ETSI TS 133 558 V19.0.0 (2026-01)

TECHNICAL SPECIFICATION

5G;
Security aspects of enhancement of support for enabling edge applications
(3GPP TS 33.558 version 19.0.0 Release 19)

Reference
RTS/TSGS-0333558vj00

Keywords
5G,SECURITY

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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 4
1 Scope 6
2 References 6
3 Definitions of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7
4 Overview 7
5 Security requirements 7
5.1 General security requirements 7
5.1.1 Authentication and authorization 8
5.1.2 Interface security 8
5.1.3 User consent requirements 8
5.1.4 Secure retrieval of 5G system UE Ids requirements 9
6 Procedures 9
6.1 Security for the EDGE interfaces 9
6.2 Authentication and authorization between EEC and ECS 9
6.3 Authentication and authorization between EEC and EES 10
6.4 Authentication and authorization between EES and ECS 11
6.4.1 General 11
6.4.2 Procedure for the authentication and authorization between EES and ECS 11
6.5 Authentication and authorization in EES capability exposure 11
6.6 Authentication and Authorization between EESs 11
6.7 Authentication and authorization between V-ECS and H-ECS 11
6.8 Authentication and Authorization between AC and EEC 12
6.9 Authentication and authorization between ECS and ECS-ER and between ECS-ERs 12
Annex A (informative): Mechanisms for secure retrieval of 5G system UE Ids and privacy related information 13
A.1 General 13
A.2 UE ID Token based mechanism 13
A.2.1 Introduction 13
A.2.2 Details 13
A.3 Hash based mechanism 16
A.3.1 Introduction 16
A.3.2 Details 16
A.4 Temporary ID based mechanism 18
A.4.1 Introduction 18
A.4.2 Details 18
A.5 AKMA based mechanism 19
A.5.1 Introduction 19
A.5.2 Details 19
Annex B (informative): Change history 21
History 22

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the security features and mechanisms to support the application architecture for enabling Edge Applications in 5G, i.e. security for the interfaces, procedures for the authentication and authorization between the entities of the application architecture, and procedures for the EES capability exposure.

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 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

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

[4] Void

[5] 3GPP TS 23.558: "Architecture for enabling Edge Applications."

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

[7] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs"

[8] Void

[9] Void

[10] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[11] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[12] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[13] Void

[14] Void

[15] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[16] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[17] IETF RFC 7519: "JSON Web Token (JWT)".

[18] IETF RFC 7515: "JSON Web Signature (JWS)".

[19] IETF RFC 9113: "HTTP/2".

[20] IETF RFC 9110: "HTTP Semantics".

[21] 3GPP TS 23.502: "Procedures for the 5G System".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

4 Overview

The overall application architecture for enabling Edge Applications that is given in TS 23.558 [5], includes several entities, such as 3GPP core network, Edge Enabler Client (EEC) deployed in the UE, Edge Configuration Server (ECS), Edge Enabler Server (EES), and Edge Application Server (EAS). The application architecture for enabling Edge Applications, is defined in TS 23.558 [2] clause 6.2.

This specification captures the following security requirements and procedures:

- Security for the EDGE interfaces: the set of security features that enable network nodes to exchange signalling data and user plane data securely.
- Authentication and Authorization between EEC and ECS/EES: the set of security features that enable the authentication between EEC and ECS/EES, and enable the EEC to be authorized by the ECS/EES.
- Authentication and Authorization between EES and ECS: the set of security features that enable the authentication between EES and ECS, and enable the EES to be authorized by the ECS.
- Authentication and Authorization in EES capability exposure: the set of security features that enable the EAS to be authenticated and authorized by the EES in EES capability exposure.
- Authentication and Authorization in 3GPP Core Network capability exposure: the set of security features that enable the ECS/EES/EAS to be authenticated and authorized by the 3GPP Core Network in 3GPP Core Network capability exposure.

5 Security requirements

5.1 General security requirements

The Edge application architecture defined in the TS 23.558 [5] shall satisfy the following requirements.

5.1.1 Authentication and authorization

Authentication and Authorization between Edge Enabler Client (EEC) and Edge Configuration Server (ECS): Edge Configuration Server (ECS) shall be able to provide mutual authentication with Edge Enabler Client (EEC) over EDGE-4 Interface. ECS shall determine whether EEC is authorized to access ECS's services.

Authentication and Authorization between EEC and EES: Edge Enabler Server (EES) shall provide mutual authentication with EEC over EDGE-1 Interface. EES shall determine whether EEC is authorized to access EES's services.

Authentication and Authorization between Edge Enabler Server (EES) and ECS: ECS shall provide mutual authentication with EES over EDGE-6 Interface. ECS shall determine whether EES is authorized to access ECS's services.

Authentication and Authorization between EESs: EES shall provide mutual authentication with another EES over EDGE-9 Interface. EES shall determine whether peer EES is authorized to access EES's services.

Authentication and Authorization in EES capability exposure to EAS: EES shall provide mutual authentication with EAS over EDGE-3 Interface. EES shall determine whether EAS is authorized to access EES's services and expose EEC Capabilities. The Edge application architecture shall support EASs to obtain the user's authorization to access sensitive information (e.g. user's location).

