ETSI TS 123 434 V17.6.0 (2022-07)

TECHNICAL SPECIFICATION

5G;
Service Enabler Architecture Layer for Verticals (SEAL);
Functional architecture and information flows
(3GPP TS 23.434 version 17.6.0 Release 17)

Reference

RTS/TSGS-0623434vh60

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or
print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any
existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI
deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of
experience to understand and interpret its content in accordance with generally accepted engineering or
other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law
and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness
for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not
limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property
rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages
for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use
of or inability to use the software.

Copyright Notification

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 under http://webapp.etsi.org/key/queryform.asp.

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

This document specifies a functional architecture for service enabler architecture layer (SEAL) over 3GPP networks to support vertical applications (e.g. V2X applications). This functional architecture will include common application plane and signalling plane entities. A set of common services (e.g. group management, configuration management, location management) specified in this document can be shared across vertical applications.

The SEAL functional architecture takes into consideration the common capabilities to support mission critical and other vertical applications.

1 Scope

The present document specifies the functional architecture for service enabler architecture layer (SEAL) and the procedures, information flows and APIs for each service within SEAL in order to support vertical applications over the 3GPP system. The present document is applicable to vertical applications using E-UTRAN or NR access based on the EPC or 5GS architecture defined in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10]. To ensure efficient use and deployment of vertical applications over 3GPP systems this specification for SEAL services includes the group management, configuration management, location management, identity management, key management and network resource management.

NOTE: In the present document, the multicast services offered by SEAL are only applicable for EPS.

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 22.104: "Service requirements for cyber-physical control applications in vertical domains".

[3]   3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[4]   3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[5]   3GPP TS 23.281: "Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2".

[6]   3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2".

[7]   3GPP TS 23.286: "Application layer support for V2X services; Functional architecture and information flows".

[8]   3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[9]   3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[10]   3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[11]   3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[12]   3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[13]   3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[14]   3GPP TS 23.002: "Network Architecture".

[15]   3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[16]   3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[17]   3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[18]   3GPP TS 23.203: "Policy and charging control architecture".

[19]   3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[20]   3GPP TS 26.348: "Northbound Application Programming Interface (API) for Multimedia Broadcast/Multicast Service (MBMS) at the xMB reference point".

[21]   3GPP TS 29.214: "Policy and charging control over Rx reference point".

[22]   3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".

[23]   3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[24]   IETF RFC 6733 (October 2012): "Diameter Base Protocol".

[25]   ETSI TS 102 894-2 (V1.2.1): "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionaryMultimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[26]   ETSI TS 102 965 (V1.4.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

[27]   ISO TS 17419: "Intelligent Transport Systems - Cooperative systems - Classification and management of ITS applications in a global context".

[28]   3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[29]   3GPP TS 33.434: "Service Enabler Architecture Layer (SEAL); Security aspects for Verticals".

[30]   3GPP TS 29.549: "Service Enabler Architecture Layer for Verticals (SEAL); Application Programming Interface (API) specification; Stage3".

[31]   3GPP TS 23.285: "Architecture enhancements for V2X services".

[32]   IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[33]   IETF RFC 8323: "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets".

[34]   3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[35]   IEEE Std 802.1Qcc-2018: "Standard for Local and metropolitan area networks - Bridges and Bridged Networks - Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements".

[36]   IEEE 802.1Q-2018: "IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks".

[37]   IEEE Std 802.1CB-2017: "Frame Replication and Elimination for Reliability".

[38]   3GPP TS 23.003: "Numbering, Addressing and Identification".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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].

VAL user: An authorized user, who can use a VAL UE to participate in one or more VAL services.

VAL user ID: A generic name for the user ID of a VAL user within a specific VAL service.

VAL UE: A UE that can be used to participate in one or more VAL services.

VAL client: An entity that provides the client side functionalities corresponding to the vertical applications.

SEAL client: An entity that provides the client side functionalities corresponding to the specific SEAL service.

VAL service: A generic name for any service offered by the VAL service provider to their VAL users.

SEAL service: A generic name for a common service (e.g. group management, configuration management, location management) that can be utilized by multiple vertical applications.

SEAL provider: Provider of SEAL service(s).

VAL server: A generic name for the server application function of a specific VAL service.

SEAL server: An entity that provides the server side functionalities corresponding to the specific SEAL service.

VAL system: The collection of applications, services, and enabling capabilities required to support a VAL service.

Primary VAL system: VAL system where the VAL user profiles of a VAL user are defined.

Partner VAL system: A VAL system that has a business relationship with the primary VAL system such that service can be offered to primary VAL system users.

VAL group: A defined set of VAL UEs or VAL users configured for specific purpose in a VAL service.

   NOTE: The set could be of either VAL UEs or VAL users depending on the specific VAL service.

VAL group home system: The VAL system where the VAL group is defined.

VAL group member: A VAL service user, whose VAL user ID is listed in a particular VAL group.

VAL stream: A time sensitive communication stream is used to transport a time sensitive data flow, and is defined by a stream specification (which identifies a source and destination of the data flow) and a traffic specification (which defines the characteristics of the data flow). VAL stream is identified by a VAL stream ID.

Vertical: See vertical domain.

Vertical application: An application catering to a specific vertical.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.104 [2] apply:

   Vertical domain

3.2 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].

5GS	5G System
5GVN	5G Virtual Network
CAPIF	Common API Framework for northbound APIs
CNC	Centralized Network Configuration
CRUDN	Create, Retrieve, Update, Delete and Notify
EPC	Evolved Packet Core
GPSI	Generic Public Subscription Identifier
LWP	Light-weight Protocol
NEF	Network Exposure Function
NR	New Radio
PCC	Policy and Charging Control
SCEF	Service Capability Exposure Function
SEAL	Service Enabler Architecture Layer for Verticals
TSC	Time Sensitive Communication
TSN	Time Sensitive Networking
VAL	Vertical Application Layer

4 Architectural requirements

4.1 General

4.1.1 Description

This subclause specifies the general requirements for SEAL.

4.1.2 Requirements

[AR-4.1.2-a] The SEAL shall support applications from one or more verticals.

[AR-4.1.2-b] The SEAL shall support multiple applications from the same vertical.

[AR-4.1.2-c] The SEAL shall offer SEAL services as APIs to the vertical applications.

[AR-4.1.2-d] The SEAL shall support notification mechanism for SEAL service events.

[AR-4.1.2-e] The API interactions between the vertical application server(s) and SEAL server(s) shall conform to CAPIF as specified in 3GPP TS 23.222 [8].

[AR-4.1.2-f] The SEAL server(s) shall provide a service API compliant with CAPIF as specified in 3GPP TS 23.222 [8].

4.2 Deployment models

4.2.1 Description

This subclause specifies the requirements for various deployment models.

4.2.2 Requirements

[AR-4.2.2-a] The SEAL shall support deployments in which SEAL services are deployed only within PLMN network.

[AR-4.2.2-b] The SEAL shall support deployments in which SEAL services are deployed only outside of PLMN network.

[AR-4.2.2-c] The SEAL shall support deployments in which SEAL services are deployed both within and outside the PLMN domain at the same time.

[AR-4.2.2-d] The SEAL shall support SEAL capabilities for centralized deployment of vertical applications.

[AR-4.2.2-e] The SEAL shall support SEAL capabilities for distributed deployment of vertical applications.

4.3 Location management

4.3.1 Description

This subclause specifies the requirements for location management service.

4.3.2 Requirements

[AR-4.3.2-a] The SEAL shall enable sharing location data between client and server for vertical applications usage.

[AR-4.3.2-b] The SEAL shall support different granularity of location data, as required by the vertical application.

[AR-4.3.2-c] The SEAL shall support requests for on-demand location reporting.

[AR-4.3.2-d] The SEAL shall support client location reporting based on triggers.

[AR-4.3.2-e] The SEAL shall enable vertical applications to receive updates to the location information.

[AR-4.3.2-f] The SEAL shall enable sharing the network location information obtained from the 3GPP network systems to the vertical applications.

[AR-4.3.2-g] The SEAL shall provide a mechanism to enable vertical applications to obtain a list of UE(s), and the location information of each UE, in the proximity to a designated/requested location.

4.4 Group management

4.4.1 Description

This subclause specifies the requirements for group management service.

4.4.2 Requirements

[AR-4.4.2-a] The SEAL shall enable group management operations (e.g. CRUDN) by the authorized users or VAL server.

[AR-4.4.2-b] The SEAL shall enable creation of group to be used by one or more vertical applications within the same VAL system.

[AR-4.4.2-c] The SEAL shall enable two or more groups to be merged (temporarily or permanently) into a single group by the authorized users or VAL server wherein all the group members of the constituent groups are designated as members of the merged group.

4.5 Configuration management

4.5.1 Description

This subclause specifies the requirements for configuration management service.

4.5.2   Requirements

[AR-4.5.2-a] The SEAL shall enable configuring service specific configuration data applicable to vertical applications.

[AR-4.5.2-b] The SEAL shall support configuring data applicable to different vertical applications.

4.6   Key management

4.6.1   Description

This subclause specifies the requirements for key management service.

4.6.2   Requirements

[AR-4.6.2-a] The SEAL shall support secure distribution of security related information (e.g. encryption keys).

[AR-4.6.2-b] The SEAL shall support all communications in SEAL ecosystem to be secured.

4.7   Identity management

4.7.1   Description

This subclause specifies the requirements for identity management service.

4.7.2   Requirements

[AR-4.7.2-a] The SEAL shall enable the access to SEAL services from the vertical application layer entities to be authorized.

> Editor's Note: The relationship between identity management service and authorization is FFS.

4.8   Network resource management

4.8.1   Description

This subclause specifies the requirements for network resource management service.

4.8.2   Requirements

[AR-4.8.2-a] The SEAL shall enable support for unicast bearer establishment and modification to support service KPIs for VAL communications.

[AR-4.8.2-b] The SEAL shall enable support for multicast bearer establishment and modification to support service KPIs for VAL communications.

[AR-4.8.2-c] The SEAL shall support announcement of multicast bearers to the UEs.

[AR-4.8.2-d] The SEAL shall support switching of bearers between unicast and multicast.

[AR-4.8.2-e] The SEAL shall support multicast bearer quality detection.

5   Involved business relationships

Figure 5-1 shows the business relationships that exist and that are needed to support a single VAL user.
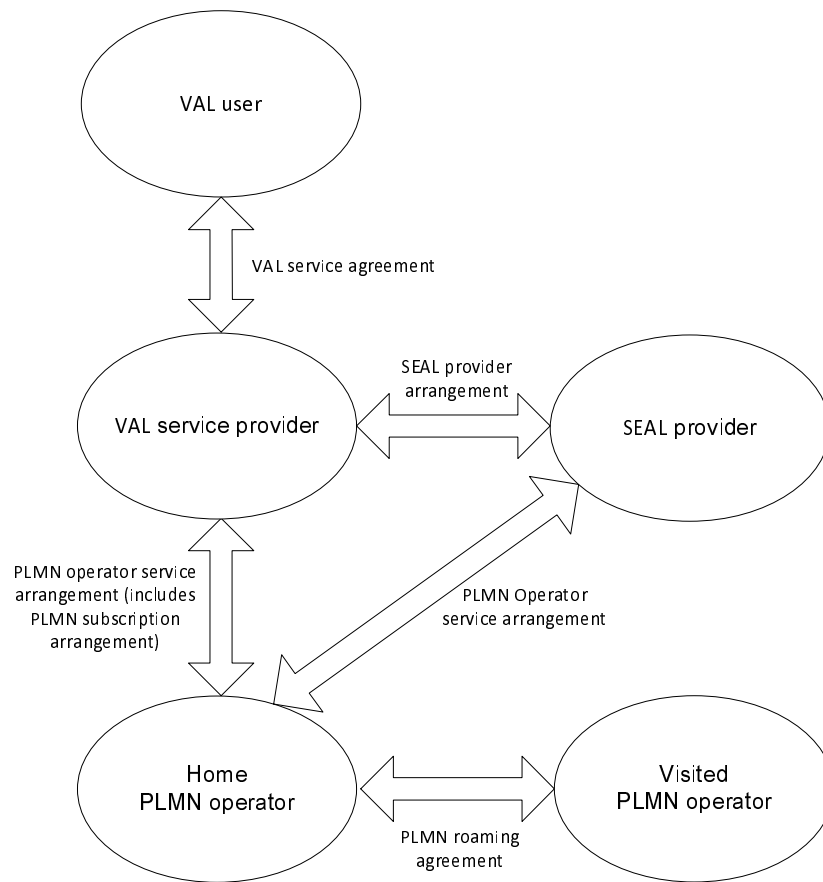
Figure 5-1: Business relationships for VAL services

The VAL user belongs to a VAL service provider based on a VAL service agreement between the VAL user and the VAL service provider. The VAL service provider can have VAL service agreements with several VAL users. The VAL user can have VAL service agreements with several VAL service providers.

The VAL service provider and the home PLMN operator can be part of the same organization, in which case the business relationship between the two is internal to a single organization.

The VAL service provider can have SEAL provider arrangements with multiple SEAL providers and the SEAL provider can have PLMN operator service arrangements with multiple home PLMN operators. The SEAL provider and the VAL service provider or the home PLMN operator can be part of the same organization, in which case the business relationship between the two is internal to a single organization.

The home PLMN operator can have PLMN operator service arrangements with multiple VAL service providers and the VAL service provider can have PLMN operator service arrangements with multiple home PLMN operators. As part of the PLMN operator service arrangement between the VAL service provider and the home PLMN operator, PLMN subscription arrangements can be provided which allows the VAL UEs to register with home PLMN operator network.

The home PLMN operator can have PLMN roaming agreements with multiple visited PLMN operators and the visited PLMN operator can have PLMN roaming agreements with multiple home PLMN operators.

6 Generic functional model for SEAL services

6.1 General

The functional model for SEAL is organized into generic SEAL service functional model and specific SEAL service functional models. The generic SEAL service functional model will be used as the reference model for the specific SEAL service functional models.

The following SEAL services are supported towards the vertical application layer:

- Location management;

- Group management;

- Configuration management;

- Identity management;

- Key management; and

- Network resource management.

The generic functional model for the SEAL is organized into generic functional entities to describe a functional architecture which addresses the application layer support aspects for vertical applications. The on-network and off-network functional model is specified in this clause.

6.2 On-network functional model description

Figure 6.2-1 illustrates the generic on-network functional model for SEAL.
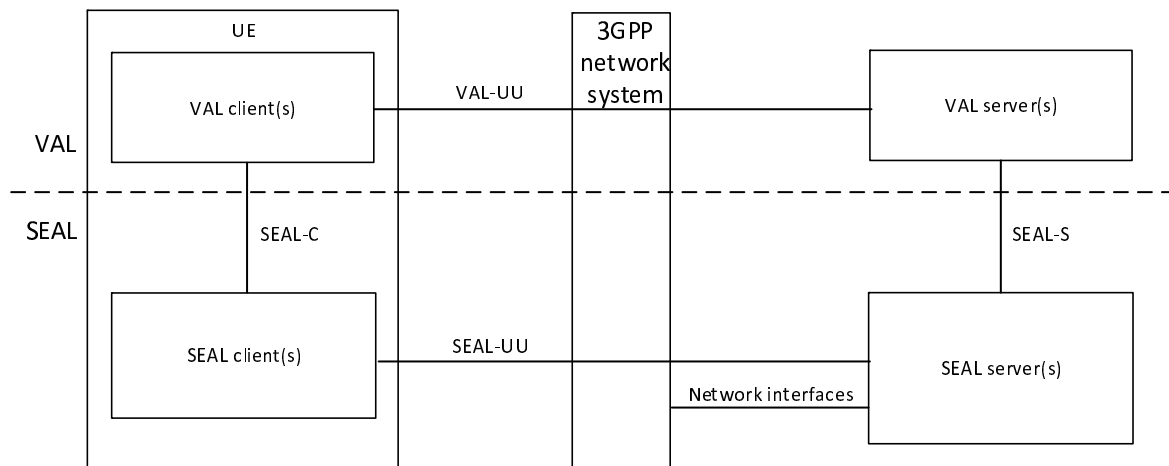
Figure 6.2-1: Generic on-network functional model

In the vertical application layer, the VAL client communicates with the VAL server over VAL-UU reference point. VAL-UU supports both unicast and multicast delivery modes.

NOTE 1: The VAL-UU reference point is out of scope of the present document.

The SEAL functional entities on the UE and the server are grouped into SEAL client(s) and SEAL server(s) respectively. The SEAL consists of a common set of services (e.g. group management, location management) and reference points. The SEAL offers its services to the vertical application layer (VAL).

NOTE 2: The functionalities and reference points of the vertical application layer are out of scope of the present document.

NOTE 3: The vertical application layer may further consist of vertical application enabler layer functionalities (specified by 3GPP) and application specific functionalities, which is out of scope of the present document.

The SEAL client(s) communicates with the SEAL server(s) over the SEAL-UU reference points. SEAL-UU supports both unicast and multicast delivery modes. The SEAL client(s) provides the service enabler layer support functions to the VAL client(s) over SEAL-C reference points. The VAL server(s) communicate with the SEAL server(s) over the SEAL-S reference points. The SEAL server(s) may communicate with the underlying 3GPP network systems using the respective 3GPP interfaces specified by the 3GPP network system.

