPIF core function 1 or CAPIF core function 2) further publishes the EAS Service APIs to CAPIF core function 3 which assumes the role of a centralized repository of EAS service APIs in the EDN 1 to support discovery of the EAS Service APIs across different EESs (EES 1 and EES 2) using CAPIF-6 for interconnection operations as shown in Figure A.5.4-1.

- The EAS (API invokers) discovers the EAS Service API(s) via CAPIF core function 1 or CAPIF core function 2 (deployed with the EESs) including the end point address of the API exposing function where the service API invocation is to be performed.

NOTE 1: EES supporting CAPIF core function may also provide the support for logging, audit, and access control of EAS Service API(s) as specified in 3GPP TS 23.222 [6].

NOTE 2: The other CAPIF operations (e.g., onboarding, authentication, authorization) are the same as specified in the Annex A.5.2.

Annex B (Informative): Involved entities and relationships

B.1 General

This clause describes the relationship of edge computing service providers, PLMN operators, application service providers and users.

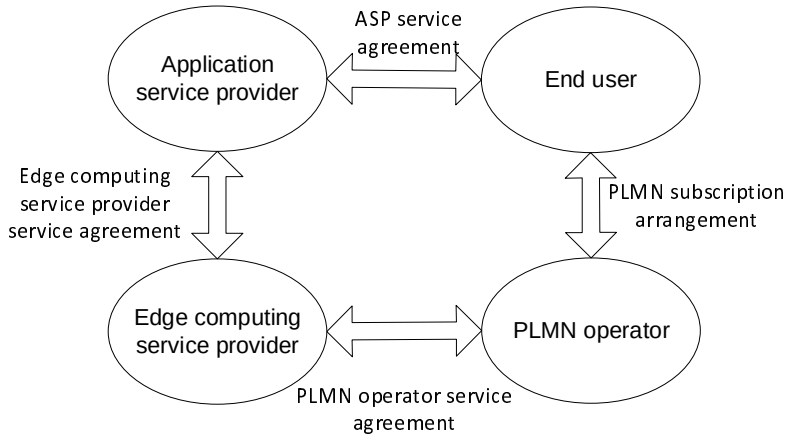

Figure B-1: Relationships involved in edge computing service

The end user is the consumer of the applications provided by the application service provider (ASP) and can have ASP service agreement with a single or multiple application service providers. The end user has a PLMN subscription arrangement with the PLMN operator. The UE used by the end user is allowed to be registered on the PLMN operator network.

The application service provider consumes the edge services (e.g. infrastructure, platform) provided by the edge computing service provider (ECSP) and can have edge computing service provider service agreement with a single or multiple edge computing service providers.

A single PLMN operator can have the PLMN operator service agreement with a single or multiple edge computing service providers.

A single ECSP can have PLMN operator service agreement with a single or multiple PLMN operators which provide edge computing support.

The edge computing service provider and the PLMN operator can be part of the same organization.

B.2 Federation and Roaming

This clause describes the relationship of edge computing service providers, PLMN operators, application service providers and end users, taking federation and roaming into account.

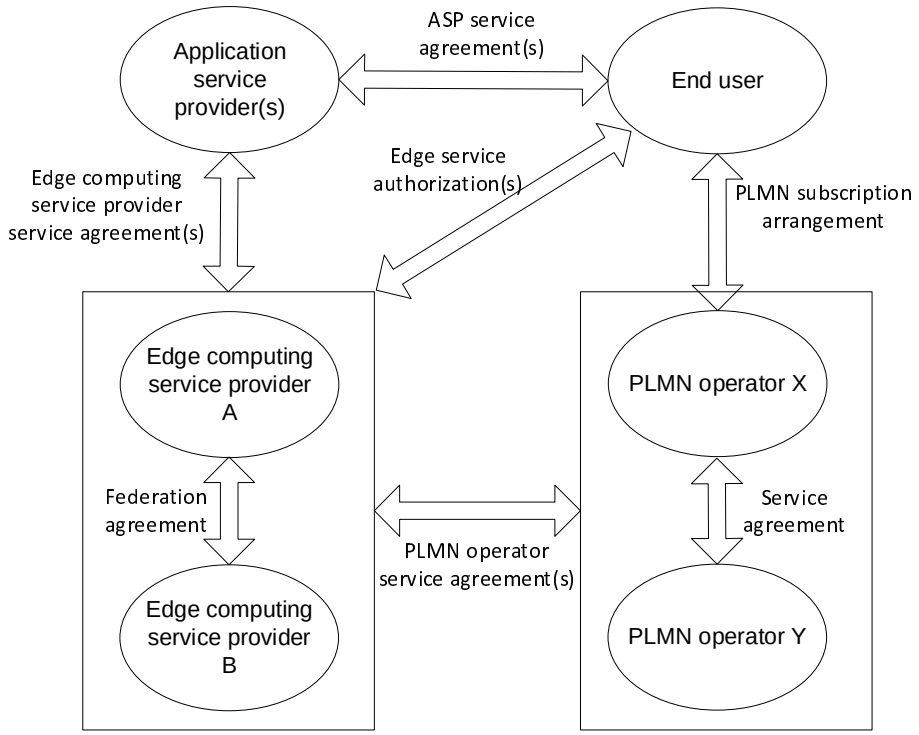

Figure B.2-1: Relationships involved in edge computing service – federation and roaming

The end user is the consumer of the applications provided by the application service provider (ASP). The End user:

- can have ASP service agreement with a single or multiple application service providers.
- has a PLMN subscription arrangement with a PLMN operator (HPLMN), and the UE used by the end user can register on the HPLMN network and network of its roaming partners; or has a SNPN subscription arrangement with a SNPN operator (subscribed SNPN), and the UE used by the end user can register on the subscribed SNPN and a serving SNPN.
- can have authorization to access edge services of a single or multiple ECSPs.

The ASP consumes the edge services (e.g. infrastructure, platform) provided by the ECSP. The ASP:

- can have edge computing service provider service agreement with a single or multiple ECSPs.

The PLMN operator provides connectivity between the end user and the edge services provided by the ECSP. The PLMN operator:

- can have the PLMN operator service agreement with a single or multiple ECSPs.
- can have service agreement for roaming including agreements for Edge Computing services, and/or federation with a single or multiple PLMN operators.

The ECSP provides the edge services. The ECSP:

- can have PLMN operator service agreement with a single or multiple PLMN operators which provide edge computing support.
- can have federation partnership to share edge services with a single or multiple ECSPs.

The ECSP and the PLMN operator can be part of the same organization.

B.3 Application Groups

This clause describes the relationship of edge computing service providers, PLMN operators, application service providers, application client instances, application server instances, and UEs for a group of application clients being served by a common application server. Figure B.3-1 shows these relationships in terms of roles, entities, and application data traffic.