NOTE1: The corresponding security requirements defined in TS 23.558 [5] is AR-5.2.6.2-a/b/d/e/f/g.

Authentication and Authorization between Application Client (AC) and EEC: EEC should provide mutual authentication with the Application Client over EDGE-5 interface, and the EEC should determine whether Application client is authorized to access EEC's service.

Authentication and Authorization between V-ECS and H-ECS: V-ECS shall provide mutual authentication with H-ECS over EDGE-10 Interface. V-ECS shall determine whether H-ECS is authorized to access V-ECS's services.

Authentication and Authorization between ECS and ECS-ER: ECS-ER shall provide mutual authentication with ECS over EDGE-10 interface. ECS-ER shall determine whether ECS is authorized to access ECS-ER's services.

Authentication and Authorization between ECS-ERs: ECS-ERs shall provide mutual authentication over EDGE-10 interface. ECS-ER shall determine whether other ECS-ERs are authorized to access ECS-ER's services.

5.1.2 Interface security

Confidentiality, integrity, and replay protection shall be supported on the EDGE-1-4 and EDGE 6-10 interfaces.

NOTE 1: The interfaces are defined in the Figure 6.2.4 of TS 23.558 [5]. The corresponding security requirement defined in TS 23.558 [5] is AR-5.2.6.2-c.

NOTE 2: The security requirement of EDGE 5 is out of the scope of this specification, since its details are out of the scope of this release of this specification, according to TS 23.558 [5].

The privacy requirements AR-5.2.6.2-h defined in TS 23.558 [5] are implicitly supported, since all the interfaces will be confidentiality and integrity protected.

5.1.3 User consent requirements

User consent for edge computing shall comply with TS 33.501 [3] (Annex V).

If EES, trusted by the 3GPP Core Network, is utilizing 5GC services without NEF, the EES acts as the consent enforcing entity. Otherwise, if the EES is utilizing 5GC services via NEF, the NEF acts as the consent enforcing entity.

User consent architecture in the present document is only applicable when EES or NEF and data provider are operated by the same entity.

5.1.4 Secure retrieval of 5G system UE Ids requirements

- The non-permanent information used in Nnef_UEId API call invocation and Eees_UEIdentifier API call invocation should prevent the use of permanent subject to be abused/compromised by malicious applications.
- The entity responsible for the generation of the non-permanent information should be part of the 5G system in HPLMN and should be verified by the 5G system in HPLMN. Alternatively, the non-permanent information can be generated by both the UE and the 5G system.
- The non-permanent information can be used by the AF invoking the NEF APIs, so that the NEF APIs can identify the UE by using the non-permanent information.
- The non-permanent information can be used by the EAS/EEC invoking the Eees_UEIdentifier API, so that the EES APIs can identify the UE by using the non-permanent information.

NOTE 1: The API invoker does not need to obtain the permanent 5G UE ID, which improves the privacy.

NOTE 2: The principles above do not prevent usage of existing mechanisms of Nnef_UEId API and UE Identifier API.

Example implementation specific mechanisms having the design principles above are captured in an informative Annex A of the present document.

6 Procedures

6.1 Security for the EDGE interfaces

For the interfaces (EDGE-1/4), the EEC, EES and ECS shall support and use HTTP/2 with "https" URIs as specified in RFC 9113 [19] and RFC 9110 [20]. In addition, the TLS profile shall be compliant with the profile given in clause 6.2 of TS 33.210 [2] .

For the interfaces EDGE-2/7/8,

- If the NEF APIs are selected, security aspects of Network Exposure Function including the protection of NEF-AF interface and support of CAPIF defined in TS 33.501 clause 12 [2] shall be reused, i.e., use of TLS.
- If the SCEF APIs are selected, the Security procedures for reference point SCEF-SCS/AS defined in TS 33.187 clause 5.5 [3] can be reused here, i.e., use of TLS.

For the interfaces (EDGE-3/6/9/10), the EAS, EES, ECS, and ECS-ER shall support and use HTTP/2 with "https" URIs as specified in RFC 9113 [19] and RFC 9110 [20]. In addition, the TLS profile shall be compliant with the profile given in clause 6.2 of TS 33.210 [2] .

6.2 Authentication and authorization between EEC and ECS

The ECS shall be configured with the information of authorization methods (token-based authorization or local authorization) used by EESes.

Authentication between EEC and ECS shall be done during the execution of the TLS handshake protocol. Server side certificate-based TLS authentication shall be supported. A mutual authentication method should be supported and used between EEC and ECS (e.g., TLS certificates (client and server certificate based authentication), usage of AKMA [11] or GBA [12] as methods to arrange the PSK for TLS). Details of such authentication method performed during the execution of the TLS handshake protocol are out of scope of the present document.

NOTE 1: Usage of application layer solutions for EEC authentication is left to implementation.

NOTE 2: If only server side certificate-based TLS authentication is performed, it is left to implementation on which information within a service procedure and services will be provided by the ECS.

The authentication method negotiation mechanism shall re-use the existing TLS v1.3 negotiation. UE may receive the supported authentication method of the ECS optionally as part of the ECS configuration information. Details of the ECS

configuration information are specified in TS 23.558 [5]. If the UE has the information about the authentication method supported by the ECS, then the EEC/UE may use this information for the authentication method negotiation.