Editor's Note: SEAL-UU support for multicast delivery is FFS.

The specific SEAL client(s) and the SEAL server(s) along with their specific SEAL-UU reference points and the specific network interfaces of 3GPP network system used are described in the respective on-network functional model for each SEAL service.

Figure 6.2-2 illustrates the functional model for interconnection between SEAL servers.
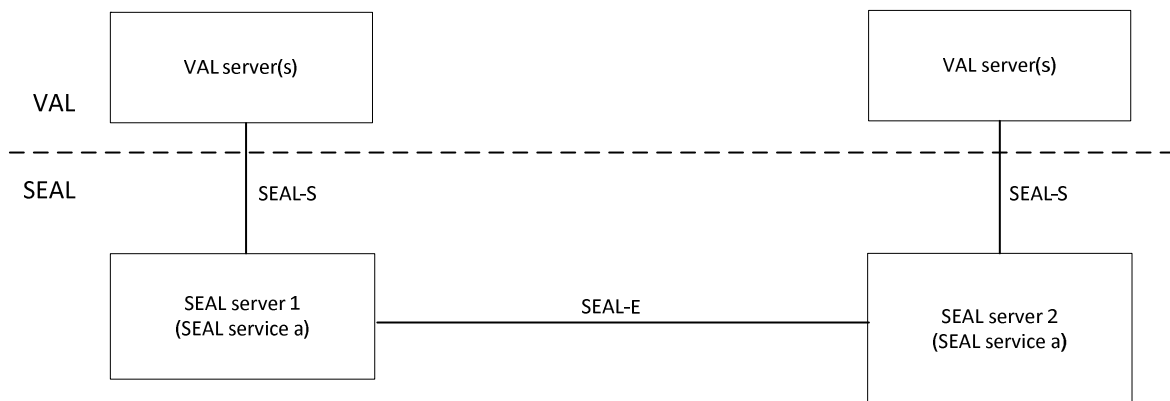
Figure 6.2-2: Interconnection between SEAL servers

To support distributed SEAL server deployments, the SEAL server interacts with another SEAL server for the same SEAL service over SEAL-E reference point.

Figure 6.2-3 illustrates the functional model for inter-service communication between SEAL servers.
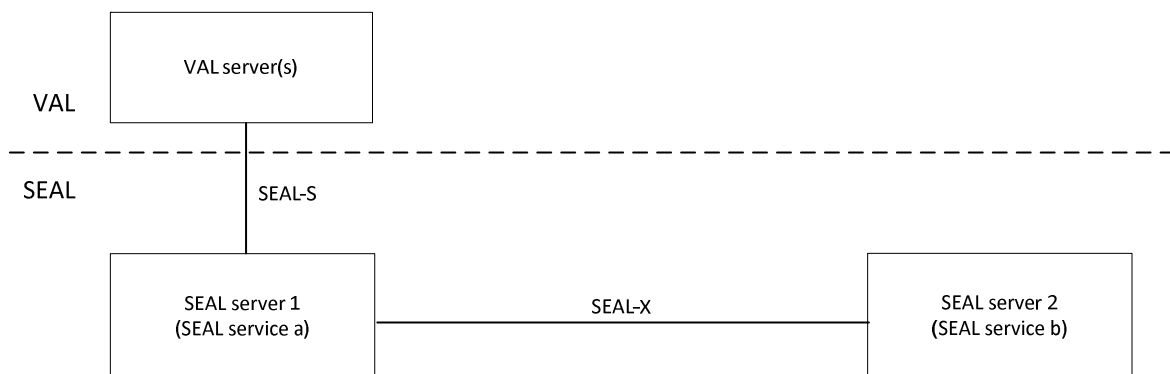
Figure 6.2-3: Inter-service communication between SEAL servers

The SEAL server interacts with another SEAL server for inter-service communication over SEAL-X reference point.

Figure 6.2-4 illustrates the functional model for communication between SEAL server and VAL user database.
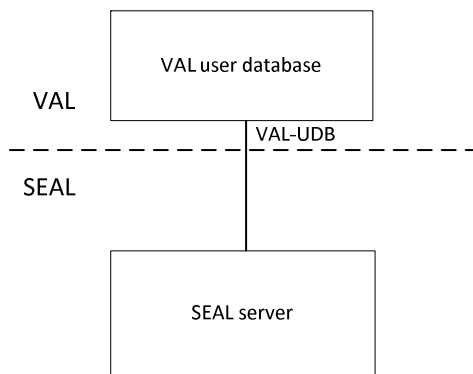
Figure 6.2-4: Communication between SEAL server and VAL user database

The SEAL server interacts with the VAL user database for storing and retrieving user profile over VAL-UDB reference point.

Figure 6.2-5 shows the functional model for the signalling control plane.
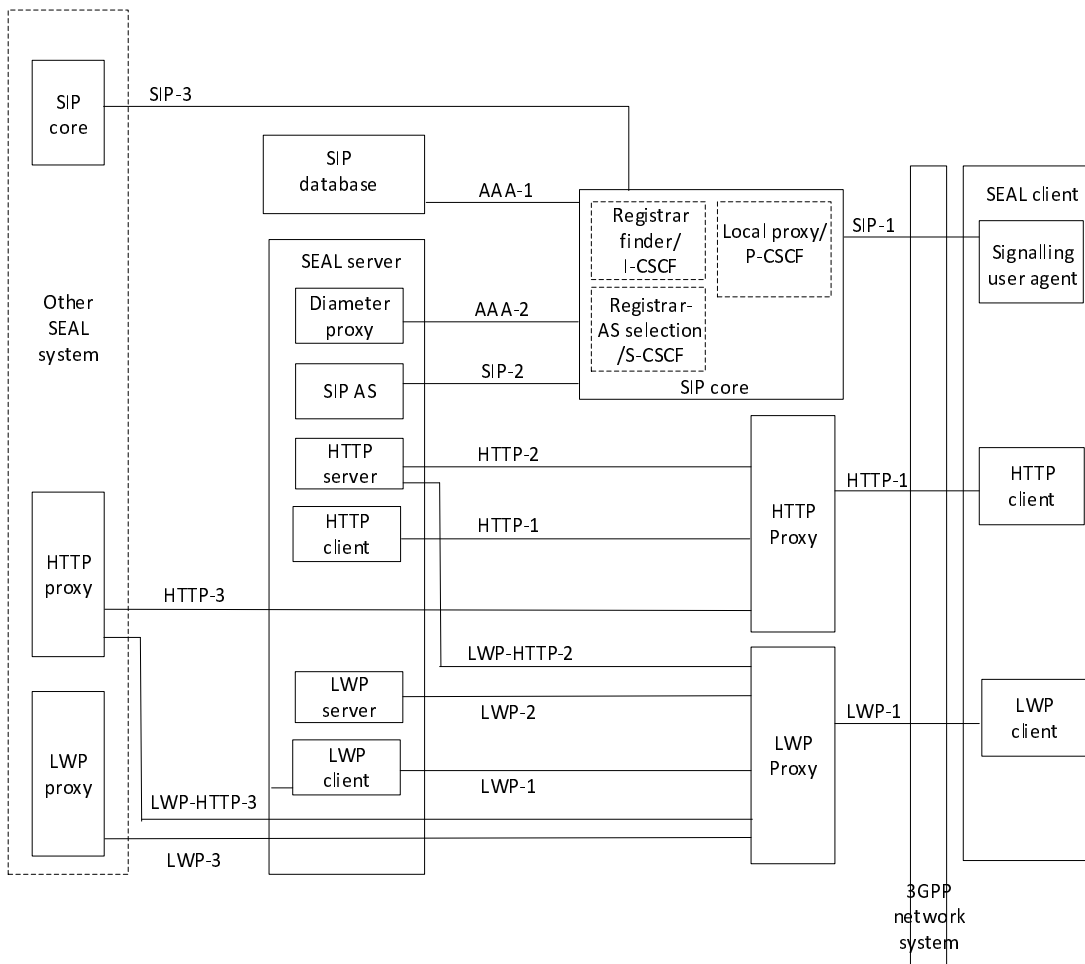
Figure 6.2-5: Functional model for signalling control plane

NOTE: The Light-weight Protocol (LWP) functional entities and reference points are a generic representation of protocol entities and reference points for use in constrained environments. Realizations of LWP by means of a particular transport protocol are defined in the annex of this specification. Realizations of LWP by means of transport protocols is not limited to those defined in the annex of this specification.

6.3 Off-network functional model description

Figure 6.3-1 illustrates the generic off-network functional model for SEAL.
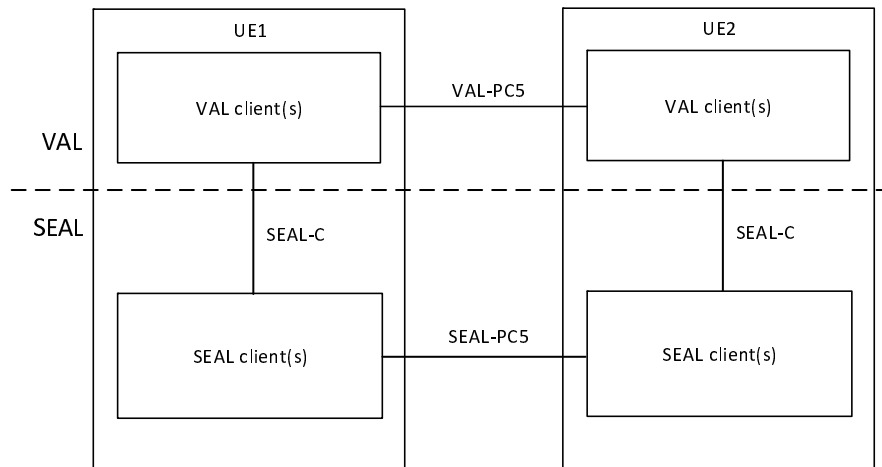
Figure 6.3-1: Generic off-network functional model

In the vertical application layer, the VAL client of UE1 communicates with VAL client of UE2 over VAL-PC5 reference point. A SEAL client of UE1 interacts with the corresponding SEAL client of UE2 over SEAL-PC5 reference points. The UE1, if connected to the network via Uu reference point, can also act as a UE-to-network relay, to enable UE2 to access the VAL server(s) over the VAL-UU reference point.

> NOTE: The VAL-PC5 reference point is out of scope of the present document.

> Editor's Note: The functionalities of reference points between the SEAL clients of two UEs over SEAL-PC5 reference point is FFS.

The specific SEAL client(s) along with their specific SEAL-PC5 reference points are described in the respective off-network functional model for each SEAL service.

6.4 Functional entities description

6.4.1 General

Each subclause is a description of a functional entity corresponding to SEAL and does not imply a physical entity.

6.4.2 Application plane

6.4.2.1 General

Entities within the application plane of a VAL system provide application control and media specific functions to support one or more VAL services.

6.4.2.2 VAL client

The VAL client provides the client side functionalities corresponding to the vertical applications (e.g. V2X client). The VAL client supports interactions with the SEAL client(s).

> NOTE: The details of the VAL client is specific to the vertical and out of scope of the present document.

6.4.2.3 VAL server

The VAL server provides the server side functionalities corresponding to the vertical applications (e.g. V2X application servers). The VAL server acts as CAPIF's API invoker as specified in 3GPP TS 23.222 [8].

NOTE: The details of the VAL server is specific to the vertical and out of scope of the present document.

6.4.2.4 SEAL client

The SEAL client provides the client side functionalities corresponding to the specific SEAL service. The SEAL client(s) supports interactions with the VAL client(s). The SEAL client also supports interactions with the corresponding SEAL client between the two UEs.

NOTE: It is up to each SEAL client to support the appropriate signalling plane entities.

6.4.2.5 SEAL server

The SEAL server provides the server side functionalities corresponding to the specific SEAL service. The SEAL server supports interactions with the VAL server(s). The SEAL server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The SEAL server also supports interactions with the corresponding SEAL server in distributed SEAL deployments.

NOTE: It is up to each SEAL server to support the appropriate signalling plane entities.

6.4.2.6 VAL user database

This functional entity contains information of the user profile associated with a VAL service that is served by the VAL service provider at the application plane.

Each VAL service may have a corresponding user database e.g. MCPTT user database as defined in 3GPP TS 23.379 [3], MCVideo user database as defined in 3GPP TS 23.281 [5] and MCData user database as defined in 3GPP TS 23.282 [6].

NOTE: It is up to each SEAL server to support the appropriate signalling plane entities.

6.4.3 Signalling control plane

6.4.3.1 SIP entities

6.4.3.1.1 Signalling user agent

This functional entity acts as the SIP user agent (both client and server) for all SIP transactions.

6.4.3.1.2 SIP AS

The SIP AS functional entity supports the following functions on behalf of the VAL service:

- influencing and impacting the SIP session; and

- supporting event subscription and event notification.

NOTE: In the IM CN subsystem, this is provided by the Application Server as defined in 3GPP TS 23.002 [14].

6.4.3.1.3 SIP core

6.4.3.1.3.1 General

The SIP core contains a number of sub-entities responsible for registration, service selection and routing in the signalling control plane.

The SIP core shall be either:

1. compliant with 3GPP TS 23.228 [15], i.e. the SIP core is a 3GPP IP multimedia core network subsystem; or

2. a SIP core, which internally need not comply with the architecture of 3GPP TS 23.228 [15], but with the reference points that are defined in subclause 6.5.3 (if exposed), compliant to the reference points defined in 3GPP TS 23.002 [14].

The data related to the functions of the SIP core, e.g. for data for application service selection, the identity of the serving registrar or authentication related information may be provided by the PLMN operator responsible for the bearer plane. In this case, the SIP database that is the source of the data may be part of the HSS. Alternatively, this data may be provided by the VAL service provider. In this case, the source of the data may be the VAL service provider's SIP database.

6.4.3.1.3.2 Local inbound / outbound proxy

The local inbound / outbound proxy functional entity acts as both an inbound proxy and an outbound proxy for all SIP transactions. This functional entity can provide the following functions:

- NAT traversal;

- Resource control;

- Route/forward requests and responses to the user agents;

- SIP signalling security; and

- Depending on the PLMN operator policy, discovery and address resolution, including E.164 numbers.

    NOTE: In the IM CN subsystem, this functional entity is provided by the P-CSCF as defined in 3GPP TS 23.228 [15].

6.4.3.1.3.3 Registrar finder

The registrar finder functional entity is responsible for:

a) Identifying the serving registrar / application service selection functional entity. The serving registrar / application service selection functional entity is identified using information provided either by the PLMN operator's own SIP database or the VAL service provider's SIP database, and optionally using the PLMN operator's internal information e.g. network topology, registrar availability.

   1) Registrar finder and registrar in the VAL service provider domain: registrar finder in the VAL service provider's domain uses the information from the VAL service provider's SIP database to identify the serving registrar in the VAL service provider domain.

   2) Registrar finder and registrar in the PLMN operator domain: registrar finder uses information from PLMN operator's SIP database to identify the serving registrar in the PLMN operator domain.

   3) Registrar finder in PLMN operator domain and registrar in VAL service provider domain: registrar finder uses information from the VAL service provider's SIP database to identify the serving registrar in the VAL service provider domain.

    NOTE 1: The need for the registrar finder is deployment specific e.g. a deployment that has only one registrar does not need the registrar finder and the related SIP database information.

b) Providing discovery and address resolution, including E.164 numbers.

    NOTE 2: In the IM CN subsystem, this is provided by the I-CSCF as defined in 3GPP TS 23.228 [15].

6.4.3.1.3.4 Registrar / application service selection

The registrar / application service selection functional entity provides the following functions:

- Registrar function (with integral provision of a location server) and also acts as an inbound proxy (with access to the integral location server), and outbound proxy for all SIP transactions where application service selection is required. It registers the user and maintains the association of the location and identity of the user in a location service. It provides notifications of the registration states.

- Supports authentication for identities provided within SIP signalling. Both the registrar (with integral location server) and authentication functions are supported by access either to the public network's own SIP database or the VAL service provider's SIP database.

- Can provide the application service selection for all SIP transactions, possibly based on application service selection information stored by either the public network's own SIP database or the VAL service provider's SIP database.

- Performs SIP signalling security.

   NOTE: In the IM CN subsystem, this is provided by the S-CSCF as defined in 3GPP TS 23.228 [15].

6.4.3.1.4   Diameter proxy

This functional entity acts as a proxy agent for Diameter messaging as specified in IETF RFC 6733 [24].

The Diameter proxy, when used on the AAA-2 interface, is collocated with the migration management server.

Other instances of the Diameter proxy may also be present in the SIP core / IMS.

   NOTE: The number of instances of the Diameter proxy is deployment specific.

6.4.3.2   SIP database

6.4.3.2.1   General

The SIP database contains information concerning the SIP subscriptions and corresponding identity and authentication information required by the SIP core, and such information as application service selection.

In deployment scenarios where the PLMN operator provides the SIP core, this database is provided by the HSS.

In deployment scenarios where the VAL service provider provides the SIP core, the SIP database may be provided by the VAL service provider.

Access to the data residing in the SIP database is restricted to the SIP core entities that are specifically serving the subscriber/user whose data are stored, i.e. registrars and registrar finders can access SIP databases only when they are part of the same trust domain for the data being provided.