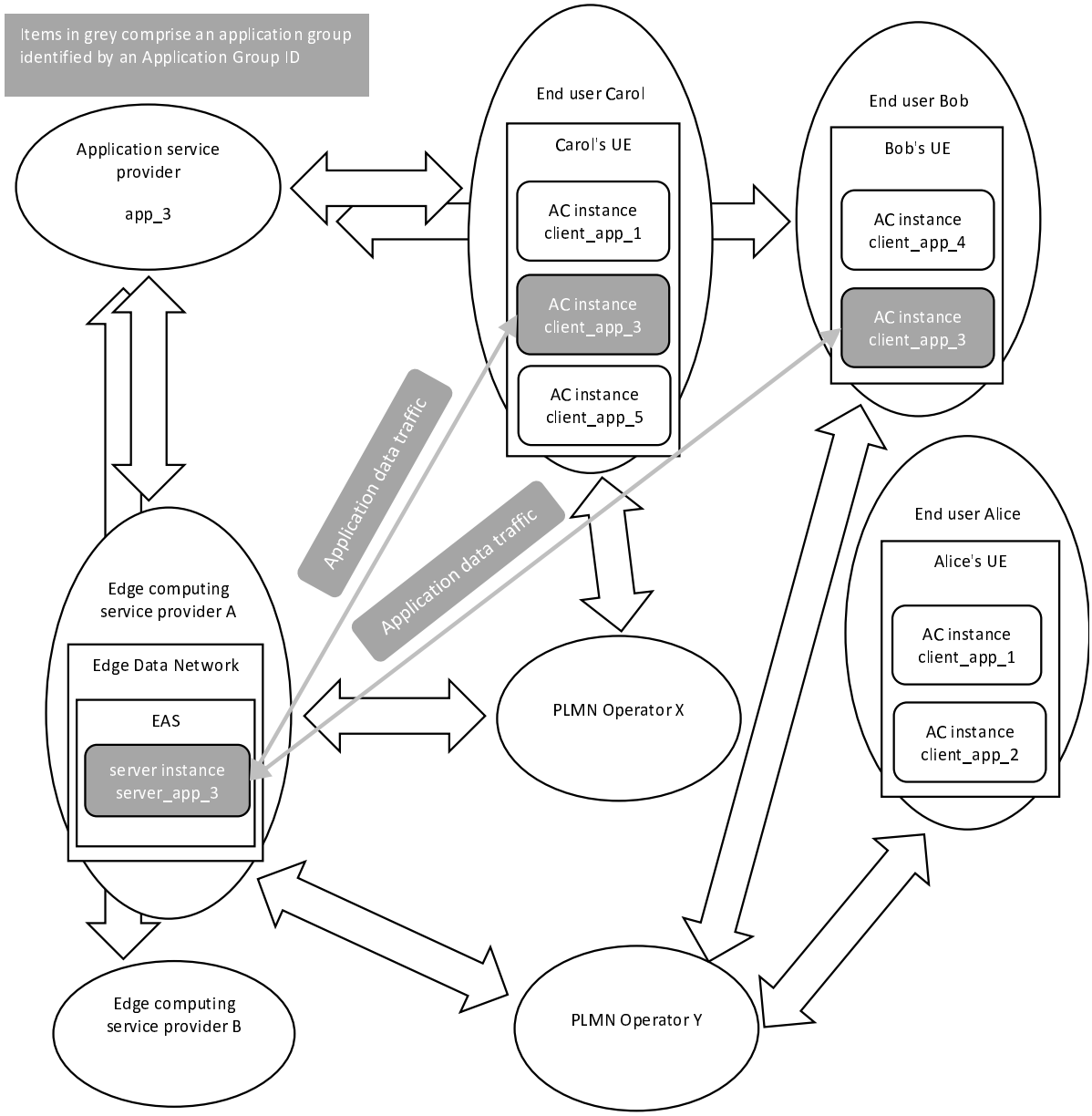

Figure B.3-1: Relationships involved in application clients served by a common server

The application service provider controls app_3 in all locations, including at different ECSPs, and provides application clients to end users. The Application Group ID links a server and clients that are all part of the application service "app_3".

The Application Group ID is unique within the application service. For a given application, no two groups of application clients share the same Application Group ID. Application Group ID is unique across ECSPs and PLMNs, i.e. the Application Group ID alone is sufficient to identify the group in Figure B-X (without any ECSP, PLMN, or EAS identifiers).

"client_app_3" and "server_app_3" indicate client and server instances running on the UE and the EAS respectively, they are not identities such as ACID, EAS ID that are used in the procedures defined in this specification.

Bob's UE and Carol's UE can be thought of as being in the same group but could also simultaneously be in other groups unrelated to app_3. An app_3 group being simultaneously provided to other app_3 clients will use a different Application Group ID. In all cases, the ASP is the single point of control of Application Group ID.

Annex C (Informative): Relationship with ETSI MEC architecture

The content of this clause has been captured in TR 23.958[27].

C.1 Void

C.2 Void

Annex D (Informative): Relationship with GSMA OPG

The content of this clause has been captured in TR 23.958[27].