NOTE 3: Further optimization regarding having prior knowledge about the capability, such as UE storing the selected algorithm from the past negotiation results, is left to EEC/UE implementation. Authentication method received in the ECS configuration information takes precedence. If more than one authentication methods are included in the ECS configuration information, then it is up to the UE implementation to select an authentication method.

If the GPSI is required, the ECS shall retrieve the GPSI from the core network no matter whether the EEC sends the GPSI to the ECS.

NOTE 4: If the ECS identifies a mismatch between the GPSI received from the EEC and the GPSI received from the network, the decision and action to be taken by the ECS for such mismatch cases are left to implementation.After successful authentication, the ECS shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the ECS decides whether OAuth 2.0 [15] access tokens are required for the candidate EESes using the configuration information and issues separate EES access tokens to be used for each candidate EESes that use token-based authorization. The ECS, EEC and EES respectively assume the role of authorization server, client and resource server roles defined in [15]. "Client Credentials" grant type and bearer tokens [16] shall be used. JSON Web Token (JWT) as specified in IETF RFC 7519 [17] for encoding and the JSON signature profile as specified in IETF RFC 7515 [18] for protection of tokens shall be followed. This token profile also applies for clause 6.3 of the present document. The claims of the EES service tokens in the form of JWT [17] shall include the ECS FQDN (issuer), EEC ID (client_id), GPSI (subject), expected EES service name(s) (scope), EES FQDN (audience), expiration time (expiration). The ECS shall send the service response back to the EEC, which may include EES access token(s).

6.3 Authentication and authorization between EEC and EES

Authentication between EEC and EES shall be done during the execution of the TLS handshake protocol. Server side certificate-based TLS authentication shall be supported. Details of the authentication method (e.g., TLS certificates, usage of AKMA [11] or GBA [12] as methods to arrange the PSK for TLS) are out of scope of the present document.

NOTE 1: Usage of application layer solutions for EEC authentication is left to implementation.

NOTE 2: If only server side certificate-based TLS authentication is performed, it is left to implementation on which information within a service procedure and services will be provided by the EES.

The authentication method negotiation mechanism shall re-use the existing TLS v1.3 negotiation. UE may receive the supported authentication method of the EES optionally as part of the EES configuration information. Details of the EES configuration information are specified in TS 23.558 [5]. If the UE has the information about the authentication method supported by the EES, then the EEC/UE may use this information for the authentication method negotiation.

NOTE 3: Further optimization regarding having prior knowledge about the capability, such as UE storing the selected algorithm from the past negotiation results, is left to EEC/UE implementation.

If the GPSI is required, the EES shall retrieve the GPSI from the core network no matter whether the EEC sends the GPSI to the ECS.

NOTE 4: If the EES identifies a mismatch between the GPSI received from the EEC and the GPSI received from the network, the decision and action to be taken by the EES for such mismatch cases are left to implementation.

For authorization of EEC by the EES, the EEC shall send the OAuth 2.0 [15] access token, if received from the ECS, to the EES. The token profile is specified in clause 6.2 of the present document. If the EES requires access token for authorization, then the EES shall authorize the EEC by using the token. Otherwise, the EES shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the EES shall process the request and sends the service response back to the EEC.

6.4 Authentication and authorization between EES and ECS

6.4.1 General

The detailed service procedures between EES and ECS are described in TS 23.558 [5].

6.4.2 Procedure for the authentication and authorization between EES and ECS

Pre-requisite:

- EES obtains onboarding information within the same PLMN domain or from a third-party domain. The information includes the Edge Configuration Server Address and Root CA certificate details, it may include an enrolment token.

NOTE1: The provisioning and usage of the onboarding information are out of the scope of this document.

- The EES and ECS are provisioned with credentials for the mutual authenticated TLS.

TLS shall be used to provide integrity protection, replay protection, and confidentiality protection for the interface between the EES and the ECS.

Security profiles for TLS implementation and usage shall follow the profiles given in clause 6.2 of TS 33.210 [2] . The certificates shall follow the profile given in clause 6.1.3a of TS 33.310 [10]. The identities in the end-entity certificates shall be used for authentication and policy checks. Identities in the end-entity certificate shall be based on endpoint information (e.g., URI, FQDN, IP address) as described in the TS 23.558 [5].

The ECS shall authorize the EES based on local authorization policy.

6.5 Authentication and authorization in EES capability exposure

According to clause 8.7.3 of TS 23.558 [5], the EES may re-expose the network capabilities of the 3GPP core network to the EAS(s) as per the CAPIF architecture specified in TS 23.222 [6]. If the CAPIF architecture is used, the CAPIF functional security model specified in TS 33.122 [7] shall be used for Authentication and authorization in EES capability exposure.

If CAPIF is not used, mutual authentication with TLS certificates using TLS shall be used. The TLS and certificates shall follow the profiles defined in TS 33.210 [2] and TS 33.310 [10], and the authorization is based on local authorization policy at the EES.