   NOTE: The SIP database can be in a different network than the registrar finder since the trust domain for the criteria for registrar selection can be different than the trust domain for the signalling plane user identities.

The SIP database is responsible for storing the following user related information:

- signalling plane user identities: Numbering and addressing information;

- signalling plane security information: SIP core access control information for authentication and authorization;

- VAL UE Location information at inter-system level: the SIP database supports the user registration, and stores inter-system location information, etc.; and

- signalling plane subscription profile (including initial filter criteria).

The SIP database also generates signalling plane security information for mutual authentication, communication integrity check and ciphering.

Based on this information, the SIP database is also responsible to support the call control and session management entities of the SIP core.

The SIP database consists of the following functionalities:

- support for control functions of the SIP core such as the Registrar and Registrar finder. This is needed to enable subscriber usage of the SIP core services. This functionality is independent of the access network used to access the SIP core; and

- authentication functionality required by the SIP core to authenticate the VAL UE.

6.4.3.2.2 SIP database logical functions

The SIP database provides the following logical functions:

a) mobility management;

   - provides the UE mobility through the SIP core.

b) registrar assignment support;

   - provides to the registrar finder the required capabilities for VAL services based on VAL service provider requirements on a per-user basis, (e.g. whether a particular registrar within the PLMN operator's network (e.g. a registrar reserved for VAL service use or a registrar in a secure location) or a registrar within the VAL service provider network is assigned.

c) call and/or session establishment support;

   - provides the call and/or session establishment procedures in the SIP core. For terminating traffic, it provides information on which registrar currently hosts the user.

d) user security information generation;

   - provides generation of user authentication, integrity and ciphering data for the SIP core.

e) signalling plane security support;

   - provides authentication procedures to access VAL services by storing the generated data for authentication, integrity and ciphering at the signalling plane and by providing these data to the appropriate registrar.

f) user identification handling;

   - provides the appropriate relations among all the identifiers uniquely determining the signalling plane identities in the SIP core e.g. IMS public identities.

g) access authorisation; and

   - provides authorisation of the user for mobile access when requested by the registrar e.g. by checking that the user is allowed to roam to that visited network.

h) service authorisation support.

   - provides basic authorisation for terminating call/session establishment and service invocation. The SIP database may update the registrar with filter criteria to trigger the VAL server(s).

6.4.3.3 HTTP entities

6.4.3.3.1 HTTP client

This functional entity acts as the client for all hypertext transactions.

6.4.3.3.2 HTTP proxy

This functional entity acts as a proxy for hypertext transactions between the HTTP client and one or more HTTP servers. The HTTP proxy terminates a TLS session on HTTP-1 with the HTTP client of the VAL UE allowing the HTTP client to establish a single TLS session for hypertext transactions with multiple HTTP servers that are reachable by the HTTP proxy.

The HTTP proxy terminates the HTTP-3 reference point that lies between different HTTP proxies. It may provide a topology hiding function from HTTP entities outside the trust domain of the VAL system.

The HTTP proxy shall be in the same trust domain as the HTTP clients and HTTP servers that are located within a VAL service provider's network. There can be multiple instances of an HTTP proxy e.g. one per trust domain.

   NOTE: The number of instances of the HTTP proxy is deployment specific.

6.4.3.3.3   HTTP server

This functional entity acts as the HTTP server for all hypertext transactions.

6.4.3.4   LWP entities

6.4.3.4.1   LWP client

This functional entity acts as the light-weight protocol client for all transactions of the SEAL client executing in a constrained UE. A SEAL client executing in an unconstrained UE may choose to use the LWP client if it is available.

6.4.3.4.2   LWP proxy

This functional entity acts as a proxy for transactions between the LWP client and one or more LWP servers. The LWP proxy typically terminates a secure transport protocol (e.g. DTLS, TLS or secure WebSocket) session on LWP-1 reference point with the LWP client of the VAL UE allowing the LWP client to establish a single secure session for transactions with multiple LWP servers that are reachable by the LWP proxy.

The LWP proxy can act as a cross-protocol LWP-HTTP proxy to enable LWP clients to access resources on HTTP servers via the LWP-HTTP-2 reference point.

The LWP proxy terminates LWP-3 reference point that lies between different LWP proxies. It may provide a topology hiding function from LWP entities outside the trust domain of the VAL system.

The LWP proxy can also terminate LWP-HTTP-3 reference point for interworking with another HTTP proxy. In this role it provides cross-protocol mapping and may provide a topology hiding function from HTTP entities outside the trust domain of the VAL system.

The LWP proxy shall be in the same trust domain as the LWP clients and LWP servers that are located within a VAL service provider's network. There can be multiple instances of a LWP proxy e.g. one per trust domain.

6.4.3.4.3   LWP server

This functional entity acts as the LWP server for all LWP transactions of the SEAL server.

> NOTE: A SEAL client can act as LWP server for certain transactions as required by the SEAL service.

6.4.3.5   LWP usage

LWP is a generic representation of a light-weight protocol for use in constrained environments. Realizations of the light-weight protocol (LWP) functional entities and reference points to a particular protocol are defined in the annexes of this specification.

LWP is a representation of a protocol to be used by the SEAL service enablers on their respective SEAL-UU reference points when the SEAL client is executing in a constrained UE. In this case the SEAL client should use the LWP-1 reference point with the LWP proxy and should use either the LWP-2 or the LWP-HTTP-2 reference point for transport and routing of the related signalling with the SEAL server.

> Editor's note: Which procedures of a SEAL service enabler are not necessary to be supported for a constrained UE is FFS.

A SEAL client executing in a non-constrained UE may choose to use the LWP-1 reference point with the LWP proxy and may use either the LWP-2 or the LWP-HTTP-2 reference point for transport and routing of the related signalling with the SEAL server.

LWP may be used for interactions between SEAL servers on their respective SEAL-E reference points. For this usage the SEAL-E reference point shall use the LWP-1 and either the LWP-2 or the LWP-3 reference point depending on the trust relationship between the interacting SEAL servers.

6.5 Reference points description

6.5.1 General reference point principle

The protocols on any reference point that is exposed for VAL service interoperability with other SIP core or other IMS entities in other systems shall be compatible with the protocols defined for the corresponding reference point defined in 3GPP TS 23.002 [14].

6.5.2 Application plane

6.5.2.1 General

The reference points for the generic functional model for SEAL are described in the following subclauses.

6.5.2.2 VAL-UU

The interactions related to vertical application layer support functions between VAL client and VAL server are supported by VAL-UU reference point. This reference point is an instance of Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

NOTE: The details of VAL-UU reference point is out of scope of the present document.

6.5.2.3 VAL-PC5

The interactions related to vertical application layer support functions between the VAL clients of two UEs are supported by VAL-PC5 reference point. This reference point is an instance of PC5 reference point as described in 3GPP TS 23.303 [12].

NOTE: The details of VAL-PC5 reference point is out of scope of the present document.

6.5.2.4 SEAL-UU

The interactions between a SEAL client and the corresponding SEAL server are generically referred to as SEAL-UU reference point. The specific SEAL service reference point corresponding to SEAL-UU is specified in the specific SEAL service functional model.

6.5.2.5 SEAL-PC5

The interactions between the SEAL clients of two VAL UEs are generically referred to as SEAL-PC5 reference point. The specific SEAL service reference point corresponding to SEAL-PC5 is specified in the specific SEAL service functional model.

6.5.2.6 SEAL-C

The interactions between the VAL client(s) and the SEAL client(s) within a VAL UE are generically referred to as SEAL-C reference point. The specific SEAL service reference point corresponding to SEAL-C is specified in the specific SEAL service functional model.

6.5.2.7 SEAL-S

The interactions between the VAL server and the SEAL server are generically referred to as SEAL-S reference point. The specific SEAL service reference point corresponding to SEAL-S is specified in the specific SEAL service functional model.

6.5.2.8 SEAL-E

The interactions between the SEAL servers of the same type are generically referred to as SEAL-E reference point. The specific SEAL service reference point corresponding to SEAL-E is specified in the specific SEAL service functional model.

6.5.2.9 SEAL-X

6.5.2.9.1 General

The interactions between the SEAL servers of different type are generically referred to as SEAL-X reference point. The specific SEAL server interactions corresponding to SEAL-X are described in the following subclauses.

6.5.2.9.2 Reference point SEAL-X1 (between the key management server and the group management server)

The SEAL-X1 reference point, which exists between the key management server and the group management server, provides a means for the key management server to provide security related information (e.g. encryption keys) to the group management server.

The SEAL-X1 reference point shall use the HTTP-1 and HTTP-2 reference points and may use the HTTP-3 reference point for transport and routing of security related information to the group management server.

NOTE: SEAL-X1 is specified in subclause 5.1.1.1 of 3GPP TS 33.434 [29].

6.5.2.9.3 Reference point SEAL-X2 (between the group management server and the location management server)

The SEAL-X2 reference point enables the group management server to interact with the location management server.

The SEAL-X2 reference point supports:

- the group management server to create a location-based group with the help from the location management server.

6.5.2.10 Reference point VAL-UDB (between the VAL user database and the SEAL server)

The VAL-UDB reference point, which exists between the VAL user database and the SEAL server, is used for:

- storing the user profile data in the specific VAL user database; and

- obtaining the user profile from the specific VAL user database for further configuration in the UE.

NOTE: The details of the VAL-UDB reference point is out of scope of the present document.

6.5.3 Signalling control plane

6.5.3.1 General

The reference points for the SIP and HTTP signalling are described in the following subclauses.

6.5.3.2 Reference point SIP-1(between the signalling user agent and the SIP core)

The SIP-1 reference point, which exists between the signalling user agent and the SIP core for establishing a session in support of VAL service, shall use the Gm reference point as defined in 3GPP TS 23.002 [14] (with necessary enhancements to support VAL service requirements and profiled to meet the minimum requirements for support of VAL service). The SIP-1 reference point fulfils the requirements of the GC1 reference point specified in 3GPP TS 23.468 [16]. The SIP-1 reference point is used for:

- SIP registration;

- authentication and security to the service layer;

- event subscription and event notification;

- communication of the TMGI for multicast operation;

- overload control;

- session management; and

- media negotiation.

6.5.3.3 Reference point SIP-2 (between the SIP core and the SIP AS)

The SIP-2 reference point, which exists between the SIP core and the SIP AS for establishing a session in support of VAL service, shall use the ISC and Ma reference points as defined in 3GPP TS 23.002 [14]. The SIP-2 reference point is used for:

- notification to the VAL service server(s) of SIP registration by the VAL UE;

- authentication and security to the service layer;

- event subscription and event notification;

- communication of the TMGI for multicast operation;

- session management; and

- media negotiation.

6.5.3.4 Reference point SIP-3 (between the SIP core and SIP core)

The SIP-3 reference point, which exists between one SIP core and another SIP core for establishing a session in support of VAL service, shall use the Mm and ICi reference points as defined in 3GPP TS 23.002 [14]. The SIP-3 reference point is used for:

- event subscription and event notification;

- session management; and

- media negotiation.

    Editor's note: it is FFS whether changes are needed to SIP-3 when used between servers in different trust domains.

6.5.3.5 Reference point HTTP-1 (between the HTTP client and the HTTP proxy)

The HTTP-1 reference point exists between the HTTP client and the HTTP proxy. Between the VAL UE and the HTTP proxy, the HTTP-1 reference point shall use the Ut reference point as defined in 3GPP TS 23.002 [14] (with necessary enhancements to support specific VAL service requirements). The HTTP-1 reference point is based on HTTP (which may be secured using e.g. SSL, TLS).

6.5.3.6 Reference point HTTP-2 (between the HTTP proxy and the HTTP server)

The HTTP-2 reference point, which exists between the HTTP proxy and the HTTP server, is based on HTTP (which may be secured using e.g. SSL, TLS).

6.5.3.7 Reference point HTTP-3 (between the HTTP proxy and HTTP proxy)

The HTTP-3 reference point, which exists between the HTTP proxy and another HTTP proxy in a different network, is based on HTTP (which may be secured using e.g. SSL, TLS).

Editor's note: it is FFS whether changes are needed to HTTP-3 when used between servers in different trust domains.

6.5.3.8 Reference point AAA-1 (between the SIP database and the SIP core)

The AAA-1 reference point, which exists between the SIP database and the SIP core, is used by the SIP core to retrieve signalling plane data from the SIP database. The AAA-1 reference point utilises the Cx reference point as defined in 3GPP TS 23.002 [14].

In some deployment scenarios the registrar and SIP database are located in the VAL service provider's network while the registrar finder is in the PLMN operator's network and the AAA-1 reference point is an inter-network interface.

6.5.3.9 Reference point AAA-2 (between the SIP core and Diameter proxy)

The AAA-2 reference point, which exists between the SIP core / IMS and Diameter proxy for SIP registration during migration, shall use the Cx reference point as defined in 3GPP TS 23.002 [14]. The AAA-2 reference point is used for:

- authentication and security to the service layer for migration;

6.5.3.10 Reference point LWP-1 (between the LWP client and the LWP proxy)

The LWP-1 reference point exists between the LWP client and the LWP proxy.

6.5.3.11 Reference point LWP-2 (between the LWP proxy and the LWP server)

The LWP-2 reference point exists between the LWP proxy and the LWP server.

6.5.3.12 Reference point LWP-3 (between the LWP proxy and LWP proxy)

The LWP-3 reference point exists between the LWP proxy and another LWP proxy in a different network.

6.5.3.13 Reference point LWP-HTTP-2 (between the LWP proxy and the HTTP server)

The LWP-HTTP-2 reference point exists between the LWP proxy and the HTTP server. HTTP-2 and LWP-HTTP-2 reference points are equivalent.

6.5.3.14 Reference point LWP-HTTP-3 (between the LWP proxy and the HTTP proxy)

The LWP-HTTP-3 reference point exists between the LWP proxy and another HTTP proxy in a different network. HTTP-3 and LWP-HTTP-3 reference points are equivalent.

7 Identities

7.1 User identity (User ID)

The VAL user presents the user identity to the identity management server during a user authentication transaction, to provide the identity management client a means for VAL service authentication. In general, since identity management is a common SEAL service, it uses a set of credentials (e.g. biometrics, secureID, username/password) that may not necessarily be tied to a single VAL service. The user credentials uniquely identifies the VAL user to the identity management server.

NOTE: The specific security and authentication mechanisms required in order to use the user ID is specified in 3GPP TS 33.434 [29].

Editor's note: The naming and definition of the identities in subclause 7 may require further study (e.g. renaming user identity to VAL user identity, and renaming VAL user identity to VAL service user identity).

7.2 VAL user identity (VAL user ID)

The VAL user ID is a unique identifier within the VAL service that represents the VAL user. For example, the VAL user ID may be a URI. The VAL user ID is used for authentication and authorization purposes for providing the VAL service towards the VAL user via the VAL UE. The VAL user ID also indicates the VAL service provider with whom the VAL user has a VAL service agreement. The VAL user may have VAL service agreement with several VAL service providers and thus will have obtained unique VAL user ID per VAL service provider. The VAL user ID can be used to access any SEAL service.

Based on the service agreement, VAL user ID may be mapped to a VAL UE ID.

7.3 VAL UE identity (VAL UE ID)

The VAL UE ID is a unique identifier within the VAL service that represents the VAL UE. For example, the VAL UE ID for V2X service is mapped to the StationID as specified in ETSI TS 102 894-2 [25]. The VAL UE ID is used to address the VAL UE in order to send VAL messages or to access SEAL services.

Based on the service agreement, GPSI (as specified in 3GPP TS 23.003 [38]) may be used as VAL UE identity.

7.4 VAL service identity (VAL service ID)

The VAL service ID is a unique identifier that represents the VAL service. A VAL server provides a list of VAL services towards the VAL users or VAL UE. Each VAL service is uniquely identified by a VAL service ID, which is an identifier of the VAL application providing that VAL service. The VAL service ID can be used for policy mapping, QoS handling for VAL communication and VAL message distribution. For example, an identifier of a V2X service, e.g. ITS-AID or PSID specified in ETSI TS 102 965 [26] and ISO TS 17419 [27], can be used as a V2X service ID.

7.5 VAL group identity (VAL group ID)

The VAL group ID is a unique identifier within the VAL service that represents a set of VAL users or VAL UE according to the VAL service. The set of VAL users may belong to the same or different VAL service providers. It indicates the VAL application server where the group is defined.

7.6 VAL system identity (VAL system ID)

The VAL system ID is a globally unique identifier representing a VAL system.

7.7 VAL Stream ID

A VAL Stream ID is an identity used by the VAL server to identify a VAL stream.

8 Application of functional model to deployments

8.1 General

This clause describes deployments of the functional model specified in clause 6.

8.2 Deployment of SEAL server(s)

The SEAL server(s) may be deployed either in the PLMN operator domain or deployed in the VAL service provider domain. The SEAL server(s) connects with the 3GPP network system in one or more PLMN operator domain. The SEAL server(s) may be supporting multiple VAL servers.