D.1 Void

D.2 Void

Annex E (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2020-01	SA6#35	S6-200283				TS skeleton	0.0.0
2020-01	SA6#35					S6-200284, S6-200285, S6-200286, S6-200288, S6-200289, S6-200294, S6-200298, S6-200299, S6-200305, S6-200307, S6-200328, S6-200338, S6-200339, S6-200341, S6-200342, S6-200343, S6-200344, S6-200345, S6-200346, S6-200347, S6-200352, S6-200353, S6-200358	0.1.0
2020-01						Editorial corrections by MCC.	0.1.1
2020-01						Editorial corrections by Rapporteur.	0.1.2
2020-04	SA6#36 BIS-e					S6-200443, S6-200489, S6-200545, S6-200546, S6-200548, S6-200550, S6-200556, S6-200564, S6-200565, S6-200566, S6-200577, S6-200592, S6-200593, S6-200594, S6-200596, S6-200598, S6-200599, S6-200601, S6-200603, S6-200607, S6-200618, S6-200621	0.2.0
2020-06	SA6#37-e					S6-200725, S6-200751, S6-200753, S6-200756, S6-200785, S6-200839, S6-200849, S6-200852, S6-200881, S6-200883, S6-200884, S6-200885, S6-200903, S6-200913, S6-200917, S6-200919, S6-200920, S6-200924, S6-200926, S6-200927, S6-200930, S6-200931, S6-200944, S6-200951, S6-200952, S6-200953, S6-200954, S6-200955	0.3.0
2020-08	SA6#38-e					S6-201024, S6-201028, S6-201036, S6-201101, S6-201102, S6-201104, S6-201120, S6-201140, S6-201144, S6-201173, S6-201261, S6-201264, S6-201267, S6-201281, S6-201282, S6-201284, S6-201287, S6-201289, S6-201298, S6-201299, S6-201302, S6-201303, S6-201305, S6-201308, S6-201311, S6-201316, S6-201317, S6-201318, S6-201320, S6-201321, S6-201322, S6-201323, S6-201324, S6-201325	0.4.0
2020-09	SA6#39-e					S6-201448, S6-201450, S6-201457, S6-201584, S6-201591, S6-201592, S6-201605, S6-201607, S6-201608, S6-201609, S6-201610, S6-201611, S6-201612, S6-201613, S6-201614, S6-201622, S6-201623, S6-201626, S6-201627, S6-201635, S6-201636, S6-201674, S6-201675, S6-201676, S6-201677, S6-201678, S6-201679, S6-201680, S6-201681, S6-201682	0.5.0
2020-09	SA#89-e	SP-200828				Presentation for information at SA#89-e	1.0.0
2020-10	SA6#39 BIS-e					S6-201770, S6-201801, S6-201808, S6-201826, S6-201829, S6-201891, S6-201892, S6-201893, S6-201907, S6-201916, S6-201917, S6-201920, S6-201921, S6-201957, S6-201958, S6-201964, S6-201968, S6-201969, S6-201984, S6-201985, S6-202023, S6-202024, S6-202026, S6-202027, S6-202028, S6-202029, S6-202030, S6-202031, S6-202032, S6-202033, S6-202034	1.1.0
2020-11	SA6#40-e					S6-202074, S6-202078, S6-202091, S6-202103, S6-202122, S6-202135, S6-202153, S6-202154, S6-202156, S6-202162, S6-202163, S6-202166, S6-202167, S6-202188, S6-202191, S6-202241, S6-202246, S6-202252, S6-202255, S6-202266, S6-202270, S6-202271, S6-202272, S6-202273, S6-202282, S6-202283, S6-202286, S6-202289, S6-202290, S6-202313, S6-202316, S6-202317, S6-202333, S6-202334, S6-202335, S6-202336, S6-202337, S6-202338, S6-202339, S6-202340, S6-202341, S6-202356, S6-202361	1.2.0
2021-01	SA6#41-e					S6-210042, S6-210116, S6-210118, S6-210131, S6-210139, S6-210201, S6-210206, S6-210207, S6-210222, S6-210227, S6-210229, S6-210230, S6-210231, S6-210232, S6-210238, S6-210241, S6-210243, S6-210277, S6-210285, S6-210289, S6-210290, S6-210291, S6-210306, S6-210309, S6-210334, S6-210335, S6-210336, S6-210337, S6-210338, S6-210339, S6-210340, S6-210341, S6-210342, S6-210343, S6-210344, S6-210345, S6-210346, S6-210347, S6-210348	1.3.0
2021-03	SA6#42-e					S6-210431, S6-210435, S6-210463, S6-210466, S6-210498, S6-210505, S6-210506, S6-210509, S6-210510, S6-210516, S6-210521, S6-210622, S6-210624, S6-210631, S6-210632, S6-210634, S6-210635, S6-210636, S6-210648, S6-210657, S6-210658, S6-210659, S6-210663, S6-210666, S6-210667, S6-210668, S6-210670, S6-210695, S6-210697, S6-210703, S6-210722, S6-210723, S6-210724, S6-210725, S6-210726, S6-210727, S6-210728, S6-210729, S6-210730, S6-210731, S6-210732, S6-210733	1.4.0
2021-03	SA#91-e	SP-210175	0001			Presentation for approval at SA#91-e	2.0.0
2021-04	SA6#42-BIS-e					S6-210802, S6-210872, S6-210882, S6-210884, S6-210955, S6-210956, S6-210980, S6-210982, S6-210983, S6-211002, S6-211005, S6-211013, S6-211018, S6-211022, S6-211052, S6-211054, S6-211055, S6-211056, S6-211079, S6-211108, S6-211109, S6-211110, S6-211111, S6-211113, S6-211114, S6-211115, S6-211116, S6-211117, S6-211119	2.1.0