NOTE: Void

6.6 Authentication and Authorization between EESs

As specified in clause 6.1, TLS is used for EDGE-9 reference point (between edge enabler servers) security. For authentication between EESs, X.509 certificates shall be used. The certificates shall follow the profile given in clause 6.1.3a of TS 33.310 [10]. The identities in the end-entity certificates shall be used for authentication and policy checks. Identities in the end-entity certificate shall be based on endpoint information (e.g., URI, FQDN, IP address) as described in TS 23.558 [5].

Authorization between EESs is based on local authorization policy.

6.7 Authentication and authorization between V-ECS and H-ECS

The V-ECS and H-ECS are provisioned with credentials (e.g., certificate, shared keys/secrets) for mutual authentication. The mutual authentication between V-ECS and H-ECS shall be done based on the preconfigured credentials. The V-ECS shall authorize the H-ECS based on local authorization policy.

6.8 Authentication and Authorization between AC and EEC

Authentication and authorization between AC and EEC in UE are based on local policy.

NOTE 1: Security mechanisms for authentication and authorization between AC and EEC in UE are left to implementation.

6.9 Authentication and authorization between ECS and ECS-ER and between ECS-ERs

Same mechanism in clause 6.7 applies for authentication and authorization between ECS and ECS-ER and between ECS-ERs.

Annex A (informative): Mechanisms for secure retrieval of 5G system UE Ids and privacy related information

A.1 General

This clause describes the alternative mechanisms aligning with the principles that described in the Clause 5.1.4 of the present document, i.e., UE ID Token based mechanism, Hash based mechanism, Temporary ID based mechanism, and AKMA based mechanism.

These principles can be addressed by solutions having the main steps:

- The network provides a non-permanent information (e.g., temporary UE ID, a UE ID Token, Hash, etc.) to the UE if required.
- The UE presents this non-permanent information to the AF.
- The AF sends a request towards the network using the non-permanent information.
- The network executes the request for the corresponding UE associated to the received non-permanent information.

The present clause gives examples of possible procedures/mechanisms that could realize the principles/steps defined above. Described examples are not standardized in the present document and their realization requires implementation specific means.

A.2 UE ID Token based mechanism

A.2.1 Introduction

According to the mechanism, a new entity called UE ID Server located inside the operator domain provides a separate UE ID Token to the Client running on the UE for each request coming from the Client. The Client interacts with the AF by using the UE ID Token and then the AF interacts with network by using the received UE ID Token. The network resolves the UE ID Token by interacting with the UE ID Server to identify the UE. The UE ID Server and the interactions with the UE ID Server can be realized by implementation specific means.

A.2.2 Details

Generic representation of the mechanism is presented in Figure A.1.2-1.

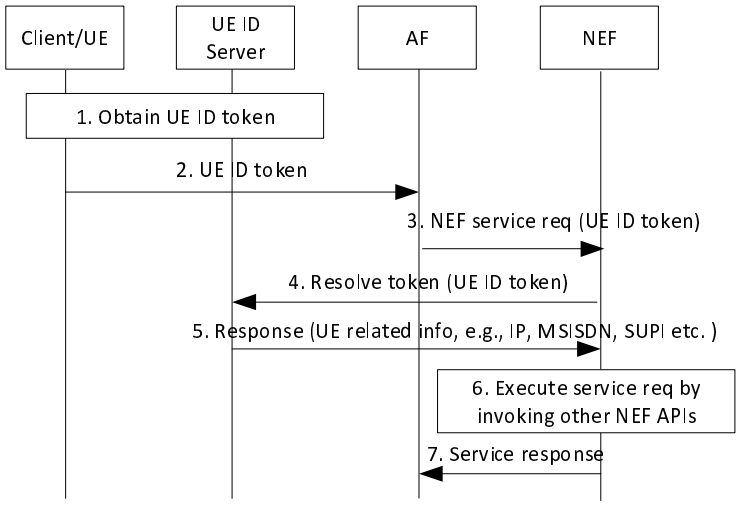

Figure A.2.2-1: Generic view of UE ID token based mechanism

Step 1: The client obtains a UE ID token from the UE ID server which is located inside the operator domain. UE ID server can identify the UE by using the private IP address of the PDU session. The UE ID Server can fetch the IP address from the IP packets received from the Client. The UE ID Server as a trusted AF can use the Nbsf_Management_Discovery service operation with UE address and IP domain to retrieve the session binding information of the UE. For the UE ID Server service consumption by the client, the UE where the client is running on needs to execute the primary authentication successfully and have a PDU session. The client can authenticate the UE ID Server by using server certificate. The Client needs to be configured with the root certificate or certificate of the UE ID Server, or the Internet (public) PKI mechanism can be used. The client does not need to authenticate with the server since the server issues the UE ID token, which does not include cleartext sensitive information, to the client running on the UE who has already executed the primary authentication.

NOTE 1: Since the issuer and resolver of the UE ID token is the UE ID Server, the details of the UE ID token (e.g., whether it is a signed token or a random number) can be left to implementation.

Step 2: The client forwards the token to the AF.

Step 3: The AF invokes a NEF service and use the UE ID token as UE identifier.

NOTE 2: The UE ID token can be provided as input in any NEF Service that takes GPSI as input (as NAI/External Id format).

Step 4: The NEF interacts with the UE ID server to resolve the UE ID token into UE information (e.g., private IP address, MSISDN, SUPI) needed for the operation.