8.2.1 SEAL server(s) deployment in PLMN operator domain

Figure 8.2.1-1 illustrates deployment of the SEAL server(s) in a single PLMN operator domain and the VAL server(s) in the VAL service provider domain.
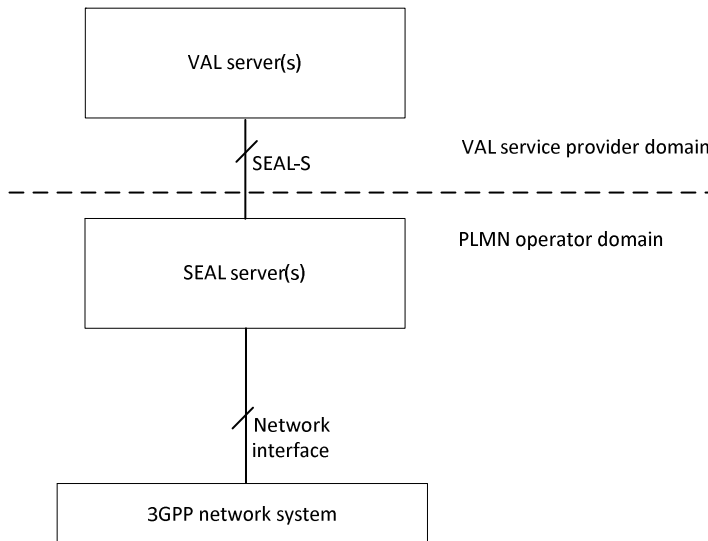
Figure 8.2.1-1: SEAL server(s) deployed in a single PLMN operator domain

Figure 8.2.1-2 illustrates the deployment of SEAL server(s) in multiple PLMN operator domain and provides SEAL services to the VAL server(s) deployed in the VAL service provider domain. SEAL servers deployed in multiple PLMN operator domain are not interconnected.
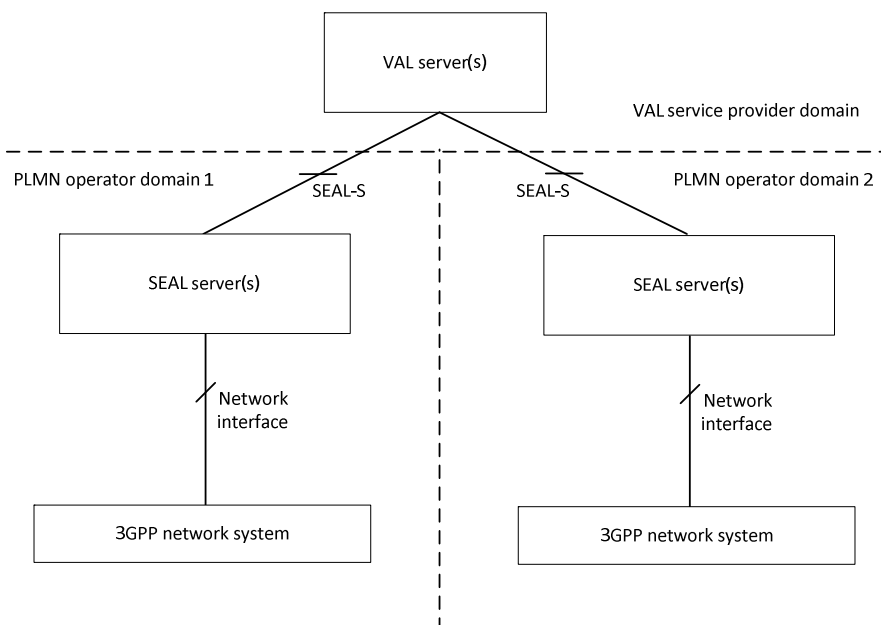
Figure 8.2.1-2: SEAL server(s) deployed in multiple PLMN operator domain without interconnection between SEAL servers

Figure 8.2.1-3 illustrates the deployment of SEAL servers in multiple PLMN operator domain and provides SEAL services to the VAL server(s) deployed in the VAL service provider domain. SEAL servers deployed in multiple PLMN operator domain are interconnected.
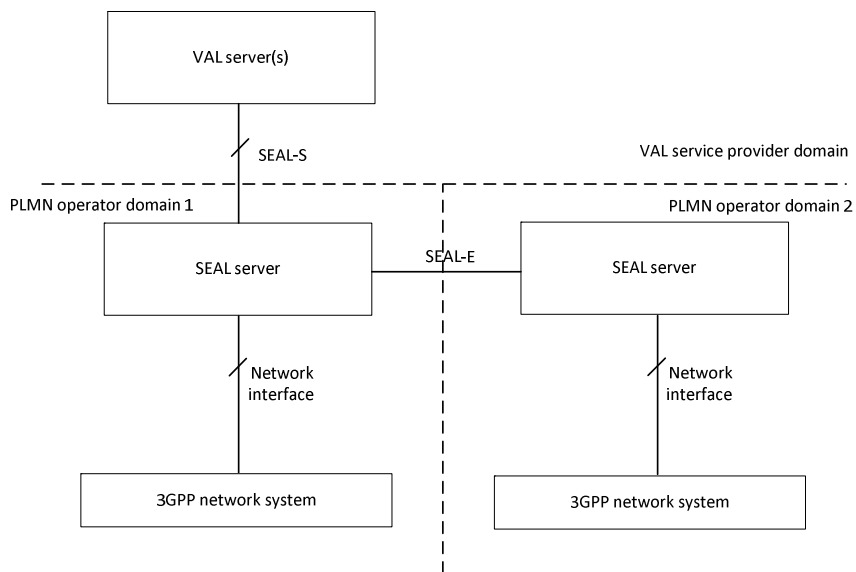
Figure 8.2.1-3: SEAL server(s) deployed in multiple PLMN operator domain with interconnection between SEAL servers

Figure 8.2.1-4 illustrates the deployment of SEAL servers in a single PLMN operator domain and provides SEAL services to the VAL server(s) deployed in the VAL service provider domain. SEAL servers deployed in a single PLMN operator domain are interconnected.
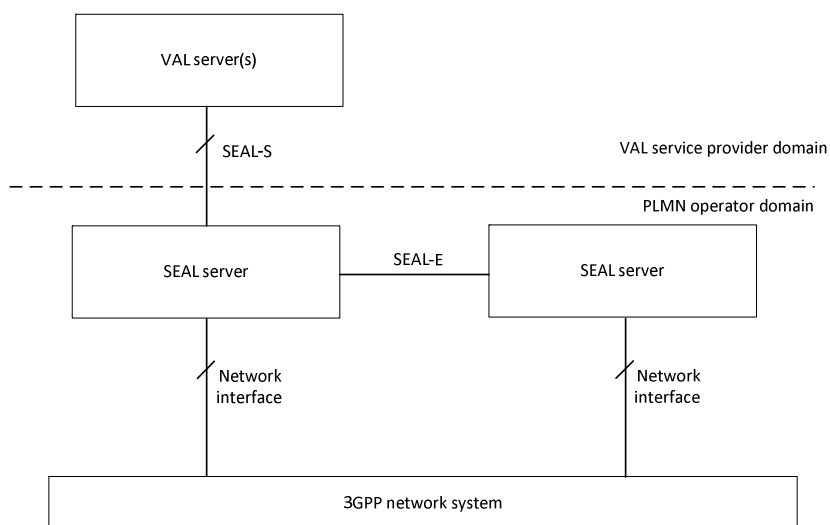
Figure 8.2.1-4: SEAL server(s) deployed in a single PLMN operator domain with interconnection between SEAL servers

8.2.2 SEAL server(s) deployment in VAL service provider domain

Figure 8.2.2-1 illustrates deployment of the SEAL server(s) and the VAL server(s) in VAL service provider domain.
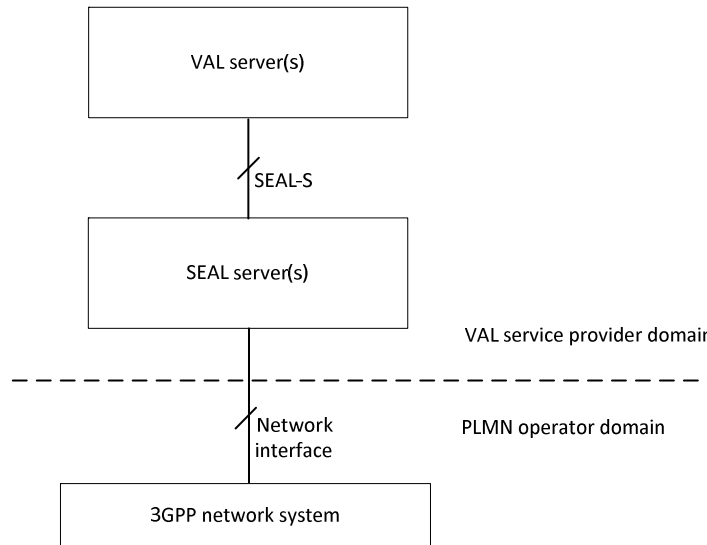
Figure 8.2.2-1: Deployment of SEAL server(s) with connections to 3GPP network system in a single PLMN operator domain

Figure 8.2.2-2 illustrates deployment of the SEAL server(s) which connects to the 3GPP network system in multiple PLMN operator domain.
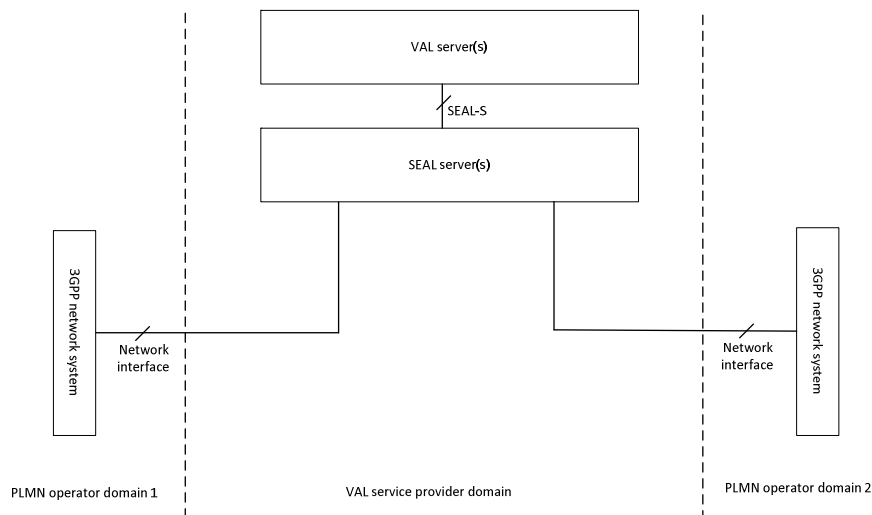
Figure 8.2.2-2: Deployment of SEAL server(s) with connections to 3GPP network system in multiple PLMN operator domains

Figure 8.2.2-3 illustrates the deployment of multiple SEAL servers in the VAL service provider domain where SEAL server 1 and SEAL server 2 connect with 3GPP network system of PLMN operator domain 1 and PLMN operator domain 2 respectively. The SEAL servers interconnect via SEAL-E and support the VAL service provider domain applications for the VAL UEs connected via both the PLMN operator domains.
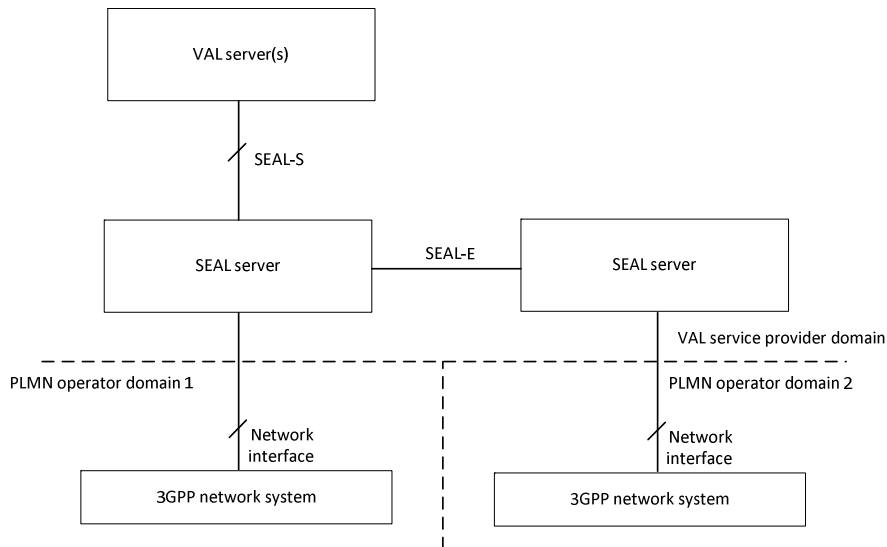
Figure 8.2.2-3: Distributed deployment of SEAL servers in VAL service provider domain

8.2.3 SEAL server(s) deployment outside of VAL service provider domain and PLMN operator domain

Figure 8.2.3-1 illustrates deployment of the SEAL server(s) outside of both the VAL service provider domain and PLMN operator domain i.e. in SEAL provider domain.
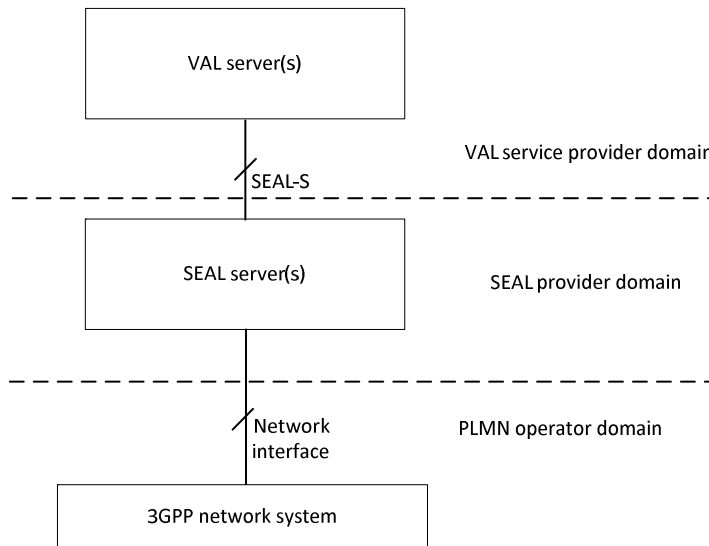
Figure 8.2.3-1: Deployment of SEAL server(s) outside of VAL service domain and PLMN operator domain

9 Location management

9.1 General

The location management is a SEAL service that offers the location management related capabilities to one or more vertical applications.

9.2 Functional model for location management

9.2.1 General

The functional model for the location management is based on the generic functional model specified in clause 6. It is organized into functional entities to describe a functional architecture which addresses the support for location management aspects for vertical applications. The on-network and off-network functional model is specified in this clause.

9.2.2 On-network functional model description

Figure 9.2.2-1 illustrates the generic on-network functional model for location management.
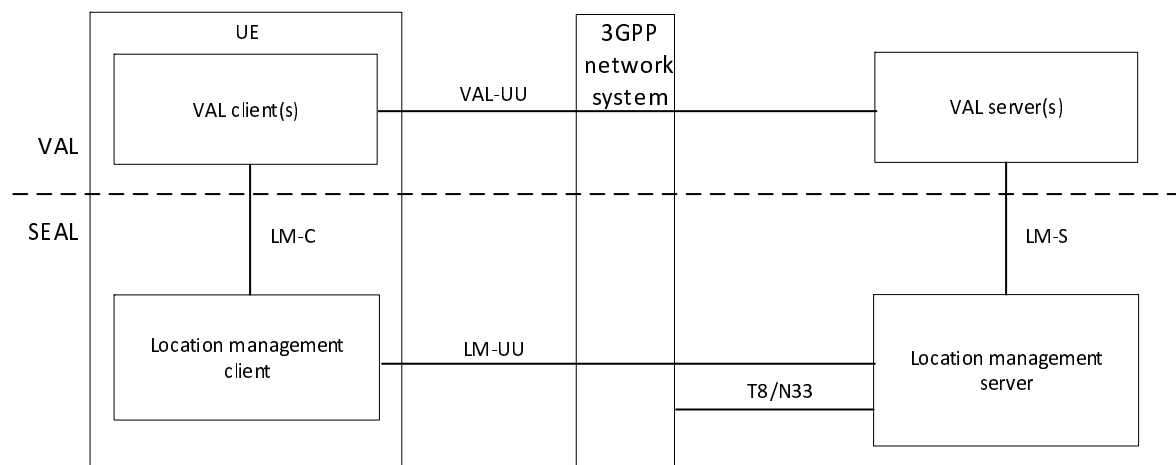
Figure 9.2.2-1: On-network functional model for location management

The location management client communicates with the location management server over the LM-UU reference point. The location management client provides the support for location management functions to the VAL client(s) over LM-C reference point. The VAL server(s) communicate with the location management server over the LM-S reference point.

The location management server communicates with the SCEF via T8 reference point to obtain location information from the underlying 3GPP network system. The location management server obtains location information from the NEF via N33 reference point by mechanism defined in clause 5.2.6.2 of 3GPP TS 23.502 [11].

NOTE: Location information from LCS of 4G system is not exposed by SCEF.

Editor's note: Use of Le interface for acquiring location information provided by PLMN is FFS.