2021-06	SA6#43-e					S6-211174, S6-211176, S6-211177, S6-211206, S6-211235, S6-211267, S6-211274, S6-211328, S6-211345, S6-211356, S6-211373, S6-211375, S6-211376, S6-211383, S6-211384, S6-211419, S6-211421, S6-211423, S6-211424, S6-211436, S6-211437, S6-211471, S6-211472, S6-211473, S6-211474, S6-211475, S6-211476, S6-211477, S6-211478, S6-211479, S6-211488	2.2.0
2021-06	SA#92-e	SP-210472				Presentation for approval at SA#92-e	2.2.1
2021-06	SA#92-e	SP-210580				MCC Editorial update for publication after TSG SA approval (SA#92)	17.0.0
2021-09	SA#93	SP-210961	0001	-	F	Update on ECS configuration information	17.1.0
2021-09	SA#93	SP-210961	0003	2	F	Corrections for AC and EEC initiated ACR scenario	17.1.0
2021-09	SA#93	SP-210961	0004	1	F	Correct service provisioning overview	17.1.0
2021-09	SA#93	SP-210961	0006	2	F	Solve EN for E1 traffic monitoring	17.1.0
2021-09	SA#93	SP-210961	0007		F	Solve EN for scenario#5	17.1.0
2021-09	SA#93	SP-210961	0008	4	F	EEC context relocation	17.1.0
2021-09	SA#93	SP-210961	0009		F	EAS DNAIs	17.1.0
2021-09	SA#93	SP-210961	0010		F	Corrections to ACR request and response	17.1.0
2021-09	SA#93	SP-210961	0011	1	F	Reference corrections	17.1.0
2021-09	SA#93	SP-210961	0012		F	Reference updates	17.1.0
2021-09	SA#93	SP-210961	0017	1	F	Adding ACR management event notification	17.1.0
2021-09	SA#93	SP-210961	0019		F	Remove EN on automated ACR service message	17.1.0
2021-09	SA#93	SP-210961	0020		F	Remove the EAS status of EAS discovery filter	17.1.0
2021-09	SA#93	SP-210961	0024	1	F	Resolving EN about Automated ACR terminology	17.1.0
2021-09	SA#93	SP-210961	0026	2	F	Resolving the editor's note on the use of SBA terminology	17.1.0
2021-09	SA#93	SP-210961	0027	4	F	Resolve EN on AC Profile Parameter Ranges IE	17.1.0
2021-09	SA#93	SP-210961	0030	2	F	Corrections to references, descriptions, and clause title of TS 23.558	17.1.0
2021-09	SA#93	SP-210961	0033	1	F	GPSI format	17.1.0
2021-09	SA#93	SP-210961	0034		F	EN on ECS info in UE subscription data	17.1.0
2021-09	SA#93	SP-210961	0036	2	F	ACR preconditions for EEC	17.1.0
2021-09	SA#93	SP-210961	0039	1	F	Corrections to ACR launching procedure	17.1.0
2021-09	SA#93	SP-210961	0040	1	F	Corrections to T-EES discovery	17.1.0
2021-09	SA#93	SP-210961	0041		F	SA3 references	17.1.0
2021-09	SA#93	SP-210961	0044	1	F	Provide EES endpoint in ACR request to enable EEC context relocation during ACR	17.1.0
2021-12	SA#94	SP-211522	0042	5	F	Cancellation Support in ACR	17.2.0
2021-12	SA#94	SP-211522	0053	2	F	Modify the entity description and add abbreviation	17.2.0
2021-12	SA#94	SP-211522	0054	2	F	List of subscriptions to the CN in EEC context	17.2.0
2021-12	SA#94	SP-211522	0056	4	F	Adding DNN/S-NSSAI information in EAS profile	17.2.0
2021-12	SA#94	SP-211522	0057	2	F	Correction on ACR failure alleviation mechanisms	17.2.0
2021-12	SA#94	SP-211522	0058	2	F	Correction on ACR information subscription request	17.2.0
2021-12	SA#94	SP-211522	0060	2	F	Correction on connectivity information	17.2.0
2021-12	SA#94	SP-211522	0062	2	F	Text order and wording corrections for ACR scenarios	17.2.0
2021-12	SA#94	SP-211522	0063	1	F	Edge functional entity relationship to 5G core	17.2.0
2021-12	SA#94	SP-211522	0064	1	F	Correction on EAS description	17.2.0
2021-12	SA#94	SP-211522	0065	1	F	Correct ACR inconsistencies	17.2.0
2021-12	SA#94	SP-211522	0066	1	F	Correct EAS required API	17.2.0
2021-12	SA#94	SP-211522	0069	1	F	Functional entity responsibilities related to ACR	17.2.0
2021-12	SA#94	SP-211522	0072	1	F	Fixes in EAS Discovery procedures	17.2.0
2021-12	SA#94	SP-211522	0074	2	F	Corrections to general requirements for service continuity	17.2.0
2022-03	SA#95	SP-220103	0079	1	F	Fix consistency issue	17.3.0
2022-03	SA#95	SP-220103	0081	1	F	Solve ACR API inconsistency	17.3.0
2022-03	SA#95	SP-220103	0085	2	F	Adding missing events for ACR notifications	17.3.0
2022-03	SA#95	SP-220103	0086		F	Correction of ACR request and response messages	17.3.0
2022-03	SA#95	SP-220103	0087	1	F	Unique identification in ACR procedures	17.3.0
2022-03	SA#95	SP-220103	0088	1	F	Unique identification of the EEC context in ACR procedures	17.3.0
2022-06	SA#96	SP-220472	0083	4	F	Implicit registration handling in service continuity	17.4.0
2022-06	SA#96	SP-220472	0089	1	F	Removal of the Editor's Note on dynamic EAS instantiation information	17.4.0
2022-06	SA#96	SP-220472	0090	1	F	Fix S-EAS decided ACR	17.4.0
2022-06	SA#96	SP-220472	0091	1	F	Solve EN in UE ID API	17.4.0
2022-06	SA#96	SP-220472	0092	1	F	Update to EEC registration update procedure	17.4.0
2022-06	SA#96	SP-220472	0093	1	F	Corrections to the ECS configuration information	17.4.0
2022-06	SA#96	SP-220472	0095	3	F	Corrections for selected T-EAS declaration	17.4.0
2022-06	SA#96	SP-220472	0096	1	F	Corrections for incomplete functions of ECS and EDGE-6	17.4.0
2022-06	SA#96	SP-220472	0097	1	F	Corrections to ACT status subscription and notification	17.4.0
2022-06	SA#96	SP-220472	0098	1	F	Issues on usage of ACR with LADNs	17.4.0
2022-06	SA#96	SP-220472	0103	1	F	Solve EN in ACR	17.4.0
2022-06	SA#96	SP-220472	0104	1	F	Solve EN in ACR Correction to the supported functions of EDGE-9	17.4.0
2022-06	SA#96	SP-220472	0106	2	F	Corrections to the incompleteness and format errors	17.4.0