Step 5: The UE ID server returns the requested information.

Step 6: The NEF interacts with other NFs as per existing NEF service procedures as per TS 23.502.

Step 7: The NEF returns the result of the NEF service execution.

Note that if the AF is a trusted AF, it can directly interact with the UE ID Server to identify the UE and the obtain required information such as IP address, and then invoke the NF/NEF directly with the required inputs.

Application of the mechanism to the case of NEF API invocation by the EAS/EES is presented in Figure 6.9.2-2.

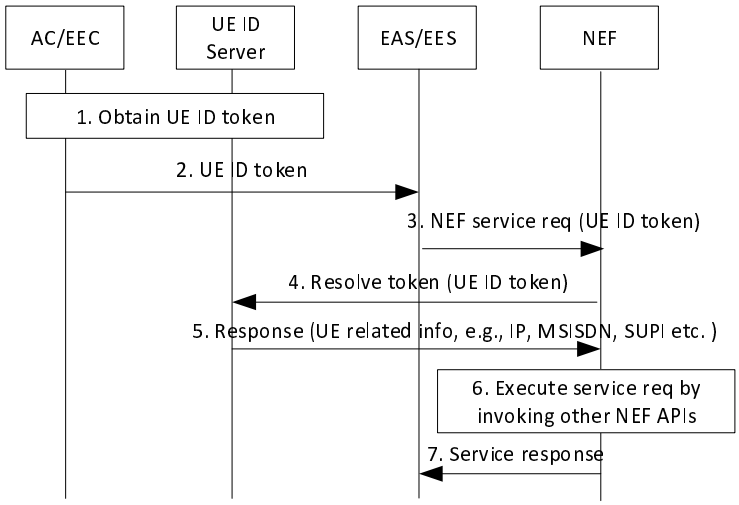

Figure A.2.2-2: The EAS/EES invokes NEF API

Step 1: The AC/EEC obtains a UE ID token from the UE ID server.

Step 2: The AC or the EEC respectively forward the token to the EAS or the EES.

Step 3: The EAS/EES invokes a NEF service and use the UE ID token as UE identifier.

Step 4: The NEF interacts with the UE ID server to resolve the UE ID token into UE information (e.g., private IP address, MSISDN, SUPI) needed for the operation.

Step 5: The UE ID server returns the requested information.

Step 6: The NEF interacts with other NFs as per existing NEF service procedures as per TS 23.502.

Step 7: The NEF returns the result of the NEF service execution.

Application of the mechanism to the case of EES API invocation by the EAS is presented in Figure 6.9.2-3.

NOTE 3: The invocation to existing APIs in step 3 and 4 by this mechanism in the following figure is left to implementation.

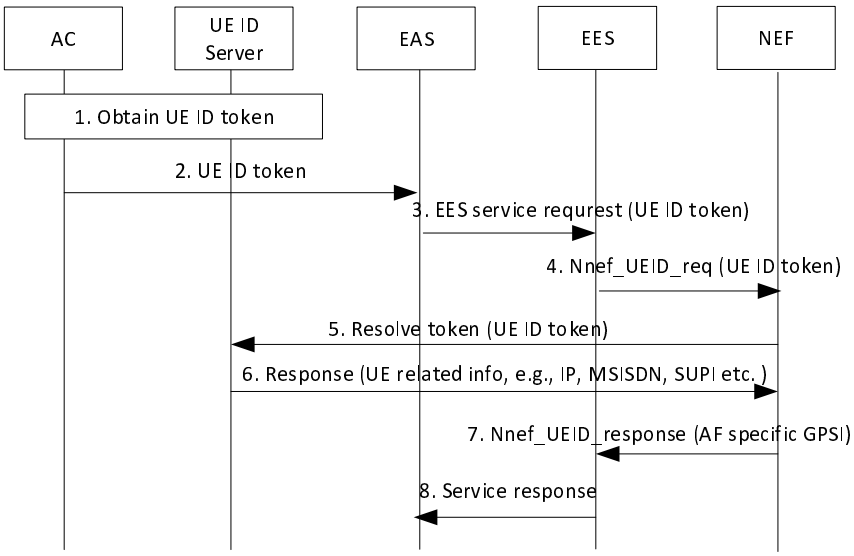

Figure A.2.2-3: The EAS invokes the EES API

Step 1: The AC obtains a UE ID token from the UE ID server.

Step 2: The AC forwards the token to the EAS.

Step 3: The EAS invokes a EES service and use the UE ID token as UE identifier.

Step 4: The EES invokes the NEF API by sending the UE ID token.

Step 5: The NEF interacts with the UE ID server to resolve the UE ID token into UE information (e.g., private IP address, MSISDN, SUPI) needed for the operation.

Step 6: The UE ID server returns the requested information.

Step 7: The NEF sends the UE ID to the EES.

Step 8: The EES returns the result of the EES service execution.

A.3 Hash based mechanism

A.3.1 Introduction

This mechanism proposes to use fresh hash value with count, which is a fresh value shared between the UE and the 5GC, to authorize the AF to retrieve the UE ID. This solution addresses the principles in clause 5.1.4. if the NAT is not deployed after the UPF.