9.2.3 Off-network functional model description

Figure 9.2.3-1 illustrates the off-network functional model for location management.
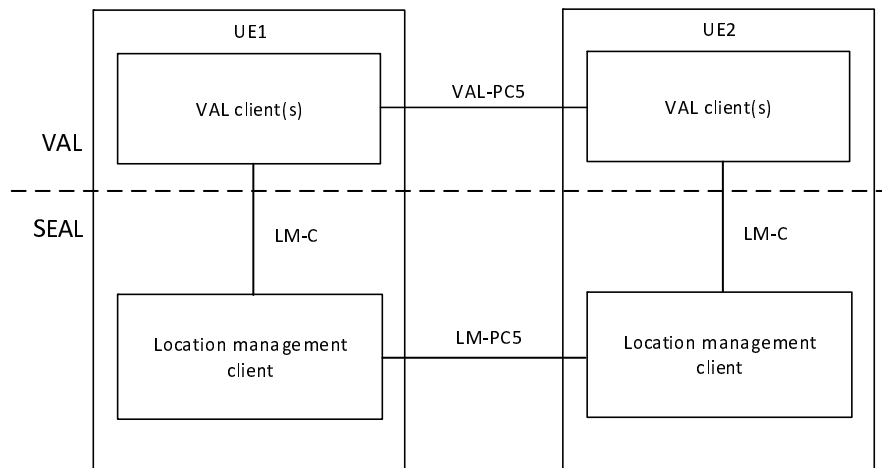
Figure 9.2.3-1: Off-network functional model for location management

The location management client of the UE1 communicates with the location management client of the UE2 over the LM-PC5 reference point.

9.2.4 Functional entities description

9.2.4.1 General

The functional entities for location management SEAL service are described in the following subclauses.

9.2.4.2 Location management client

The location management client functional entity acts as the application client for location management functions. It interacts with the location management server. The location management client also supports interactions with the corresponding location management client between the two UEs.

9.2.4.3 Location management server

The location management server is a functional entity that receives and stores user location information and provides user location information to the vertical application server. The location management server may also acquire location information provided by PLMN operator via T8 reference point. The location management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The location management server also supports interactions with the corresponding location management server in distributed SEAL deployments.

NOTE: The accuracy of location information acquired from 4G system via T8 reference point is not higher than at cell level (ECGI) for E-UTRAN.

9.2.5 Reference points description

9.2.5.1 General

The reference points for the functional model for location management are described in the following subclauses.

9.2.5.2 LM-UU

The interactions related to location management functions between the location management client and the location management server are supported by LM-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

LM-UU reference point provides a means for the location management server to receive location information report from the location management client. The LM-UU reference point shall use SIP-1 and SIP-2 reference points for

subscription/notification related signalling. And for transport and routing of location management related signalling LM-UU reference point uses the HTTP-1 and HTTP-2 signalling control plane reference points.

9.2.5.3 LM-PC5

The interactions related to location management functions between the location management clients located in different VAL UEs are supported by LM-PC5 reference point. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [12].

9.2.5.4 LM-C

The interactions related to location management functions between the VAL client(s) and the location management client within a VAL UE are supported by LM-C reference point.

9.2.5.5 LM-S

The interactions related to location management functions between the VAL server(s) and the location management server are supported by LM-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

LM-S reference point is used by the VAL server to request and receive location information from location management server. The LM-S reference point shall use SIP-1 and SIP-2 reference points for subscription/notification related signalling. And for transport and routing of location management related signalling LM-S reference point uses the HTTP-1 and HTTP-2 signalling control plane reference points.

9.2.5.6 LM-E

The interactions related to location management functions between the location management servers in a distributed deployment are supported by LM-E reference point.

Editor's Note: The functions enabled over LM-E reference point is FFS.

9.2.5.7 T8

The reference point T8 supports the interactions between the location management server and the SCEF and is specified in 3GPP TS 23.682 [13]. The functions related to location management of T8 are supported by the location management server.

9.3 Procedures and information flows for Location management (on-network)

9.3.1 General

Location information of VAL service user shall be provided by the location management client to the location management server. The location information reporting triggers are based on the location reporting configuration. Different type of location information can be provided.

Editor's note: The security and privacy aspects related to VAL server obtaining UE's location information are to be addressed by SA3.

9.3.2 Information flows for location information

9.3.2.0 Location reporting configuration request

Table 9.3.2.0-1 describes the information flow from the location management client to the location management server for requesting the location reporting configuration.

Table 9.3.2.0-1: Location reporting configuration request

Information element	Status	Description
Identity	M	Identity of the VAL user or identity of the VAL UE.
VAL service ID	O	Identity of the VAL service for which the location reporting configuration is requested.

9.3.2.1　　Location reporting configuration response

Table 9.3.2.1-1 describes the information flow from the location management server to the location management client for the location reporting configuration. This information flow may be sent individually addressed or group addressed on unicast or multicast.

Table 9.3.2.1-1: Location reporting configuration response

Information element	Status	Description
Identity	M	Identity of the VAL user or VAL group to which the location reporting configuration is targeted or identity of the VAL UE.
Requested location information	O (see NOTE)	Identifies what location information is requested
Triggering criteria	O (see NOTE)	Identifies when the location management client will send the location report
Minimum time between consecutive reports	O (see NOTE)	Defaults to 0 if absent otherwise indicates the time interval between consecutive reports
NOTE:	If none of the information element is present, this represents a cancellation for location reporting.	

9.3.2.2　　Location information report

Table 9.3.2.2-1 describes the information flow from the location management client to the location management server for the location information reporting or from the location management server to the requesting location management client or VAL server to report location information.

Table 9.3.2.2-1: Location information report

Information element	Status	Description
Set of identities	M	Set of identities of the reporting VAL users or VAL UEs
Triggering event	M	Identity of the event that triggered the sending of the report
Location Information	M	Location information
Timestamp	O	Timestamp of the location report

9.3.2.3　　Location information request

Table 9.3.2.3-1 describes the information flow from the VAL server to the location management server and from the location management server to the location management client for requesting an immediate location information report.

Table 9.3.2.3-1: Location information request

Information element	Status	Description
Identity list	M	List of VAL users or VAL UEs whose location information is requested
VAL service ID	O	Identity of the VAL service for which the location information is requested.

Editor's Note: It's FFS whether and how the LMS need to identify the VAL service when the VAL UE ID is used for location request.

Editor's Note: It's FFS the security aspects for LM-Uu and LM-S in relation to the VAL service ID that need to be coordinated with SA3.

9.3.2.4 Location reporting trigger

Table 9.3.2.4-1 describes the information flow from the location management client or VAL server to the location management server for triggering a location reporting procedure.

Table 9.3.2.4-1: Location reporting trigger

Information element	Status	Description
Identity	M (see NOTE 1)	Identity of the requesting authorized VAL user or VAL UE
Identity	M (see NOTE 1)	Identity of the requested VAL user or VAL UE
VAL service ID	O	Identity of the VAL service for which the location reporting trigger is set.
Immediate Report Indicator	O (see NOTE 2)	Indicates whether an immediate location report is required
Requested location information	O (see NOTE 2)	Identifies what location information is requested
Triggering criteria	O (see NOTE 2)	Identifies when the requesting client/VAL server is expecting to receive the location report from the requested VAL user/ VAL UE
Minimum time between consecutive reports	O see (NOTE 2)	Defaults to 0 if absent otherwise indicates the interval time between consecutive reports
Endpoint information	O	Information of the endpoint of the requesting VAL server to which the location report notification has to be sent. It is provided if Immediate Report Indicator is set to required.
NOTE 1: The identity of the requesting VAL user/UE and the requested VAL user/UE should belong to the same VAL service.		
NOTE 2: At least one of these rows shall be present.		

9.3.2.5 Location information subscription request

Table 9.3.2.5-1 describes the information flow from the VAL server or location management client to the location management server for location information subscription request.

Table 9.3.2.5-1: Location information subscription request

Information element	Status	Description
Identity	M	Identity of the requesting VAL server/VAL user or VAL UE
Identities list	M	List of VAL users or VAL UEs whose location information is requested.
VAL service ID	O	Identity of the VAL service for which the location information is subscribed.
Time between consecutive reports	M	It indicates the interval time between consecutive reports

9.3.2.6 Location information subscription response

Table 9.3.2.6-1 describes the information flow from the location management server to the VAL server or location management client for location information subscription response.

Table 9.3.2.6-1: Location information subscription response

Information element	Status	Description
Identity	M	Identity of the requesting VAL server/VAL user or VAL UE
Subscription status	M	It indicates the subscription result

9.3.2.7 Location information notification

Table 9.3.2.7-1 describes the information flow from the location management server to the VAL server or the location management client.

Table 9.3.2.7-1: Location information notification

Information element	Status	Description
Identities list	M	List of the VAL users or VAL UEs whose location information needs to be notified
Identity	M	Identity of the VAL user or VAL UE subscribed to location of another VAL user or VAL UE (see NOTE)
Triggering event	M	Identity of the event that triggered the sending of the notification
Location Information	M	Location information
Timestamp	O	Timestamp of the location report
NOTE: This is only used for location management server sends location information notification to the VAL user or VAL UE who has subscribed the location.		

9.3.2.8 Location reporting configuration cancel request

Table 9.3.2.8-1 describes the location reporting configuration cancel request information flow from the location management client or VAL server to the location management server.

Table 9.3.2.8-1: Location reporting configuration cancel request

Information element	Status	Description
Identity	M	Identity of the requesting authorized VAL user or VAL UE
Identity	M	Identity of the requested VAL user or VAL UE
VAL service ID	O	Identity of the VAL service for which the location reporting configuration is requested to be canceled.

9.3.2.9 Get UE(s) information request

Table 9.3.2.9-1 describes the information flow for a VAL server to get UE(s) information at the LM server.

Table 9.3.2.9-1: Get UE(s) information request

Information element	Status	Description
Location information	M	Location information around which the UE(s) information is requested.
Application defined proximity range information	M	Description of the range information over which the UE(s) information is required.

9.3.2.10 Get UE(s) information response

Table 9.3.2.10-1 describes the information flow for a LM server to respond with UE(s) information to the VAL server.

Table 9.3.2.10-1: Get UE(s) information response

Information element	Status	Description
Result	M	Result from the VAE server in response to subscription request indicating success or failure
List of UEs information (see NOTE)	O	The information of the UEs which were detected in the application defined proximity range. The list can be empty.
>UE ID	M	The identifier of UE
>Location information	M	Location information of UE within the application defined proximity range
NOTE: This IE shall be included when the Result indicates success.		

9.3.2.11 Monitor Location Subscription Request

Table 9.3.2.11-1 describes the information flow from the VAL server to the LM server for monitoring the location deviation of the VAL UE(s).

Table 9.3.2.11-1: Monitor Location Subscription Request

Information element	Status	Description
Identity	M	Identifier of the VAL users or VAL UE whose location monitoring is requested to be monitored in a given location.
Area of Interest	M	Geographic area location information where the VAL server wishes to monitor the VAL UE's location adherence.
Notify Interval	M	Periodic time interval in which the LM server needs to notify the VAL UE's location information to the VAL server.
Notification Target URI	M	Target URI where the VAL server wishes to receive the notifications about VAL UE's location.
Timeout	O	A timeout period when subscription response is not received.

9.3.2.12 Monitor Location Subscription Response

Table 9.3.2.12-1 describes the information flow from LM server to the VAL server for Monitor Location Subscription Response.

Table 9.3.2.12-1: Monitor Location Subscription Response

Information element	Status	Description
Subscription status	M	It indicates the subscription result

9.3.2.13 Notify Location Monitoring Event

Table 9.3.2.13-1 describes the information flow from LM server to the VAL server for notification of location monitoring events.

Table 9.3.2.13-1: Notify Location Monitoring Event message

Information element	Status	Description
Event	M	Information of the event to be reported. The event shall be one of the following: "Notify_Mismatch_Location" – When the location information of the VAL UE, from the location management client and the core network do not match. "Notify_Absence" – When the VAL UE's current location is deviating from the VAL server's area of interest information. "Notify_Presence" – When the VAL UE's current location is within the VAL server's area of interest information.
Identity	M	Identifier of the VAL UE whose location information is reported.
Location	M	Current location of the VAL UE.

Editor's note: It is FFS how the VAL Server's area of interest information is related with the Area of Interest within 3GPP system defined by SA2.

9.3.2.14 Location area monitoring subscription request

Table 9.3.2.14-1 describes the information flow from the VAL server to the location management server for location area monitoring subscription request.

Table 9.3.2.14-1: Location information monitoring subscription request

Information element	Status	Description
Identity	M	Identity of the requesting VAL server, VAL UE or SEAL Server
Location Information criteria	M	Location information to be monitored. It includes the geographic location information or a reference UE along with the application defined proximity range from the reference UE.
Time between consecutive reports	O	It indicates the interval time between consecutive reports
Immediate Report Indicator	O	Indicates whether an immediate location report is required
Triggering events	O	Identifies when the server will send the notification (e.g. distance travelled)

9.3.2.15 Location area monitoring subscription response

Table 9.3.2.15-1 describes the information flow from the location management server to the VAL server for location area monitoring subscription response.

Table 9.3.2.15-1: Location area monitoring subscription response

Information element	Status	Description
Subscription status	M	It indicates the subscription result
Subscription identity	O (see NOTE)	If subscription is successful, identifies the subscription
NOTE: This IE shall be present if subscription status is set to success.		

9.3.2.16 Location area monitoring notification

Table 9.3.2.16-1 describes the information flow from the location management server to the VAL server.

Table 9.3.2.16-1: Location area monitoring notification

Information element	Status	Description
Subscription identity	M	Identity of the subscription
UEs currently present (see NOTE)	O	List of the identities of all VAL UEs who are currently present in the given location area
UEs moved in/out (see NOTE)	O	List of UEs either moved in to the location area or moved out of the location area
>> UEs moved in	O	List of the identities of the VAL UEs who moved in to the given location area since previous notification.
>> UEs moved out	O	List of the identities of the VAL UEs who moved out of the given location area since previous notification.
Triggering event	O	Identity of the event that triggered the sending of the notification
NOTE: Any one of these shall be present.		

9.3.2.17 Location area monitoring subscription modify request

Table 9.3.2.17-1 describes the information flow from the VAL server to the location management server for location area monitoring subscription modify request.

Table 9.3.2.17-1: Location information monitoring subscription modify request

Information element	Status	Description
Identity	M	Identity of the requesting VAL server, VAL UE or SEAL Server
Subscription identity	M	Identifies the subscription
Location Information criteria	M	Location information to be monitored. It includes the geographic location information or a reference UE along with the application defined proximity range from the reference UE.
Time between consecutive reports	O	It indicates the interval time between consecutive reports
Immediate Report Indicator	O	Indicates whether an immediate location report is required
Triggering events	O	Identifies when the server will send the notification (e.g. distance travelled)

9.3.2.18 Location area monitoring subscription modify response

Table 9.3.2.18-1 describes the information flow from the location management server to the VAL server for location area monitoring subscription modify response.

Table 9.3.2.18-1: Location area monitoring subscription modify response

Information element	Status	Description
Subscription modification status	M	It indicates the request result

9.3.2.19 Location area monitoring unsubscribe request

Table 9.3.2.19-1 describes the information flow from the VAL server to the location management server for location area monitoring unsubscribe request.

Information element	Status	Description
Identity	M	Identity of the requesting VAL server, VAL UE or SEAL Server
Subscription identity	M	Identifies the subscription

9.3.2.20 Location area monitoring unsubscribe response

Table 9.3.2.20-1 describes the information flow from the location management server to the VAL server for location area monitoring unsubscribe response.

Table 9.3.2.20-1: Location area monitoring unsubscribe response

Information element	Status	Description
Subscription status	M	It indicates the request result

9.3.3 Event-triggered location reporting procedure

9.3.3.1 General

The location management server provides location reporting configuration to the location management clients, indicating what information the location management server expects and what events will trigger the sending of this information to the location management server. The decision to report location information can be triggered at the location management client by different conditions, e.g., the reception of the location reporting configuration, initial registration, distance travelled, elapsed time, cell change, MBMS SAI change, MBMS session change, leaving a specific MBMS bearer service area, tracking area change, PLMN change, call initiation, or other types of events such as emergency. The location report can include information described as ECGI, MBMS SAIs, geographic coordinates and other location information.

9.3.3.2 Fetching location reporting configuration

Figure 9.3.3.2-1 illustrates the procedure for fetching location reporting configuration.

Pre-condition:

- If multicast delivery mode is used, the MBMS bearer being used is activated by the location management server.

- The location management client is aware that the location reporting configuration is available at the location management server.
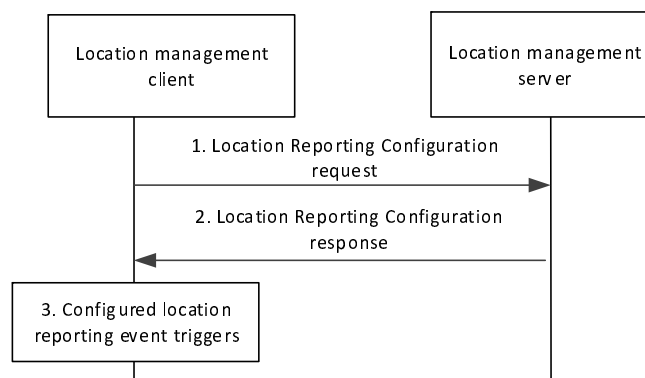
Figure 9.3.3.2-1: Fetching location reporting configuration procedure

1. The location management client sends location reporting configuration request message to the location management server.