2022-09	SA#97	SP-220919	0108	1	F	Add security info in service provisioning response	17.5.0
2022-09	SA#97	SP-220919	0109	1	F	Clarify location user consent	17.5.0
2022-09	SA#97	SP-220919	0114	1	F	Introduction of a reference to charging	17.5.0
2022-09	SA#97	SP-220919	0117	2	F	Correction to Relationship between EDGEAPP and ETSI MEC architectures	17.5.0
2022-09	SA#97	SP-220919	0122	1	F	Correction of EES discovery to EAS discovery	17.5.0
2022-09	SA#97	SP-220922	0119	1	B	EDGE-5 APIs	18.0.0
2022-09	SA#97	SP-220922	0120	2	B	Edge Notification Service - architecture	18.0.0
2022-09	SA#97	SP-220922	0121	2	B	Edge Notification Service - solution	18.0.0
2022-12	SA#98	SP-221242	0123	6	B	ACR Scenario Combination	18.1.0
2022-12	SA#98	SP-221242	0124	2	C	Implementation of TR 23.700-98 solution for KI#8	18.1.0
2022-12	SA#98	SP-221242	0125		B	ECS information configured by edge-aware AC	18.1.0
2022-12	SA#98	SP-221242	0126	4	B	Addition of prediction expiration time IE and ACR information procedure	18.1.0
2022-12	SA#98	SP-221242	0127		F	Correct detection entity in EES executed ACR	18.1.0
2022-12	SA#98	SP-221242	0128	2	B	Support more traffic filters	18.1.0
2022-12	SA#98	SP-221242	0129	2	B	Support simu-EAS connectivity in ACR	18.1.0
2022-12	SA#98	SP-221242	0130	3	B	ACR request trigger timing	18.1.0
2022-12	SA#98	SP-221242	0131	1	B	Updates to architectural assumptions for EAS Service APIs enablement	18.1.0
2022-12	SA#98	SP-221242	0134	2	B	MCC note: Not implemented as CR was revised in 148R5	18.1.0
2022-12	SA#98	SP-221242	0135	5	B	Traffic influence for initial EAS discovery	18.1.0
2022-12	SA#98	SP-221242	0139	2	B	eEDGE_Application traffic influence trigger from EAS	18.1.0
2022-12	SA#98	SP-221242	0140	3	B	AF traffic influence for a given EAS	18.1.0
2022-12	SA#98	SP-221238	0144		A	Correction of ACR management notification	18.1.0
2022-12	SA#98	SP-221242	0145	2	B	Update ACR scenarios with ACR parameter procedure	18.1.0
2022-12	SA#98	SP-221242	0147	5	B	EAS instantiation status provisioned by ECS	18.1.0
2022-12	SA#98	SP-221242	0148	5	B	EES monitoring the UE mobility for service continuity planning	18.1.0
2022-12	SA#98	SP-221242	0149	3	B	EDGE-5 – AC registration	18.1.0
2022-12	SA#98	SP-221242	0150	1	B	EDGE-5 – EAS discovery	18.1.0
2022-12	SA#98	SP-221242	0152	3	B	EDGE-5 – Subscription	18.1.0
2022-12	SA#98	SP-221242	0153		B	Updates to Involved entities and relationships	18.1.0
2023-03	SA#99	SP-230286	0136	5	B	Dynamic EAS instantiation enhancements	18.2.0
2023-03	SA#99	SP-230286	0138	11	B	EEC triggering service	18.2.0
2023-03	SA#99	SP-230278	0141	3	A	Correction for EEC registration expiration time	18.2.0
2023-03	SA#99	SP-230286	0154		D	Editorial correction "General Context holding time duration" IE usage	18.2.0
2023-03	SA#99	SP-230286	0155	5	B	New AC-EEC procedure to invoke UE ID request	18.2.0
2023-03	SA#99	SP-230286	0156	6	B	Updating UE Identifier API procedure to enable EEC invoke UE ID request for NATed IP address	18.2.0
2023-03	SA#99	SP-230286	0158	2	B	Adding a CAPIF deployment for exposure of EAS Service APIs	18.2.0
2023-03	SA#99	SP-230286	0159	6	B	Supporting dynamic EAS instantiation triggering and notifications	18.2.0
2023-03	SA#99	SP-230278	0161		A	Corrections to A.5 of TS 23.558 for CAPIF deployment	18.2.0
2023-03	SA#99	SP-230278	0163		A	Correction to 'Event ID' IE of EAS discovery notification	18.2.0
2023-03	SA#99	SP-230301	0165	4	C	Update ACR parameter information procedure	18.2.0
2023-03	SA#99	SP-230286	0167	2	B	Architecture with CAS and CES	18.2.0
2023-03	SA#99	SP-230286	0168	2	B	EAS discovery support for constraint UE	18.2.0
2023-03	SA#99	SP-230286	0170	1	B	Selected EAS instantiation	18.2.0
2023-03	SA#99	SP-230286	0171		B	Solve EN about multi-EAS connection	18.2.0
2023-03	SA#99	SP-230294	0173	1	B	Seamless transport support	18.2.0
2023-03	SA#99	SP-230286	0176	1	D	Update description of EAS information element in ACR information notification table	18.2.0
2023-03	SA#99	SP-230286	0183	2	B	Relationship between EDGEAPP and ETSI MEC	18.2.0
2023-03	SA#99	SP-230286	0190	2	B	ACR scenario selection enhancement	18.2.0
2023-03	SA#99	SP-230286	0193	2	B	Fix inconsistency of service continuity planning	18.2.0
2023-03	SA#99	SP-230301	0196	4	B	Support for federation and roaming	18.2.0
2023-03	SA#99	SP-230286	0197	2	B	ACR modification procedure	18.2.0
2023-03	SA#99	SP-230286	0198	1	F	Delete the remaining Editor’s note in clause 8.8.3.9	18.2.0
2023-03	SA#99	SP-230286	0201	1	B	Definitions of terms, symbols and abbreviations	18.2.0
2023-03	SA#99	SP-230286	0203	2	B	Solution #38 - completion	18.2.0
2023-03	SA#99	SP-230301	0205	3	B	Resolving EN in clause 8.15	18.2.0
2023-03	SA#99	SP-230301	0207	5	B	EEC sharing UE Mobility requirement	18.2.0

2023-03	SA#99	SP-230286	0211		F	Delete the Editor's note in ACR scenarios	18.2.0
2023-03	SA#99	SP-230278	0213	1	A	Corrections to ECS configuration information	18.2.0
2023-03	SA#99	SP-230301	0214	5	B	ACR trigger request on EDGE-5	18.2.0
2023-03	SA#99	SP-230301	0220	4	C	Updates to dynamic instantiation solution	18.2.0
2023-03	SA#99	SP-230286	0222	2	B	Architecture for ACR between edge and cloud	18.2.0
2023-03	SA#99	SP-230301	0229	2	B	EAS-specific UE ID (Edge UE ID)	18.2.0
2023-03	SA#99	SP-230301	0230	2	B	Explaining usage of EES's capability exposure by EEC	18.2.0
2023-03	SA#99	SP-230301	0231	2	F	UE ID definition Clarification	18.2.0
2023-03	SA#99	SP-230301	0232	1	F	Editorial corrections	18.2.0
2023-03	SA#99	SP-230301	0233	2	B	Support Discover T-EAS with Edge load performance information	18.2.0
2023-03	SA#99	SP-230301	0234	3	B	ACR procedure btw EAS and CAS	18.2.0
2023-03	SA#99	SP-230301	0235	5	B	EAS discovery in edge node sharing	18.2.0
2023-03	SA#99	SP-230301	0236	3	B	EES service differentiation	18.2.0
2023-03	SA#99	SP-230301	0237		B	Support Edge computing in SNPN	18.2.0
2023-03	SA#99	SP-230301	0238	2	F	Correction of service provisioning overview	18.2.0
2023-03	SA#99	SP-230301	0240	2	B	ACR scenario re-selection after a successful ACR	18.2.0
2023-03	SA#99	SP-230278	0246		A	Corrections to EES provider information	18.2.0
2023-03	SA#99	SP-230301	0247	2	B	EAS bundles	18.2.0
2023-03	SA#99	SP-230301	0248	1	B	EDGE-5 release scope	18.2.0
2023-03	SA#99	SP-230278	0252	2	A	Clarification for EES executed ACR scenario	18.2.0
2023-03	SA#99	SP-230301	0254	2	B	EEC selected ACR scenario for EAS bundles	18.2.0
2023-03	SA#99	SP-230301	0255	2	B	EES determines ACR scenario for EAS bundles	18.2.0
2023-03	SA#99	SP-230301	0258	2	F	Fix the inconsistency in EAS discovery	18.2.0
2023-03	SA#99	SP-230301	0259	2	F	Fix the inconsistency in ACR complete message	18.2.0
2023-03	SA#99	SP-230301	0263	2	F	T-EES selection considering the service continuity support information	18.2.0
2023-03	SA#99	SP-230301	0264	1	B	Enabling ACR with cloud applications	18.2.0
2023-06	SA#100	SP-230699	0265	1	F	Correcting a NOTE related to UE Identifier API	18.3.0
2023-06	SA#100	SP-230699	0266	1	B	Updating clause 4.5 to also indicate EES Capability Exposure to EEC	18.3.0
2023-06	SA#100	SP-230699	0267	1	B	Updating missing EEC's supporting functions	18.3.0
2023-06	SA#100	SP-230699	0268	1	F	Update on ECS discovery procedure description regarding DNN and slice information	18.3.0
2023-06	SA#100	SP-230699	0269	2	B	Resolve EN on EAS Acknowledgement for service continuity planning	18.3.0
2023-06	SA#100	SP-230699	0270	1	B	Optionality of Trigger Description for EEC Triggering Service	18.3.0
2023-06	SA#100	SP-230699	0271	3	B	Moving alignment Annex from TS to external TR	18.3.0
2023-06	SA#100	SP-230699	0272	1	F	Correction in description of EESID information element in Retrieve EES request Table 8.8.4.6-1	18.3.0
2023-06	SA#100	SP-230699	0273	1	B	Availability of EEC triggering service	18.3.0
2023-06	SA#100	SP-230699	0276	2	F	CAS requirements and cardinalities	18.3.0
2023-06	SA#100	SP-230699	0279	2	B	Clarifications on Instantiable EAS Information	18.3.0
2023-06	SA#100	SP-230699	0281	1	D	Resolving Editor's Note about ECS registration	18.3.0
2023-06	SA#100	SP-230699	0282	1	B	Resolving Editor's Note about CES features	18.3.0
2023-06	SA#100	SP-230699	0284	1	B	General clause for roaming and federation	18.3.0
2023-06	SA#100	SP-230699	0286	2	B	Resolving Editor's Note about T-EAS discovery	18.3.0
2023-06	SA#100	SP-230699	0288	1	B	Reference correction for service continuity clauses	18.3.0
2023-06	SA#100	SP-230699	0290	2	F	Correction in the description of requestor identifier in ACR request table	18.3.0
2023-06	SA#100	SP-230698	0294	1	A	Correction of ACR management notification	18.3.0
2023-06	SA#100	SP-230698	0296	1	A	ACR scenario correction to include post-ACR clean-up for service continuity planning	18.3.0
2023-06	SA#100	SP-230699	0297		B	Definition of the API of ACR parameter information	18.3.0
2023-06	SA#100	SP-230699	0299	1	B	Usage of ADAES for edge load analytics	18.3.0
2023-06	SA#100	SP-230699	0304	2	B	Enhancement on EAS instantiation notification	18.3.0
2023-06	SA#100	SP-230699	0306	2	F	Resolve the EN in the EEC executed ACR via T-EES	18.3.0
2023-06	SA#100	SP-230700	0308	9	F	Common EAS discovery	18.3.0
2023-06	SA#100	SP-230698	0310		A	Clarification for EAS decided ACR scenario	18.3.0
2023-06	SA#100	SP-230700	0312	4	B	ENS – IE tables updates	18.3.0
2023-06	SA#100	SP-230700	0315	2	C	Removing AC registration	18.3.0
2023-06	SA#100	SP-230700	0316	2	B	Subscription for service provisioning information retrieval by ECS	18.3.0
2023-06	SA#100	SP-230700	0317	5	B	Information flows - Federation and roaming	18.3.0
2023-06	SA#100	SP-230700	0318	2	C	Replacing OP terminology and reusing existing procedures for ENS	18.3.0
2023-06	SA#100	SP-230700	0319	1	C	Applicability of service provisioning information retrieval for federation	18.3.0
2023-06	SA#100	SP-230700	0321	1	C	EAS bundle types and bundle requirements	18.3.0