A.3.2 Details

This mechanism supports the 5GC in implementation specific way to verify whether the AF is authorized by the UE to retrieve the UE ID based on the IP address, and verify whether the parameters used for verification is replayed by the adversary. Specifically, when the UE receives the UE ID request, it in implementation specific way generates a hash value based on the count, salt, SUPI and IP address, and then sends the generated hash value and count to the AF, which uses the IP address to request for the UE ID from the NEF. The NEF then requests BSF to provide information of the UE (i.e., SUPI). Before providing the SUPI of UE, the BSF in implementation specific way also generates a hash' based on the shared count, salt, SUPI and IP address, and then compare the hash' value with the received hash value. If the hash value is equal to the hash' value, the BSF can provide the SUPI to the NEF. Otherwise, the BSF will provide a failure indication to the NEF.

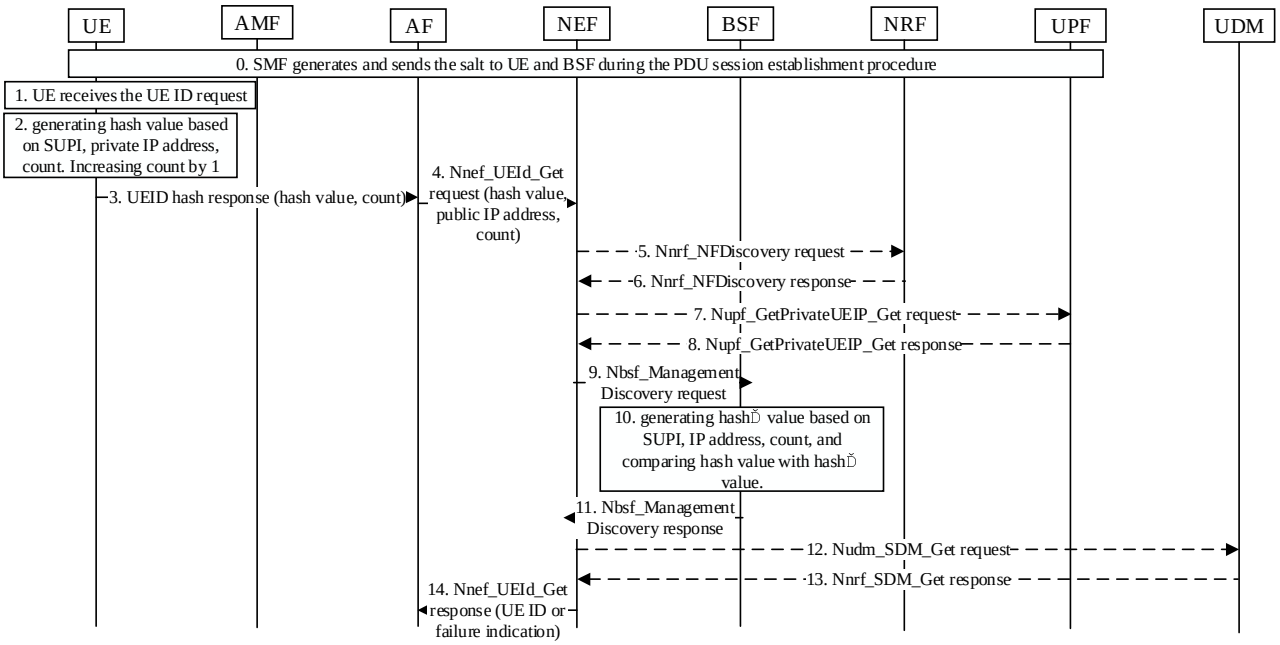

Figure A.3.2-1: Authorization of AF and verification of AF provided IP address

0. During the PDU session establishment procedure, SMF generates the salt, which is a random value, and then sends the salt to both UE and BSF in an implementation specific way. SMF can send the salt to the BSF along with SM policy Association Establishment or SM policy Association Modification message in clauses 4.16.4 or 4.16.5 of TS 23.502 [8]. If the SM policy Association Establishment and SM policy Association Modification procedures are not performed, SMF will not send the salt to the UE.

1. UE receives the UE ID request.

2. The UE generates a hash value based on the SUPI, private IP address, salt, and count, and other values that is only known to both the EEC and BSF (e.g., DNN of the PDU Session, and S-NSSAI of the PDU Session). After that, the UE increases the count by 1, which is used for the next hash value generation procedure. Note that the count can be configured to start from 0 in each PDU session. In order to mitigate the rainbow table attack, the following mechanisms should be adopted:

    (1) increasing the length of the hash algorithm's input.

The length of the salt can be set as 128bits to make the rainbow table attack infeasible [15].

    (2) key stretching. The inputs can be run through the hash function multiple times to increase the time to build a precomputed rainbow table.

    The UE sends the hash value and the count together to avoid the out-of-synchronization between the UE and BSF.

3. The UE sends the generated hash value and count to the AF.

4. The AF in an implementation specific way invokes the Nnef_UEId_Get request with the parameter of hash value, count, and public IP address to get the UE ID.

5-8. This mechanism reuses Steps 3-6 in Clause 4.15.10, TS 23.502 [8].

9. When the NEF invokes the Nbsf_Management_Discovery service operation, the NEF in an implementation specific way provides the hash value and private IP address to the BSF.