2. The location management server sends location reporting configuration message to the location management client(s) containing the initial location reporting event triggers configuration (or a subsequent update) , e.g. minimum time between consecutive reports, SAI changes, or ECGI changes for reporting the location of the VAL UE. This message can be sent over a unicast bearer to a specific location management client or as a group message over an MBMS bearer to update the location reporting configuration for multiple location management clients at the same time.

NOTE 1: The location reporting configuration information can be made part of the user profile, in which case the sending of the message is not necessary.

NOTE 2: Different location management clients may be given different location reporting criteria.

3. The location management client stores or updates the location reporting event triggers configuration. A location reporting event occurs, triggering step 3.

9.3.3.3 Location reporting

Figure 9.3.3.3-1 illustrates the procedure for location reporting.
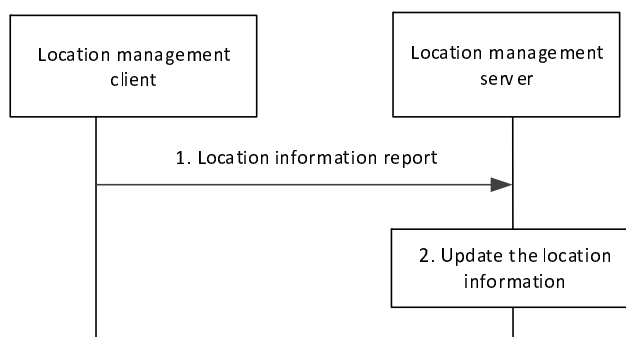
Figure 9.3.3.3-1: Location reporting procedure

1. The location management client sends a location information report to the location management server, containing location information identified by the location management server and available to the location management client.

2. Upon receiving the report, the location management server updates location of the reporting location management client. If the location management server does not have location information of the reporting location management client before, then just stores the reporting location information for that location management client.

9.3.4 On-demand location reporting procedure

The location management server can request UE location information at any time by sending a location information request to the location management client, which may trigger location management client to immediately send the location report.
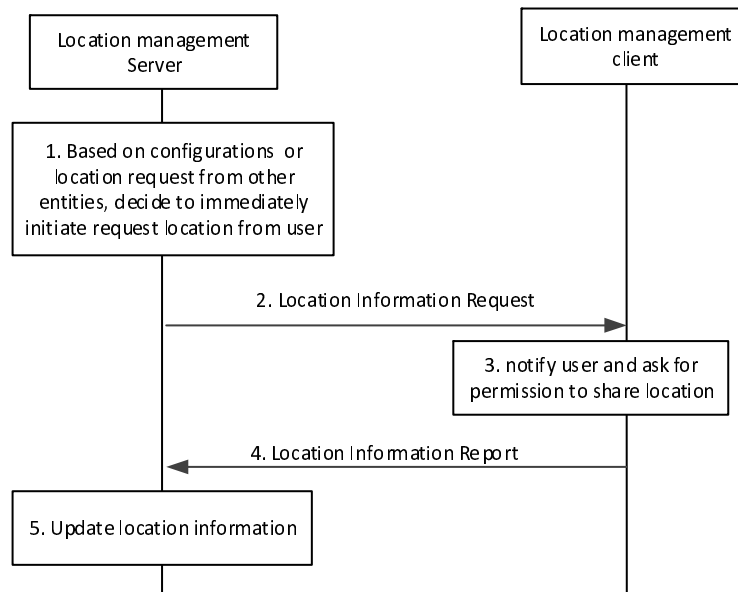
Figure 9.3.4-1: On-demand location information reporting procedure

1. Based on configurations such as periodical location information timer, or location information request from other entities (e.g., another location management client, VAL server), location management server initiates the immediately request location information from the location management client.

2. The location management server sends a location information request to the location management client.

3. VAL user or VAL UE is notified and asked about the permission to share its location. VAL user can accept or deny the request

4. The location management client immediately responds to the location management server with a report containing location information identified by the location management server and available to the location management client.

5. Upon receiving the report, the location management server updates location of the reporting location management client. If the location management server does not have location information of the reporting location management client before, then just stores the reporting location information for that location management client.

9.3.5 Client-triggered or VAL server-triggered location reporting procedure

Figure 9.3.5-1 illustrates the high level procedure of client-triggered or VAL server-triggered location reporting.
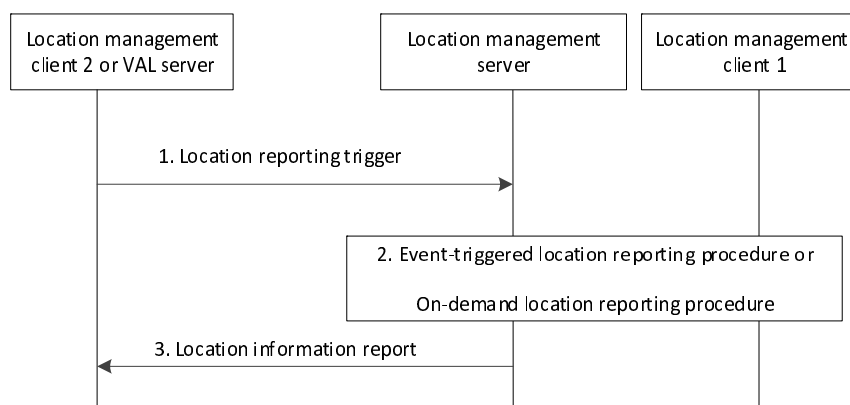
Figure 9.3.5-1: Client-triggered location reporting procedure

1. Location management client 2 (authorized VAL user or VAL UE) or VAL server sends a location reporting trigger to the location management server to activate a location reporting procedure for obtaining the location information of location management client 1.

NOTE: Step 1 can be performed when Location management client 2 or VAL server require to update the location reporting trigger.

2. Location management server checks whether location management client 2 or VAL server is authorized to send a location reporting trigger. Depending on the information specified by the location reporting trigger, location management server initiates an on-demand location reporting procedure or an event-triggered location reporting procedure for the location of location management client 1.

3. Once the location information of the location management client 1 is available in the location management server by the on-demand location reporting procedure, a location information report is sent to the location management client 2 or VAL server.

9.3.6   Location reporting triggers configuration cancel

Figure 9.3.6-1 illustrates the procedure used for cancelling the location reporting triggers configuration at the target Location management client.

Pre-conditions:

1. The location management server has subscribed the location management client 2 location with the location reporting event triggers.

2. If multicast delivery mode is used, the MBMS bearer being used is activated by the location management server.
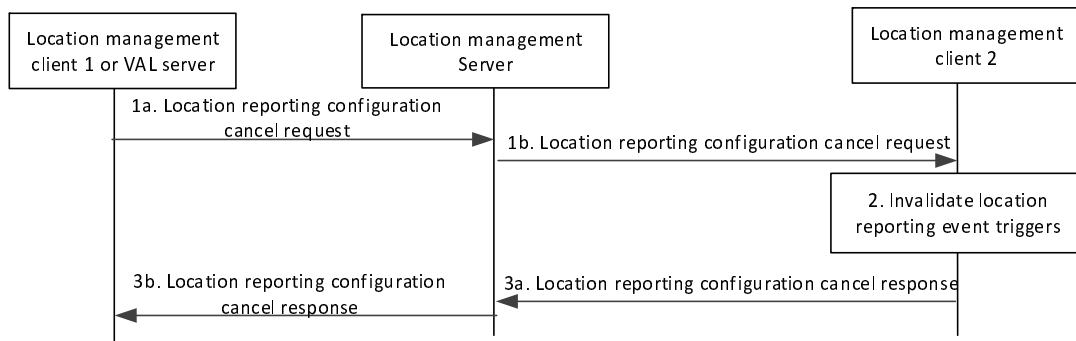
Figure 9.3.6-1: Location reporting triggers configuration cancel

1. The location management client 1 (authorized VAL user or VAL UE) or VAL server sends a location reporting configuration cancel request to the location management server (1a). The location management server sends the location reporting configuration cancel request to the location management client 2 to stop receiving the UE location information (1b). This message can be sent via unicast or multicast.

NOTE: Step 1b can be initiated without step 1a.

2. The location management client invalidates the location reporting triggers configuration and no longer reports its location to the location management server.

3. The location management client 2 sends the location reporting configuration cancel response to the location management server (3a) as an acknowledgement. The location management server sends the location reporting configuration cancel response to the location management client 1 (3b) as an acknowledgement.

9.3.7 Location information subscription procedure

Figure 9.3.7-1 illustrates the high level procedure of location information subscription request. The same procedure can be applied for location management client and other entities that would like to subscribe to VAL user or VAL UE location information. This procedure is also used for intiating tracking a UE's location.
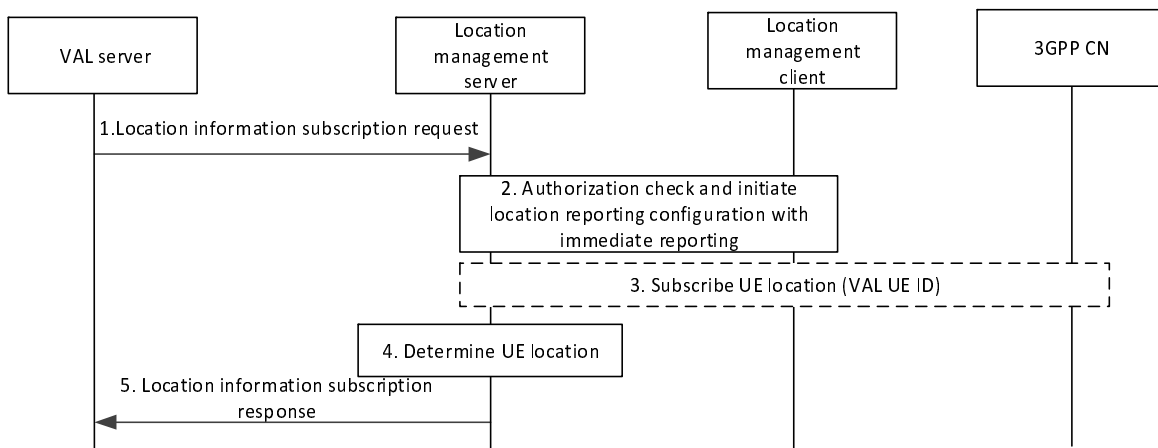
Figure 9.3.7-1: Location information subscription request procedure

1. The VAL server sends a location information subscription request to the location management server to subscribe location information of one or more VAL users or VAL UEs. The request may include an indication for supplementary location information.

2. The location management server shall check if the VAL server is authorized to initiate the location information subscription request. Further, the location management server may initiate location reporting configuration with the location management client of the UE for immediate reporting.

3. The location management server may optionally subscribe for UE location information from 3GPP core network for the UE. If the indication for supplementary location information is included in step 1, then UE location information is obtained from the 3GPP core network.

4. The location management server determines the UE location information of the UE as received in steps 3 and 4.

5. The location management server replies with a location information subscription response indicating the subscription status and if immediate reporting was requested, the location information of the VAL UE(s).

9.3.8 Event-trigger location information notification procedure

Figure 9.3.8-1 illustrates the high level procedure of event-trigger usage of location information. The same procedure can be applied for location management client and other entities that would like to subscribe to location information of VAL user or VAL UE. This procedure is also used for obtaining latest UE's location for tracking purpose.
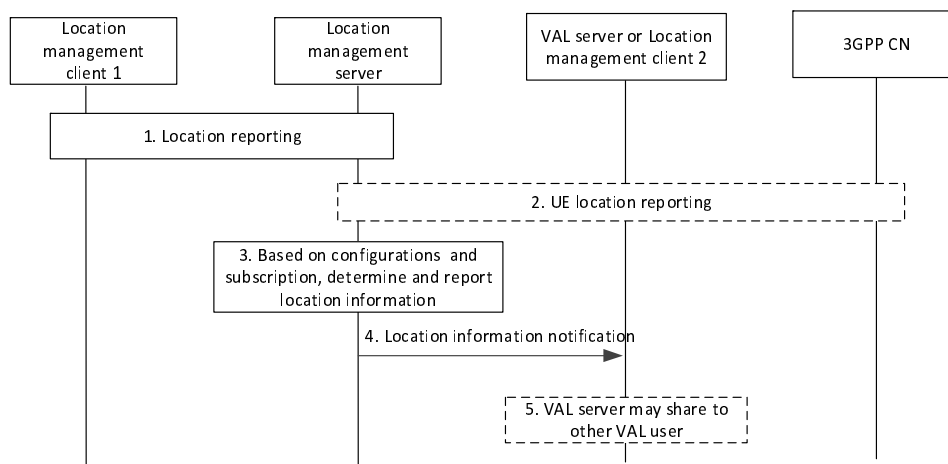
Figure 9.3.8-1: Event-trigger usage of location information procedure

1. The location management server receives the latest location information of the UE as per the location report procedure described in clause 9.3.3.3.

2. The location management server may optionally receive the location information of the UE from 3GPP core network. If the indication for supplementary location information is included in the subscription, then UE location information is obtained from the 3GPP core network.

3. Based on the configurations, e.g., subscription, periodical location information timer, location management server is triggered to report the latest user location information to VAL server. The location management server determines the location information of UE as received in steps 1 and 2, including the supplementary location information (if indicated).

4. The location management server sends the location information report including the latest location information of one or more VAL users or VAL UEs to the VAL server or to the location management client that has previously configured.

5. VAL server may further share this location information to a group or to another VAL user or VAL UE.

NOTE: For other entities, the step 5 can be skipped if not needed.

9.3.9 On-demand usage of location information procedure

The VAL server can request UE location information at any time by sending a location information request to the location management server, which may trigger location management server to immediately send the location report.

Figure 9.3.9-1 illustrates the high level procedure of on demand usage of location information. The same procedure can be applied for location management client and other entities that would like to subscribe to location information of VAL user or VAL UE.
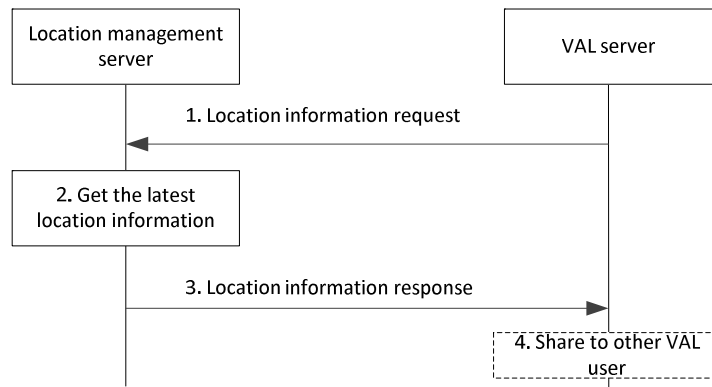
Figure 9.3.9-1: On-demand usage of location information procedure

1. VAL server sends a location information request to the location management server.

2. The location management server acquires the latest location of the UEs being requested, by triggering an on-demand location report procedure as described in subclause 9.3.4, or from PLMN operator.

3. Then, location management server immediately sends the location information report including the latest location information acquired of one or more VAL users or VAL UEs.

4. VAL server may further share this location information to a group or to another VAL user or VAL UE.

NOTE: For other entities, the step 3 can be skipped if not needed.

9.3.10 Obtaining UE(s) information at a location

Figure 9.3.10-1 describes the procedure for obtaining UE(s) information at a location.

Pre-condition:

- The VAL server has a jurisdiction over a geographical area for which the location management server is configured to operate.

- The UE(s) in the geographical area have provided its location information to the location management server.
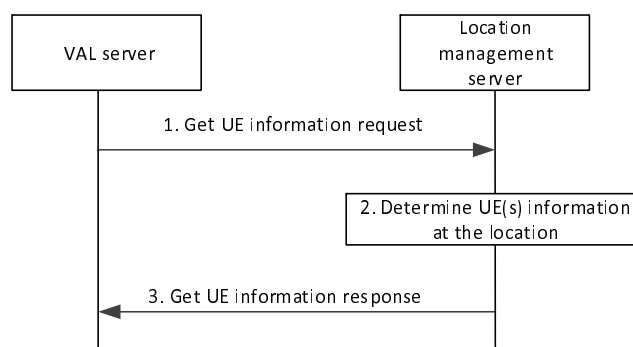
Figure 9.3.10-1: Obtaining UE(s) information at a location

1. The VAL server sends get UE information request to the location management server. The request contains a location information and application defined proximity range.

2. The location management server determines the UE(s) whose location are within the application defined proximity range of the location information provided in step 1.

3. The location management server sends get UE information response to the VAL server with a list of UE(s) and its corresponding location information as determined in step 1.

9.3.11 Monitoring Location Deviation

9.3.11.1 General

The VAL server requests the Location Management Server to monitor the location of the VAL UE in relation to an area of interest. The LMS fetches the VAL UE's location information periodically from 3GPP core network as specified in 3GPP TS 23.502 [11] and also, using the Location Information procedures specified in clause 9.3.7 and clause 9.3.10. With the periodic location information of the UE from 3GPP core network and SEAL procedures, the LMS server evaluates the current location of the VAL UE in relation to the area of interest configured by the VAL server. If subscribed, the VAL server is notified by the LMS server when the VAL UE relationship (e.g. inside or outside) to the area of interest changes along with current location information of the VAL UE.