2023-06	SA#100	SP-230700	0322		D	Cleanup of EES provider IDs	18.3.0
2023-06	SA#100	SP-230700	0326	2	D	EES specfic UE ID	18.3.0
2023-06	SA#100	SP-230700	0327		F	Fix EAS discovery	18.3.0
2023-06	SA#100	SP-230700	0328	5	B	More procedures with CES	18.3.0
2023-06	SA#100	SP-230700	0329	1	F	Reference and editorial corrections	18.3.0
2023-06	SA#100	SP-230700	0331	1	F	Profile information sources	18.3.0
2023-06	SA#100	SP-230700	0333	2	C	Dynamic instantiation at registration	18.3.0
2023-06	SA#100	SP-230700	0334	2	B	ACR with CAS - EEC executed ACR via S-EES	18.3.0
2023-06	SA#100	SP-230700	0337	1	B	ACR with CAS - S-EAS decided ACR	18.3.0
2023-06	SA#100	SP-230700	0338	2	B	ACR with CAS - S-EES executed ACR	18.3.0
2023-06	SA#100	SP-230700	0340	1	C	ACR between Edge and Cloud in Overload Situations	18.3.0
2023-06	SA#100	SP-230700	0341	1	D	Editorial clean up	18.3.0
2023-06	SA#100	SP-230700	0342	1	F	CES clarifications and editorial fix	18.3.0
2023-06	SA#100	SP-230700	0343	2	C	Retrieve EES List	18.3.0
2023-06	SA#100	SP-230700	0347	1	B	Invoke non-roaming UE location	18.3.0
2023-06	SA#100	SP-230701	0349	3	B	Application groups entity relationships	18.3.0
2023-06	SA#100	SP-230701	0353	1	C	Remove the EN in cl.8.2.2 in TS 23.558	18.3.0
2023-06	SA#100	SP-230701	0354	1	F	Clarification on the decision-making entity and execution entity	18.3.0
2023-06	SA#100	SP-230701	0355	1	B	EEC Triggering execution for Service Provisioning	18.3.0
2023-06	SA#100	SP-230701	0356	2	B	EEC Triggering execution	18.3.0
2023-06	SA#100	SP-230701	0357	3	C	Application Group Profile EN resolution proposal	18.3.0
2023-06	SA#100	SP-230701	0358	1	D	Clarification Application Group ID definition	18.3.0
2023-06	SA#100	SP-230701	0360	1	B	Handling instantiation-in-progress status at the EAS discovery subscription procedure	18.3.0
2023-06	SA#100	SP-230701	0361	1	B	Provision ECS configuration information together with PLMN ID to 5GC	18.3.0
2023-06	SA#100	SP-230701	0362	1	B	EEC Triggering setup for EAS discovery	18.3.0
2023-06	SA#100	SP-230701	0363		D	ACR Parameter Information procedure clarification	18.3.0
2023-06	SA#100	SP-230701	0365	1	F	Support for ACR between EAS and CAS	18.3.0
2023-06	SA#100	SP-230701	0366	1	F	Corrections to ACR management event notification	18.3.0
2023-06	SA#100	SP-230698	0367	1	A	EASID definition update	18.3.0
2023-06	SA#100	SP-230701	0368		B	Information element alignment for ECS discovery	18.3.0
2023-06	SA#100	SP-230701	0370		B	Use of ECS profile instead of ECS configuration information	18.3.0
2023-06	SA#100	SP-230701	0371	1	B	Service continuity for EAS composition	18.3.0
2023-06	SA#100	SP-230701	0373	1	C	Details of EAS information	18.3.0
2023-06	SA#100	SP-230701	0376	2	B	Bundle EAS ACR within the same DNAI for S-EES executed ACR	18.3.0
2023-06	SA#100	SP-230701	0378	2	F	Fix the in-consistency for the service continuity support	18.3.0
2023-06	SA#100	SP-230701	0379	1	F	Fix the misalignment on UE ID API request	18.3.0
2023-06	SA#100	SP-230701	0382	3	B	T-EES discovery enhancement for composite EAS	18.3.0
2023-06	SA#100	SP-230701	0383	4	B	ACR for EAS bundle	18.3.0
2023-06	SA#100	SP-230702	0385	4	B	EAS synchronization	18.3.0
2023-06	SA#100	SP-230702	0386	4	B	Edge performance prediction	18.3.0
2023-06	SA#100	SP-230702	0387		B	IE table update for ENS	18.3.0
2023-06	SA#100	SP-230702	0388	3	B	Interaction with CR in common EAS discovery	18.3.0
2023-06	SA#100	SP-230702	0389	2	B	Selected EES declaration	18.3.0
2023-06	SA#100	SP-230702	0390	2	B	Correction and alignment for EAS instantiation status	18.3.0
2023-06	SA#100	SP-230702	0391	1	B	Ability details of handling bundled EAS ACR	18.3.0
2023-06	SA#100	SP-230702	0392	1	F	Resolving SA3 dependent ENs	18.3.0
2023-06	SA#100	SP-230702	0393		F	Resolving EN related to possible deployment models of the ECS	18.3.0
2023-06	SA#100	SP-230702	0394		F	Resolving EN about updating EEC Context with EDGE-3 subscriptions	18.3.0
2023-06	SA#100	SP-230702	0395	1	F	Resolving EN related to redirection	18.3.0
2023-06	SA#100	SP-230702	0396		F	Resolving EN on constrained device identification	18.3.0
2023-06	SA#100	SP-230702	0399	1	F	Resolving EN related to ACR	18.3.0
2023-06	SA#100	SP-230702	0401	2	B	CAS decided ACR scenario via old S-EES for CESless architecture	18.3.0
2023-06	SA#100	SP-230702	0402		C	EEC subscribing to SEAL notification service and requesting UE ID in ACR to CAS	18.3.0
2023-06	SA#100	SP-230702	0403	3	F	AC information exposure update and correction	18.3.0
2023-06	SA#100	SP-230702	0404	1	C	Resolving the ENs related to retrieve EES procedure	18.3.0
2023-06	SA#100	SP-230702	0405	3	C	Resolving EN in ACR to Cloud	18.3.0
2023-06	SA#100	SP-230698	0407		A	EES is provided by ECSP and is not necessarily in PLMN domain.	18.3.0
2023-06	SA#100	SP-230698	0408	1	A	Alignment of terminologies for the ECSP management system	18.3.0
2023-09	SA#101	SP-230994	0413	1	F	Modify term from central repository to ECS-ER	18.4.0
2023-09	SA#101	SP-230994	0416	1	F	Status correction for Session with QoS create request IEs	18.4.0
2023-09	SA#101	SP-230994	0417	3	F	Complete common EAS serving an EDN	18.4.0
2023-09	SA#101	SP-230994	0418	1	F	Complete ECS-ER API	18.4.0
2023-09	SA#101	SP-230994	0419	1	F	Complete EES declaration API	18.4.0
2023-09	SA#101	SP-230994	0420	1	F	Correct application group id description	18.4.0