10. In an implementation specific way, the BSF determines the SUPI, salt and count based on the private IP address and then generates the hash' value, and then compares the hash' value with the received hash value.

11. If the hash' value is equal to the received hash value, the BSF in an implementation specific way will respond to the NEF with a SUPI. Otherwise, the BSF in an implementation specific way will respond to the NEF with an indication that request is denied with the reason that the private IP address is not associated with the UE.

12-14. This mechanism reuse Steps 9-11 in Clause 4.15.10, TS 23.502 [8].

A.4 Temporary ID based mechanism

A.4.1 Introduction

This mechanism proposes to use temporary ID to addresses the security requirements illustrated in clause 5.4.1.

The main design principle of the mechanism is based on the utilization of a temporary identifier (ID) as UE identity to fetch the Application Function (AF) specific UE Id from Nnef_UEId service. The temporary ID is generated by the 5G Core, such as UDM (this is left to implementation), it includes a randomly generated value, and it is for example associated to the PDU session.

A.4.2 Details

Figure A.3.2-1 illustrates the procedure to fetch the 5G system UE Id and privacy related information.

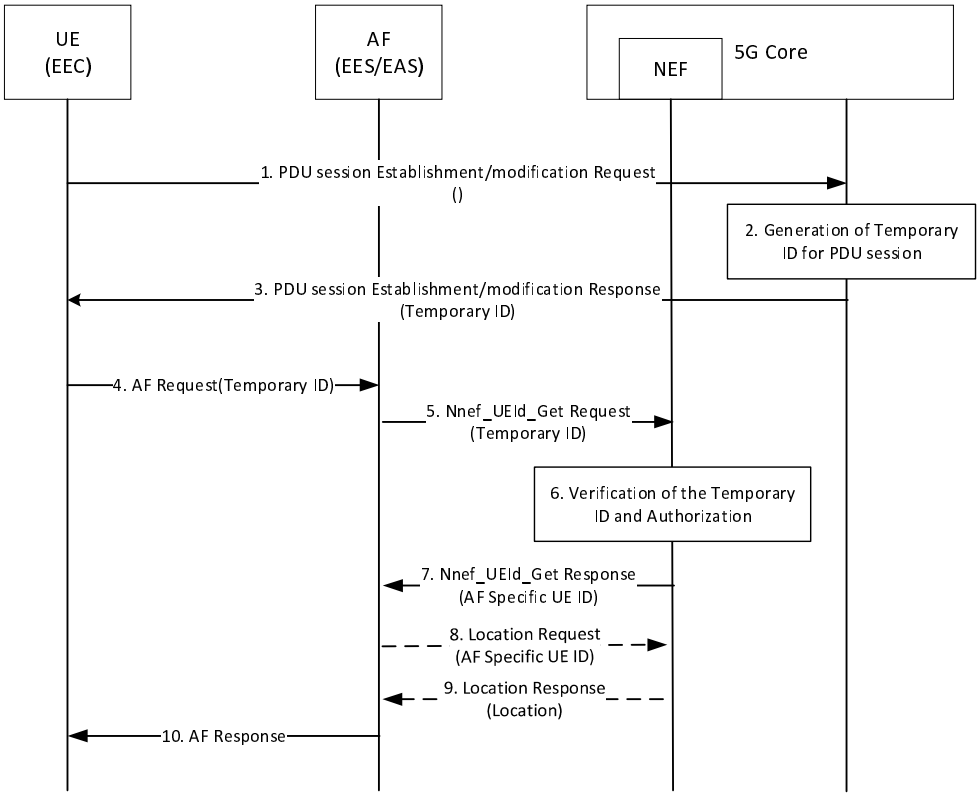

Figure A.4.2-1: Procedure to fetch the 5G system UE Id and privacy related information

Precondition:

0. The EEC requests a Temporary ID to UE through interface provided by UE module.

1. PDU session establishment / modification request is sent from the UE to the 5G system.

2. The 5G Core generates (per UE) an internal temporary ID (with a randomly generated part) for PDU session.

NOTE 1: The concrete network entity in 5G Core responsible for generating the internal temporary ID is to be decided by the implementation.

NOTE 2: The UE could request multiple temporary IDs during the same PDU session (PDU Session modification). The UE can use this to invalidate previous IDs which might have been compromised and/or at fix intervals without initializing another PDU session establishment/modification.

3. The 5G Core returns the internal temporary ID to the UE as part of the NAS PDU session establishment/modification response.

4. The EEC uses the allocated temporary ID, received from the UE, inside the Edge application layer communication with the application function AF (e.g., EAS).

5. The AF uses the received temporary ID to invoke the Nnef_UEId API intended to fetch the 5G system UE identifier.

6. The NEF verifies the temporary ID, authorizes the request coming from the AF and accordingly retrieves from the 5G Core the AF specific UE Id corresponding to the temporary ID.

7. The NEF replies to the AF with the corresponding AF specific UE Id.

8-9 (Optional). Assuming the application logic requires to fetch the UE location, a location request is sent to the NEF using the AF specific UE Id, and the corresponding information is provided by the 5G system through the NEF.