9.3.11.2 Monitoring Location Deviation procedure

Figure 9.3.11.2-1 describes the procedure for monitoring the VAL UE's location in a given area of interest.

Pre-condition:

- The LMS server authorized to consume the 3GPP core network service (Monitoring events as specified in 3GPP TS 23.502 [11]).
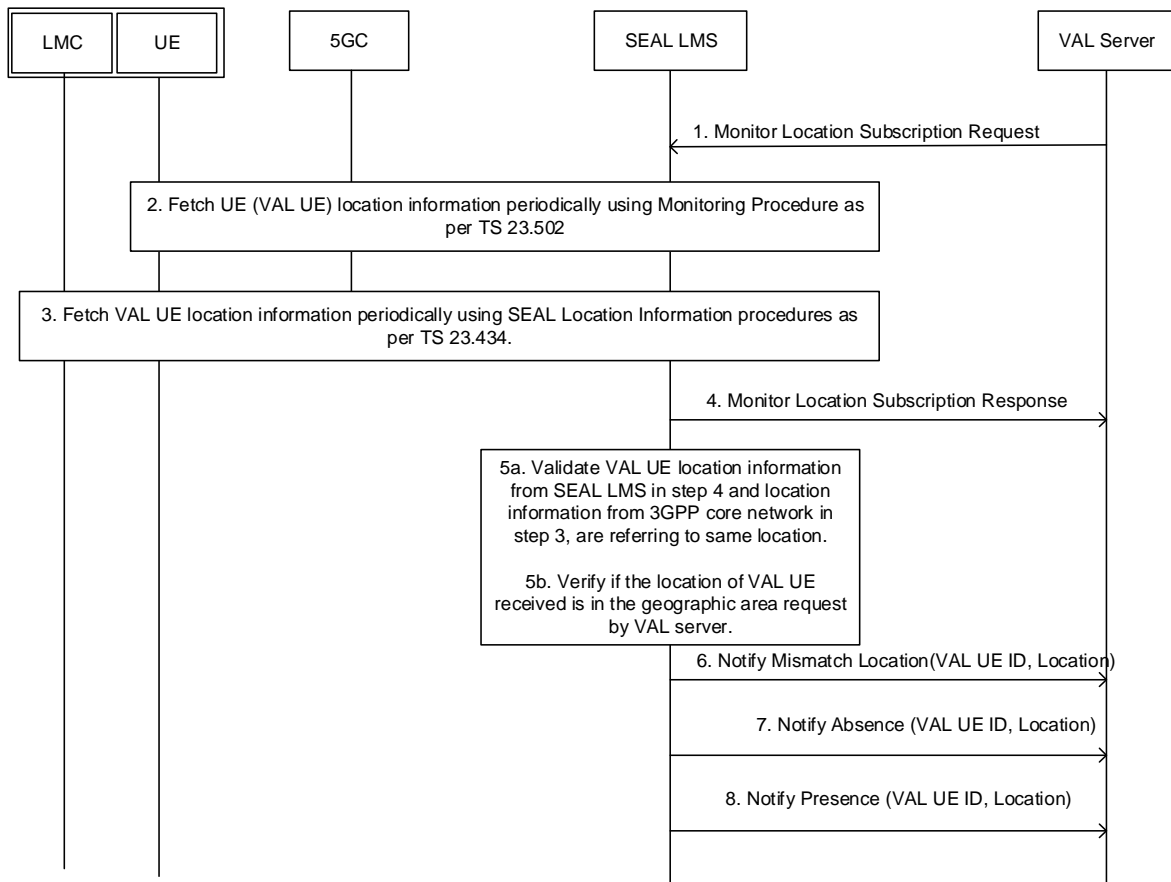
Figure 9.3.11.2-1: Monitoring VAL UE's location at a given location

1. The VAL server sends Monitor Location Subscription Request to LMS server including VAL UE Identifier, predetermined area of interest information, notification interval and notification URI where the VAL server intends to receive the notifications from LMS server regarding VAL UE's presence in a given area.

   - "Area of interest" is the location information, which the VAL server wishes to monitor the VAL UE's location adherence. This parameter can include an area of interest information and other relevant parameters.

   - "Notify_Interval" represents the periodic interval in which the LMS server needs to notify VAL UE's location information to the VAL server. When the VAL UE moves away from the " Area of interest", then the LMS server ignores the "Notify_Interval" and sends the location notification to the VAL server immediately.

2. LMS processes the Area of interest information in the request, and then subscribes to UE location monitoring as specified in 3GPP TS 23.502 [11] with appropriate parameters mapping. Based on the subscription, the LMS receives the VAL UE location information periodically from the 3GPP core network.

Editor's note: How the LMS's processing of Area of Interest information and the subscription of UE location monitoring based on Area of Interest are related with procedures in 3GPP TS 23.502 and 3GPP TS 23.256 are FFS.

3. LMS shall use the Location information procedures as specified in clause 9.3.7 and clause 9.3.10, to periodically obtain the VAL UE location information. Based on the geographic information from the VAL server, the LMS server may determine to additionally include the positioning methods in SEAL LMS procedures to obtain location information.

4. LMS server, after successful subscription according to steps 2 and 3, sends Monitor Location Subscription response, indicating that the LMS server accepts VAL server's request and will monitor the location of the VAL UE to verify if the VAL UE is in the area of interest.

5a and 5b. LMS server processes the location information received from SEAL Location Information procedures and the core network, and validates the information. If the location information is matching, then the LMS shall check if the VAL UE's current location is within the area of interest received in step 1. The LMS will continue with step 6, step 7 and step 8 as applicable.

6. If the location information received from Location management client and the core network do not match, then the LMS server shall consider the VAL UE as outside from its specified area of interest and shall notify ("Notify Mismatch Location" message) the VAL server of the same, including VAL UE ID and the location information from LMS and the core network in the notification message.

7. If the VAL UE's current location is from Location management client and the core network matches, and not in the area of interest received from VAL server in Monitor Location Subscription Request message, then the LMS considers the VAL UE as outside from its specified area of interest and shall notify the VAL server that the VAL UE's current location is outside of area of interest and VAL UE ID in "Notify Absence" message.

8. When the VAL UE's current location is in area of interest, then the LMS shall notify ("Notify Presence" message) the VAL server periodically, according to the "Notify_Interval" value in "Monitor Location Subscription Request" message, indicating the VAL server that the VAL UE is within the area of interest, along with VAL UE's current location information.

9.3.12   Location area monitoring information procedure

9.3.12.1   Location area monitoring subscribe procedure

Figure 9.3.12.1-1 illustrates the high level procedure of location area monitoring subscription request. The same procedure can be applied for location management client and other SEAL servers that would like to subscribe to the list of UEs moving in or moving out of the specific location area. The subscribe request can be for a reference UE for which the subscriber is authorized to monitor location information.
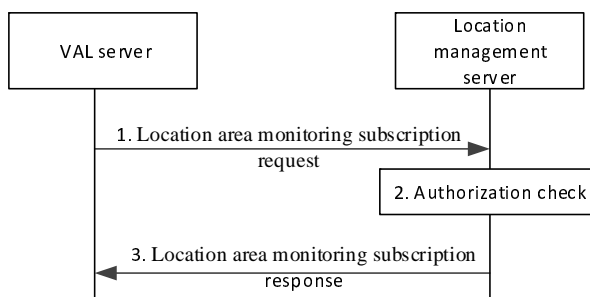
Figure 9.3.12.1-1: Location area monitoring subscription procedure

1. The VAL server sends a location area monitoring subscription request to the location management server to subscribe to the list of UEs moving in or moving out of the specific location area. In the request message, the VAL server includes the information as specified in Table 9.3.2.14-1. The location information criteria may include the geographic location information where the UEs moving in or moving out to be monitored, or it may include reference UE information where in the UEs moving in or moving out of given application defined proximity range from the reference UE (target UE) to be monitored. The reference UE information may include VAL UE ID.

2. The location management server shall check if the VAL server is authorized to initiate the location area monitoring subscription request.

3. The location management server replies with a location area monitoring subscription response indicating the subscription status. In the response message, the location management server includes the information as specified in Table 9.3.2.15-1.

9.3.12.2 Location area monitoring subscribe modify procedure

Figure 9.3.12.2-1 illustrates the high level procedure of location area monitoring subscribe modify request. The same procedure can be applied for location management client and other SEAL servers that would like to modify the subscription to the list of UEs moving in or moving out of the specific location area. The subscribe modify request can be for a reference UE for which the subscriber is authorized to monitor location information.
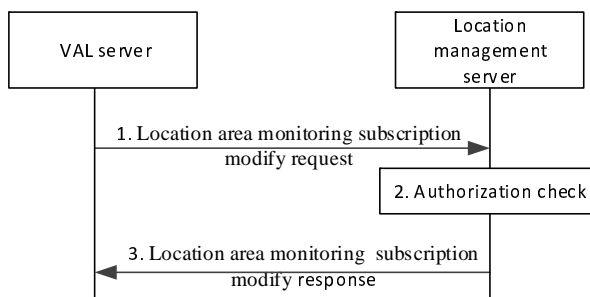
Figure 9.3.12.2-1: Location area monitoring subscription modify procedure

1. The VAL server sends a location area monitoring subscription modify request to the location management server to modify the subscription to the list of UEs moving in or moving out of the specific location area. In the request message, the VAL server includes the information as specified in Table 9.3.2.17-1.

2. The location management server shall check if the VAL server is authorized to initiate the location area monitoring subscription modification request.

3. The location management server replies with a location area monitoring subscription modify response indicating the subscription status. In the response message, the location management server includes the information as specified in Table 9.3.2.18-1.

9.3.12.3 Location area monitoring unsubscribe procedure

Figure 9.3.12.3-1 illustrates the high level procedure of location area monitoring unsubscribe request. The same procedure can be applied for location management client and other SEAL servers that would like to unsubscribe to the

list of UEs moving in or moving out of the specific location area. The unsubscribe request can be for a reference UE for which the subscriber is authorized to monitor location information.
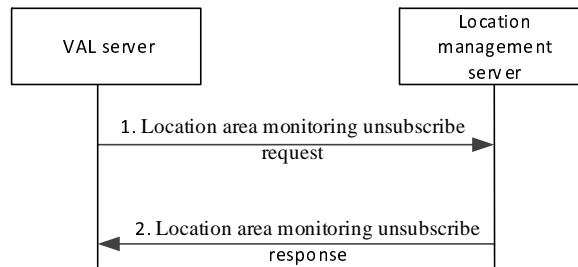
Figure 9.3.12.3-1: Location area monitoring unsubscribe procedure

1. The VAL server sends a location area monitoring unsubscrbe request to the location management server to unsubscribe to the subscription to the list of UEs moving in or moving out of the specific location area. In the request message, the VAL server includes the information as specified in Table 9.3.2.19-1.

2. The location management server replies with a location area monitoring unsubscrbe response indicating the subscription status. In the response message, the location management server includes the information as specified in Table 9.3.2.20-1.

9.3.12.4 Location area monitoring notification procedure

Figure 9.3.12.4-1 illustrates the high level procedure of location area monitoring notification. The same procedure can be applied for location management client and other SEAL servers who have subscribe to the list of the UEs moving in or moving out of the specific location area.
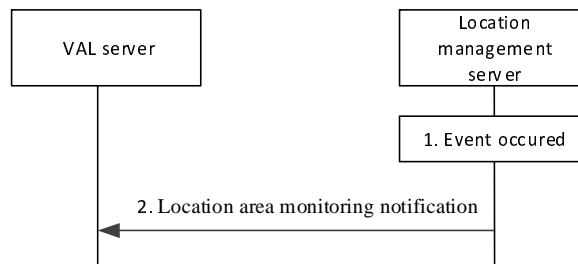
Figure 9.3.12.4-1: Location are monitoring notification procedure

1. One of the events occurs at the location management server as specified in the subscribe request. The location management server identifies the UEs which are moved into the area or moved out of the area based on their location data and time stamp of the location. The LMS may report the list of all UEs in the given location or UEs moved in and moved out.

2. The location management server sends a location area monitoring notification to the VAL server. In the notification message, the location management server includes the information as specified in Table 9.3.2.16-1.

9.4 SEAL APIs for location management

9.4.1 General

Table 9.4.1-1 illustrates the SEAL APIs for location management.

Table 9.4.1-1: List of SEAL APIs for location management

API Name	API Operations	Known Consumer(s)	Communication Type
SS_LocationReporting	Create_Trigger_Location_Reporting Update_Trigger_Location_Reporting Cancel_Trigger_Location_Reporting	VAL server	Request /Response
SS_LocationInfoEvent	Subscribe_Location_Info	VAL server	Subscribe/Notify
	Notifiy_Location_Info	VAL server	
SS_LocationInfoRetrieval	Obtain_Location_Info	VAL server	Request /Response
SS_LocationAreaInfoRetrieval	Obtain_UEs_Info	VAL server	Request/Response
SS_LocationMonitoring	Subscribe_Location_Monitoring	VAL server	Subscribe/Notify
	Notify_Location_Monitoring_Events	VAL server	

9.4.2   SS_LocationReporting API

9.4.2.1   General

API description: This API enables the VAL server to trigger reporting of location information to the location management server over LM-S.

9.4.2.2   Create_Trigger_Location_Reporting operation

API operation name: Create_Trigger_Location_Reporting

Description: Creates the trigger to report location information.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.4

Outputs: Refer subclause 9.3.2.4

See subclause 9.3.5 for the details of usage of this API operation.

9.4.2.3   Update_Trigger_Location_Reporting operation

API operation name: Update_Trigger_Location_Reporting

Description: Updates the trigger to report location information.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.4

Outputs: Refer subclause 9.3.2.4

See subclause 9.3.5 for the details of usage of this API operation.

9.4.2.4   Cancel_Trigger_Location_Reporting operation

API operation name: Cancel_Trigger_Location_Reporting

Description: Cancels the trigger to report location information.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.8

Outputs: Refer subclause 9.3.2.8

See subclause 9.3.6 for the details of usage of this API operation.

9.4.3 SS_LocationInfoEvent API

9.4.3.1 General

API description: This API enables the VAL server to subscribe and receive the UEs location information from the location management server over LM-S.

9.4.3.2 Subscribe_Location_Info operation

API operation name: Subscribe_Location_Info

Description: Subscription to the location information.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.5

Outputs: Refer subclause 9.3.2.6

See subclause 9.3.7 for the details of usage of this API operation.

9.4.3.3 Notify_Location_Info operation

API operation name: Notify_Location_Info

Description: Location information notification to the existing subscription.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.7

Outputs: Refer subclause 9.3.2.7

See subclause 9.3.8 for the details of usage of this API operation.

9.4.4 SS_LocationInfoRetrieval API

9.4.4.1 General

API description: This API enables the VAL server to obtain UEs location information from the location management server over LM-S.

9.4.4.2 Obtain_Location_Info operation

API operation name: Obtain_Location_Info

Description: Request UEs location information.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.3

Outputs: Refer subclause 9.3.2.2

See subclause 9.3.9 for the details of usage of this API operation.

9.4.5 SS_LocationAreaInfoRetrieval API

9.4.5.1 General

API description: This API enables the VAL server to obtain UE(s) information in an application defined proximity range of a location from the location management server over LM-S.

9.4.5.2 Obtain_UEs_Info operation

API operation name: Obtain_UEs_Info

Description: Request UEs information in an application defined proximity range of a location.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.9

Outputs: Refer subclause 9.3.2.10

See subclause 9.3.10 for the details of usage of this API operation.

9.4.6 SS_LocationMonitoring API

9.4.6.1 General

API description: This API enables the VAL server to monitor the VAL UE's location in a given area of interest, from the location management server over LM-S.

9.4.6.2 Subscribe_Location_Monitoring

API operation name: Subscribe_Location_Monitoring

Description: Subscription to location monitoring.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.11

Outputs: 9.3.2.12.

See subclause 9.3.11.2 for the details of usage of this API operation.

9.4.6.3 Notify_Location_Monitoring_Events

API operation name: Notify_Location_Monitoring_Events

Description: Notifying the VAL server with the location monitoring events related to VAL UE.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.13

Outputs: None.

See subclause 9.3.11.2 for the details of usage of this API operation.

9.4.7 SS_LocationAreaMonitoring API

9.4.7.1 General

API description: This API enables the VAL server to monitor the list of UEs moving in or moving out of the specific location area.

9.4.7.2 Subscribe_Location_Area_Monitoring

API operation name: Subscribe_Location_Area_Monitoring

Description: Subscription to location area monitoring.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.14

Outputs: 9.3.2.15.

See subclause 9.3.12.1 for the details of usage of this API operation.

9.4.7.3 Notify_Location_Area_Monitoring_Events

API operation name: Notify_Location_Area_Monitoring_Events

Description: Notifying the VAL server with the list of UEs moved in or moved out of the specific location area.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.16

Outputs: None.

See subclause 9.3.12.4 for the details of usage of this API operation.