2023-09	SA#101	SP-230994	0421		F	Correct desired ECSP id handling	18.4.0
2023-09	SA#101	SP-230994	0422	1	F	Fix ACR between edge and cloud	18.4.0
2023-09	SA#101	SP-230994	0423	2	F	Fix ACR management event	18.4.0
2023-09	SA#101	SP-230994	0424	1	F	Solve EN for ACR in ENS	18.4.0
2023-09	SA#101	SP-230994	0429	3	F	Authentication methods in ECS configuration	18.4.0
2023-09	SA#101	SP-230994	0430		F	Correcting analytics info IE	18.4.0
2023-09	SA#101	SP-230994	0432	1	F	APIs for EDGE-5 interface	18.4.0
2023-09	SA#101	SP-230994	0434	1	F	Duplicate IE in EAS information provisioning request	18.4.0
2023-09	SA#101	SP-230994	0436	1	F	IE Correction on Service Provisioning request	18.4.0
2023-09	SA#101	SP-230994	0438		F	API definition of EAS information Provisioning	18.4.0
2023-09	SA#101	SP-230994	0439	1	F	API definition of common EAS announcement	18.4.0
2023-09	SA#101	SP-231042	0440	1	F	API definition of roaming and federation	18.4.0
2023-09	SA#101	SP-231042	0445		F	Missing APIs in the EES-provided API Table	18.4.0
2023-09	SA#101	SP-231042	0447		F	Corrections to the notification procedures for EEC triggering	18.4.0
2023-09	SA#101	SP-231042	0448	2	F	Solve EN in EAS information provisioning procedure	18.4.0
2023-09	SA#101	SP-231042	0449	1	F	Editorial corrections	18.4.0
2023-09	SA#101	SP-231042	0450	1	F	Resolve EN in bundle information	18.4.0
2023-09	SA#101	SP-231042	0451	1	F	Corrections for alignment with CAPIF deployments	18.4.0
2023-09	SA#101	SP-231042	0452	2	F	Correction for bundle in EDN configuration information	18.4.0
2023-09	SA#101	SP-231042	0454	2	F	Resolve the EN on Application group profile	18.4.0
2023-09	SA#101	SP-231042	0455	4	F	Clean-up on the bundle EAS	18.4.0
2023-09	SA#101	SP-231042	0456	1	F	Resolve the EN on ACR management event API	18.4.0
2023-09	SA#101	SP-231042	0457	2	F	Resolve the EN on ACR management subscription request	18.4.0
2023-09	SA#101	SP-231042	0458	1	F	Resolve the EN on discover T-EAS	18.4.0
2023-09	SA#101	SP-231042	0461	1	F	Resolve the EN on EEC context handling procedure	18.4.0
2023-09	SA#101	SP-231042	0462		F	Resolve the EN on selected ACR scenario list transmission	18.4.0
2023-09	SA#101	SP-231042	0464	2	F	Cleanup on CAS decided ACR scenario via the last S-EES	18.4.0
2023-09	SA#101	SP-231042	0466	2	F	Clarifications on proxy bundle type	18.4.0
2023-12	SA#102	SP-231549	0467	2	F	Correction on EAS bundle discovery	18.5.0
2023-12	SA#102	SP-231549	0478	2	F	EAS bundle information corrections	18.5.0
2023-12	SA#102	SP-231549	0480	-	F	Solving EN to pass on EASID in Nnef_UEId	18.5.0
2023-12	SA#102	SP-231549	0482	-	F	Clarification on ACR from edge to cloud	18.5.0
2023-12	SA#102	SP-231549	0484	1	F	Solving EN on selected ACR scenario transfer	18.5.0
2023-12	SA#102	SP-231549	0485	2	F	Solving EN on CAS - S-EES executed ACR	18.5.0
2023-12	SA#102	SP-231549	0486	3	F	Functionalities of ECI-1	18.5.0
2023-12	SA#102	SP-231549	0487	6	F	Remove ENs regarding use of EASID / EESID in place of AF Identifier	18.5.0
2023-12	SA#102	SP-231549	0489	1	F	event ID description in ACR management event subscribe request	18.5.0
2023-12	SA#102	SP-231549	0490	1	F	Service continuity	18.5.0
2023-12	SA#102	SP-231549	0492	1	F	Resolve the EN on EES interaction with the Central repository	18.5.0
2023-12	SA#102	SP-231549	0494		F	APIs for ENS	18.5.0
2023-12	SA#102	SP-231549	0496	1	F	Add missing EES endpoint in ECS-ER interaction	18.5.0
2023-12	SA#102	SP-231549	0498		F	Clarify CAS endpoint in T-EAS declaration	18.5.0
2023-12	SA#102	SP-231549	0499	3	F	Add missing event IE to EAS	18.5.0
2023-12	SA#102	SP-231549	0500	1	F	Remove duplication	18.5.0
2023-12	SA#102	SP-231549	0502	4	F	Clarification on default instantiation behaviour for EAS discovery subscription	18.5.0
2023-12	SA#102	SP-231549	0513	2	F	Registrar EES endpoint missing in common EAS procedures	18.5.0
2023-12	SA#102	SP-231549	0516	1	F	Missing definition for Common EES	18.5.0
2023-12	SA#102	SP-231549	0518		F	Correction of the term AC group profile to App Group profile in clause 8.3.3.2.2	18.5.0
2023-12	SA#102	SP-231549	0519	1	F	Correction to add App Group ID info associated with EAS profile in EAS discovery response	18.5.0
2023-12	SA#102	SP-231549	0520	1	F	Correction to the usage of App Group ID list description in Service provisioning response	18.5.0
2023-12	SA#102	SP-231549	0521		F	Correction to the pre-conditions of Common EAS announcement	18.5.0
2023-12	SA#102	SP-231548	0523	1	A	S-EES executed ACR correct reference to missing step	18.5.0
2023-12	SA#102	SP-231548	0524	1	A	UE groups corrections in EES capability exposure to EAS and EEC	18.5.0
2023-12	SA#102	SP-231549	0529	2	F	Clarification on ACR capability and ACR scenario	18.5.0
2023-12	SA#102	SP-231549	0537	2	F	Incomplete EAS discovery notification	18.5.0
2023-12	SA#102	SP-231549	0538	2	F	Add common EAS endpoint in EAS selection response	18.5.0
2023-12	SA#102	SP-231549	0539		F	QoS API correction	18.5.0
2023-12	SA#102	SP-231549	0540	1	F	Remove EN in architecture with CAS	18.5.0
2023-12	SA#102	SP-231549	0543	1	F	Correction on EAS information provisioning procedure	18.5.0
2023-12	SA#102	SP-231549	0544	1	F	Update the dynamic EAS instantiation triggering behavior	18.5.0
2023-12	SA#102	SP-231548	0546		A	Corrections to Eees_EELManagedACR_Notify operation	18.5.0
2023-12	SA#102	SP-231549	0548	1	F	CES functionalities	18.5.0
2023-12	SA#102	SP-231549	0549	2	F	ECI-1 functionalities	18.5.0
2024-03	SA#103	SP-240302	0553	1	F	Correction in S-EES executed ACR to CAS	18.6.0