10. The AF responds to the UE (EEC).

A.5 AKMA based mechanism

A.5.1 Introduction

The main design principle of the solution is based on AKMA feature, more specifically on the A-KID, an application specific ID derived from the long term symmetric pre-shared key K between the UE and the network. The EDGE application server (EAS) and/or enabler server (EES), use the AKMA protocol to retrieve the 5G UE privacy related information.

The solution assumes that AF (EES/EAS) communicates with 5GC through NEF.

A.5.2 Details

Figure A.4.2-1 illustrates the procedure to fetch the 5G system UE privay related information based on AKMA.

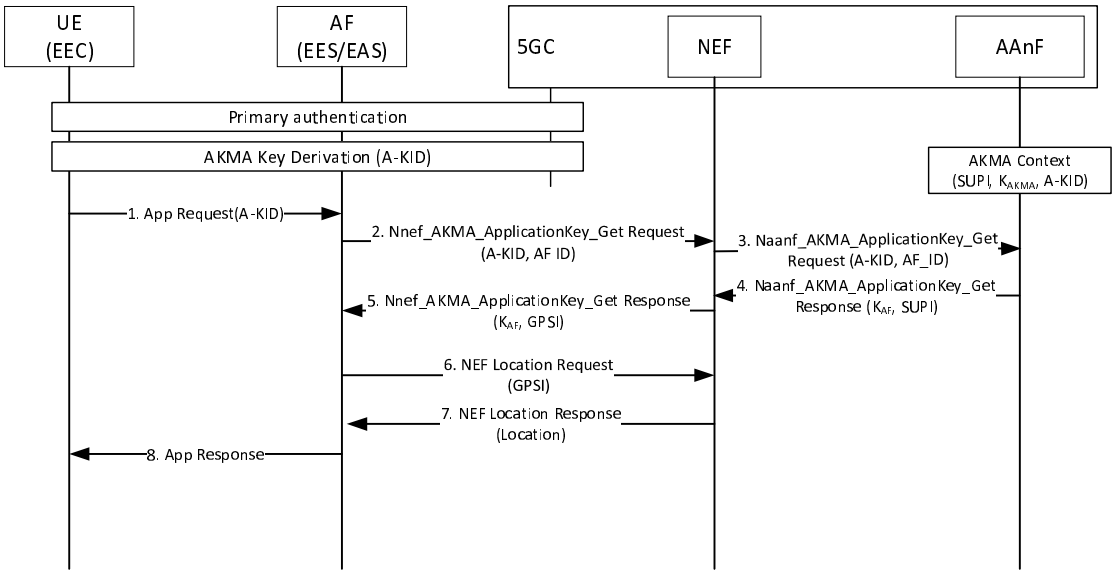

Figure *A*.5.2-1: Procedure to fetch the 5G system UE privacy information based on AKMA

Preliminary steps:

- Primary authentication
- AKMA Key derivation (A-KID) as per procedure in TS 33.535 [11].
- Creation of AKMA context in AAnF (SUPI, K_{AKMA}, A-KID) as per procedure in [11].

Step 1. The application client in the UE (EEC) requests a service to the AF, i.e., EDGE application server (EAS, EES), including the A-KID (AKMA Key Identifier) in the request.

Step 2-5. AKMA procedure intended to provide K_{AF} to the AF from the AAnF via NEF as specified in clause 6.3 of [11].

NOTE 1: AF specific UE Id does not need to be part of the of the incoming request (step 2), since the NEF will provide the GPSI (external ID) to AF.

Step 6. The AF requires to know privacy information of the UE available in the 5G Core, such as the the location of UE, and makes the request to the 5G Core via NEF, using the given GPSI as UE identifier.

Step 7. The NEF checks the GPSI and if the request is authorized, the corresponding information, in this example location of the UE, is provided to the AF.

Step 8. The AF responds to the UE (EEC).

NOTE 2: Special consideration can be needed for the point that the same A-KID will be used until the next execution of the primary authentication, and it will be same for all the AFs.

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-03	SA#95e	SP-220189				Presented for information and approval	1.0.0
2022-03	SA#95e					Upgrade to change control version	17.0.0
2022-06	SA#96	SP-220558	0001	2	F	Editorial corrections and technical clarifications	17.1.0
2022-06	SA#96	SP-220558	0002	1	F	Clarification of access token usage in EC	17.1.0
2022-09	SA#97e	SP-220879	0006	-	F	Corrections and clarifications on the usage of HTTPS and X.509 certificates	17.2.0
2022-12	SA#98e	SP-221158	0008	-	F	Addressing authentication and authorization for EDGE-9	17.3.0
2023-09	SA#101	SP-230885	0015	1	B	Authentication and authorization between Edge Entities	18.0.0
2023-10						Correction of CR implementation	18.0.1
2023-12	SA#102	SP-231328	0017	1	F	Clarification on EDGE-10 interface to cover the ECS-ER security	18.1.0
2024-07	SA#104	SP-240661	0018	1	F	Clarification on the authentication method(s) between EEC and ECS	18.2.0
2025-03	SA#107	SP-250106	0021		B	CR on skeleton for TS 33.558 on ID verification	18.3.0
2025-03	SA#107					Upgrade to change control version	19.0.0

History

Document history		
V19.0.0	January 2026	Publication