2024-03	SA#103	SP-240302	0558		F	Remove EN on EAS ID definition	18.6.0
2024-03	SA#103	SP-240302	0560	1	F	Remove EN on EEC triggering service parameter	18.6.0
2024-03	SA#103	SP-240302	0562	1	F	Correction on ECS registration procedure	18.6.0
2024-03	SA#103	SP-240302	0567	3	F	Fix for allowed MNO details IE	18.6.0
2024-03	SA#103	SP-240302	0578	1	F	Add missing common EAS removal	18.6.0
2024-03	SA#103	SP-240302	0580	1	F	CAS consumes EES services	18.6.0
2024-03	SA#103	SP-240302	0582		F	CES consumes EEL services	18.6.0
2024-03	SA#103	SP-240302	0584		F	Clarify CES service	18.6.0
2024-03	SA#103	SP-240302	0598	2	F	Add Update and Cancellation services of Eees_TrafficInfluenceEAS	18.6.0
2024-06	SA#104	SP-240756	0613	2	F	Add Update services of Eees_TrafficInfluenceEAS	18.7.0
2024-06	SA#104	SP-240756	0620		F	Correct ACR information subscription	18.7.0
2024-06	SA#104	SP-240756	0632	2	F	EES as consent enforcing entity	18.7.0
2024-06	SA#104	SP-240756	0634	2	F	Remove EN on simultaneous PSA connectivity	18.7.0
2024-06	SA#104	SP-240751	0636	2	A	EES capability to influence traffic routing	18.7.0
2024-06	SA#104	SP-240756	0639	1	F	Remove EN on EAS instantiation	18.7.0
2024-06	SA#104	SP-240756	0650		F	Solve EN for CAS	18.7.0
2024-06	SA#104	SP-240751	0661		A	Identity token as a UE identifier	18.7.0
2024-06	SA#104	SP-240756	0662	1	C	Add missing ACR failure cause	18.7.0
2024-09	SA#105	SP-241214	0663	1	F	Remove EN on the use of UE ID request from AC	18.8.0
2024-09	SA#105	SP-241214	0665	1	F	Remove EN on exposure of EAS Service APIs across multiple EDNs	18.8.0
2024-09	SA#105	SP-241214	0667		F	Remove EN on ECS-ER	18.8.0
2024-09	SA#105	SP-241214	0668		F	Remove EN on ECS profile	18.8.0
2024-09	SA#105	SP-241214	0675		F	CES consumes EEL services details	18.8.0
2024-09	SA#105	SP-241214	0677		F	EES consumes Eees_AppContextRelocation service	18.8.0
2024-12	SA#106	SP-241706	0688		F	Remove EN on capability exposure via CES	18.9.0
2024-12	SA#106	SP-241706	0690		F	Remove EN on App Group Profile	18.9.0
2024-12	SA#106	SP-241706	0692		F	Remove EN on ECS-ER	18.9.0
2024-12	SA#106	SP-241706	0699	1	F	Correction on ACR scenario determination considering bundle EAS capability	18.9.0
2024-12	SA#106	SP-241706	0700	2	F	Correction on bundle EAS feature	18.9.0
2024-12	SA#106	SP-241706	0702	1	F	EN on EAS ID list in UE ID request from AC	18.9.0
2024-12	SA#106	SP-241706	0704	2	F	EN on ensuring user's authorization/consent and AC's authorization	18.9.0
2024-12	SA#106	SP-241706	0706	1	F	EN on EEC-provided information verification and trustfulness	18.9.0
2024-12	SA#106	SP-241706	0708	1	F	EN on security aspect for app info sharing between ECSPs	18.9.0
2024-12	SA#106	SP-241704	0711	2	A	Resolve EN on AF specific UE identifier	18.9.0

History

Document history		
V18.6.0	April 2024	Publication
V18.7.0	July 2024	Publication
V18.8.0	October 2024	Publication
V18.9.0	January 2025	Publication