9.4.7.4 Update_Location_Area_Monitoring_Subscribe

API operation name: Update_Location_Area_Monitoring_Subscribe

Description: Updates subscription to location area monitoring.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.17

Outputs: See subclause 9.3.2.18

See subclause 9.3.12.2 for the details of usage of this API operation.

9.4.7.5 Unsubscribe_Location_Area_Monitoring

API operation name: Unsubscribe_Location_Area_Monitoring

Description: Unsubscribing from location area monitoring.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.19

Outputs: See subclause 9.3.2.20

See subclause 9.3.12.3 for the details of usage of this API operation.

9.5 Procedures and information flows for Location management (Off-network)

9.5.1 General

Location information of VAL service user shall be provided by the location management client of one UE to the location management client of another UE. The location information reporting triggers are based on the location reporting configuration. Different type of location information can be provided e.g. retrieved from non-3GPP source.

NOTE: VAL clients sharing location information directly at vertical enabler layer is outside the scope of this specification.

Editor's note: Adding architecture requirement(s) for off-network location management is FFS.

Editor's note: Charging aspects for off-network location management is FFS.

9.5.2 Information flows for off network location management

9.5.2.1 Off-network location reporting trigger configuration

Table 9.5.2.1-1 describes the information flow from the location management client-1 to the location management client-2 for the off-network location reporting configuration.

Table 9.5.2.1-1: Off-network location reporting trigger configuration

Information element	Status	Description
Identity	M	Identity of the VAL user to which the location reporting configuration is targeted or identity of the VAL UE.
Requested location information	M	Identifies what location information is requested
List of triggering criteria(s)	M	One or more triggering criteria that identifies when the location management client will send the location report. Each triggering criteria is identified by trigger-id.
Minimum time between consecutive reports	O	Defaults to 0 if absent otherwise indicates the time interval between consecutive reports
Life Time of the configuration	O	Time till when location report configurations are valid.

9.5.2.2 Off-network location reporting trigger configuration response

Table 9.5.2.2-1 describes the information flow from the location management client-2 to the location management client-1 for the off-network location reporting configuration response. The Off-network location reporting trigger configuration response acts as an acknowledgement to the location management client-1.

Table 9.5.2.2-1: Off-network location reporting trigger configuration response

Information element	Status	Description
Result	M	Indicates the success or failure for the operation
Cause	O	Provides reason for the failure.

9.5.2.3 Off-network location management ack

The Off-network location management ack message is sent from the message receiver location management client-2 to message originator location management client-1.

9.5.2.4 Off-network location report

Table 9.5.2.4-1 describes the information flow from the location management client-2 to the location management client-1 for the off-network location report.

Table 9.5.2.4-1: Off-network location report

Information element	Status	Description
Triggering event	M	Identity of the event that triggered the sending of the report
Location Information	M	Location information shared by VAL client e.g. retrieved from non-3GPP source
Acknowledgement Required	O	If present, indicate the recipient of the message to acknowledge the message.

9.5.2.5 Off-network location reporting trigger cancel

Table 9.5.2.5-1 describes the information flow from the location management client-1 to the location management client-2 for the off-network location reporting trigger cancel.

Table 9.5.2.5-1: Off-network location reporting trigger cancels

Information element	Status	Description
Identity	M	Identity of the VAL user to which the location reporting trigger cancel is targeted or identity of the VAL UE.

9.5.2.6 Off-network location reporting trigger cancel response

Table 9.5.2.6-1 describes the information flow from the location management client-2 to the location management client-1 for the off-network location reporting cancel response. The Off-network location reporting trigger cancel response acts as an acknowledgement to the location management client-1.

Table 9.5.2.6-1: Off-network location reporting trigger cancel response

Information element	Status	Description
Result	M	Indicates the success or failure for the operation

9.5.2.7 Off-network location request

Table 9.5.2.7-1 describes the information flow from the location management client-1 to the location management client-2 for the off-network location request.

Table 9.5.2.7-1: Off-network location request

Information element	Status	Description
Identity	M	Identity of the VAL user to which the location request is targeted or identity of the VAL UE.
Requested location information	M	Identifies what location information is requested

9.5.2.8 Off-network location response

Table 9.5.2.8-1 describes the information flow from the location management client-2 to the location management client-1 for the off-network location response. The Off-network location response acts as an acknowledgement to the location management client-1.

Table 9.5.2.8-1: Off-network location response

Information element	Status	Description
Result	M	Indicates the success or failure for the operation
Location Information	M	Location information shared by VAL client e.g. retrieved from non-3GPP source

9.5.3 Event-triggered location reporting procedure

9.5.3.1 Location reporting trigger configuration

Figure 9.5.3.1-1 illustrates the procedure for configuring location reporting triggers from the location management client-1 residing in UE-1 to the location management client-2 residing in UE-2.

Pre-condition:

- The UE-1 and UE-2 are within PC5 communication range of each other, and aware of Layer-2 ID of each other.

- The VAL service user in UE-1 is authorized to configure location reporting trigger to the UE-2.

- The VAL service user in UE-1 requests to configure location reporting triggers to the UE-2.
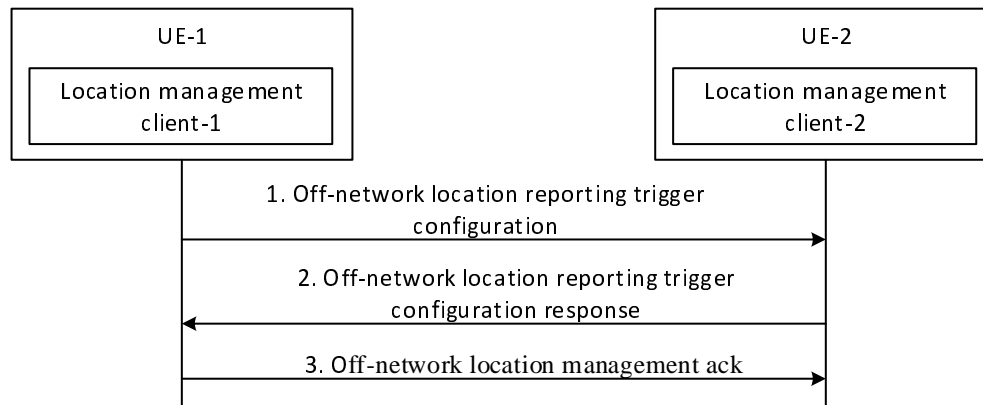
Figure 9.5.3.1-1: Location reporting trigger configuration

1. The location management client-1 in UE-1 sends off network location reporting trigger configuration message to the location management client-2 in UE-2 containing the initial location reporting event triggers configuration (or a subsequent update) for reporting the location of the VAL UE. The message includes information elements as specified in Table 9.5.2.1-1.

2. The location management client-2 stores the location reporting configuration, and sends off network location reporting trigger configuration response to the location management client-1. The message includes information elements as specified in Table 9.5.2.2-1.

3. Upon receiving the off network location reporting trigger configuration response message, the location management client-1 sends off-network location management ack messages. The message includes information elements as specified in clause 9.5.2.3.

9.5.3.2 Location reporting

Figure 9.5.3.2-1 illustrates the procedure for sending off-network location report from the location management client-2 residing in UE-2 to the location management client-1 residing in UE-1.

Pre-condition:

- The UE-1 and UE-2 are within PC5 communication range of each other, and aware of Layer-2 ID of each other.

- The location management client-1 has previously configured off-network location reporting triggers to the location management client-2 as specified in clause 9.5.3.1.
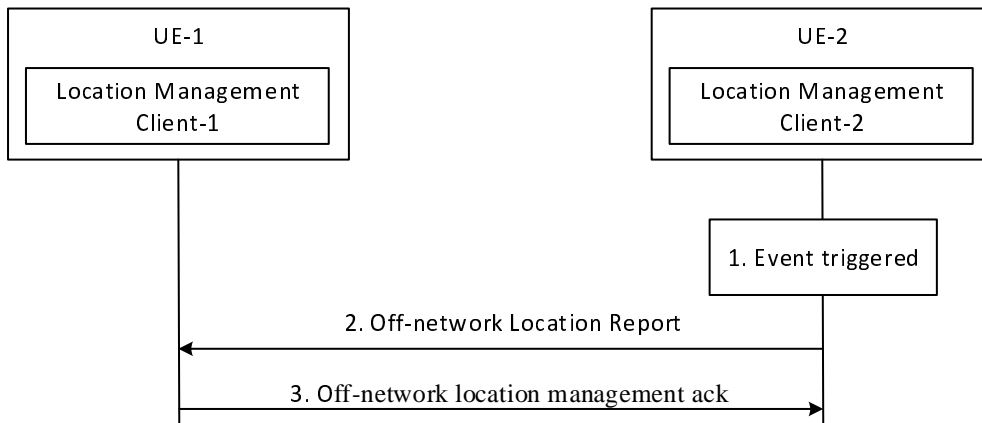
Figure 9.5.3.2-1: Location reporting

1. The location management client-2 is monitoring the location reporting triggers and one of the event is triggered.

2. The location management client-2 sends the off-network location report message. The message includes information elements as specified in Table 9.5.2.4-1.

3. Upon receiving the off network location report message, the location management client-1 sends the off-network location management ack message if requested in the received message. The message includes information elements as specified in clause 9.5.2.3.

9.5.3.3 Location reporting trigger cancel

Figure 9.5.3.3-1 illustrates the procedure for sending off-network location reporting trigger cancel from the location management client-1 residing in UE-1 to the location management client-2 residing in UE-2.

Pre-condition:

- The UE-1 and UE-2 are within PC5 communication range of each other, and aware of Layer-2 ID of each other.

- The location management client-1 has previously configured location reporting triggers to the location management client-2 as specified in clause 9.5.3.1.
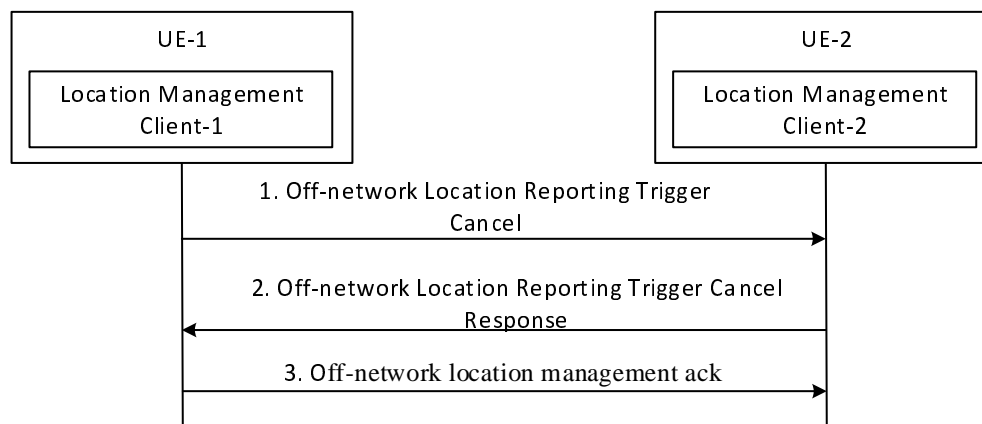
Figure 9.5.3.3-1: Location reporting trigger cancel

1. The location management client-1 in UE-1 sends off network location reporting trigger cancel message to the location management client-2 in UE-2 to cancel the location reporting trigger configuration. The message includes information elements as specified in Table 9.5.2.5-1.

2. The location management client-2 clears the location reporting configuration, and sends off network location reporting trigger cancel response to the location management client-1. The message includes information elements as specified in Table 9.5.2.6-1.

3. Upon receiving the off network location reporting trigger configuration response message, the location management client-1 sends off-network location management ack message. The message includes information elements as specified in clause 9.5.2.3.

9.5.4 On-demand location reporting procedure

Figure 9.5.4-1 illustrates the procedure for on-demand location report from the location management client-1 residing in UE-1 to the location management client-2 residing in UE-2.

Pre-condition:

- The UE-1 and UE-2 are within PC5 communication range of each other, and aware of Layer-2 ID of each other.

- The VAL service user in UE-1 is authorized to request location report from the UE-2.

- The VAL service user in UE-1 requests immediate location reporting to the UE-2.
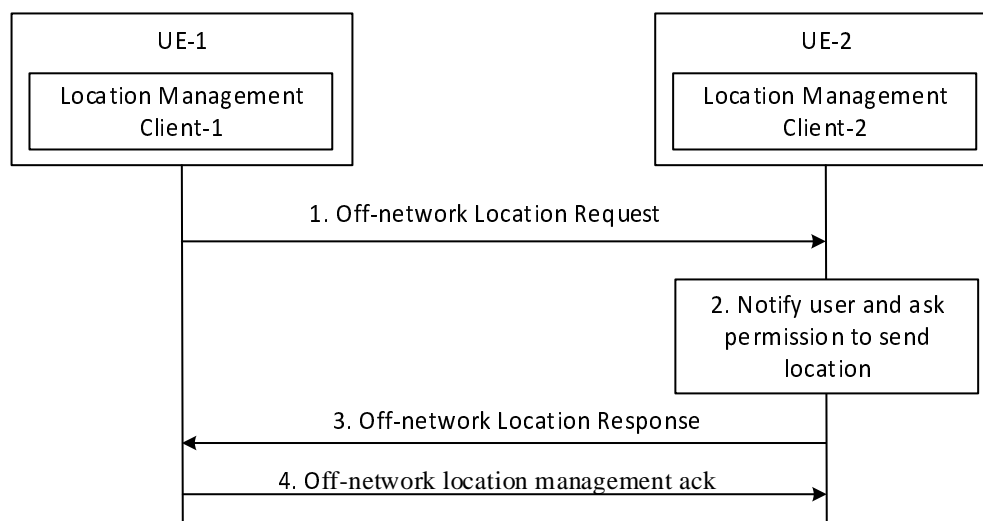
Figure 9.5.4-1: Location reporting trigger cancel

1. Based on configurations such as periodical location information timer the location management client-1 initiates the immediately request location information from the location management client-2. The location management client sends an off-network location request to the location management client-2. The message includes information elements as specified in Table 9.5.2.7-1.

2. VAL user or VAL UE is notified and asked about the permission to share its location. VAL user can accept or deny the request

3. The location management client-2 immediately responds to the location management client-1. If permission is received from the VAL user, the location management client-2 includes a report containing location information identified by the location management client-1 and available to the location management client-2. The message includes information elements as specified in Table 9.5.2.8-1.

4. Upon receiving the off network location reporting trigger configuration response message, the location management client-1 sends off-network location management ack message. The message includes information elements as specified in clause 9.5.2.3

10 Group management

10.1 General

The group management is a SEAL service that offers the group management related capabilities to one or more vertical applications.

10.2 Functional model for group management

10.2.1 General

The functional model for the group management is based on the generic functional model specified in clause 6. It is organized into functional entities to describe a functional architecture which addresses the support for group management aspects for vertical applications. The on-network and off-network functional model is specified in this clause.

10.2.2 On-network functional model description

Figure 10.2.2-1 illustrates the generic on-network functional model for group management.
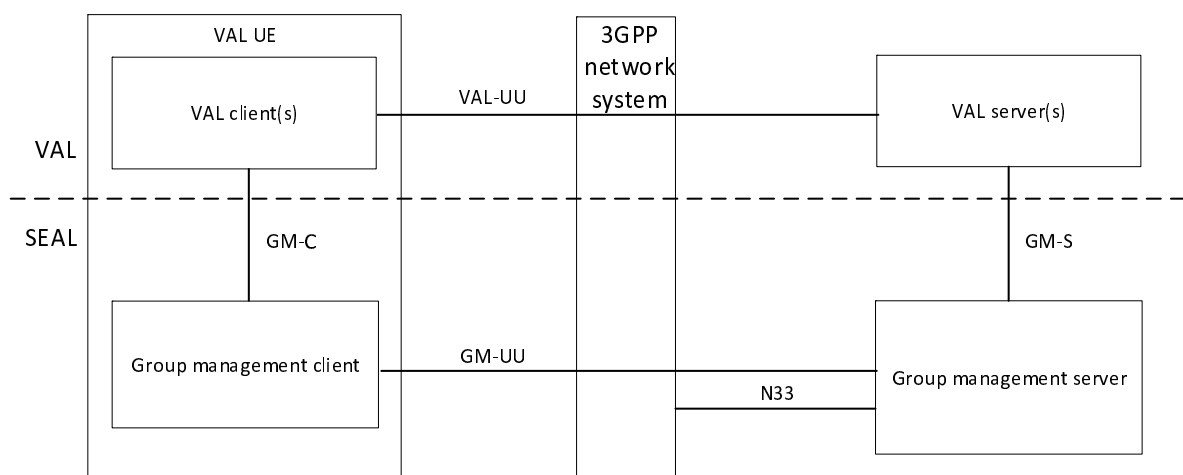
Figure 10.2.2-1: On-network functional model for group management

The group management client communicates with the group management server over the GM-UU reference point. The group management client provides the support for group management functions to the VAL client(s) over GM-C reference point. The VAL server(s) communicate with the group management server over the GM-S reference point.

The group management server interacts with the NEF of the underlying 3GPP network system via N33 reference point to perform group management procedures for 5G Virtual Network (5GVN) groups.

10.2.3 Off-network functional model description

Figure 10.2.3-1 illustrates the off-network functional model for group management.
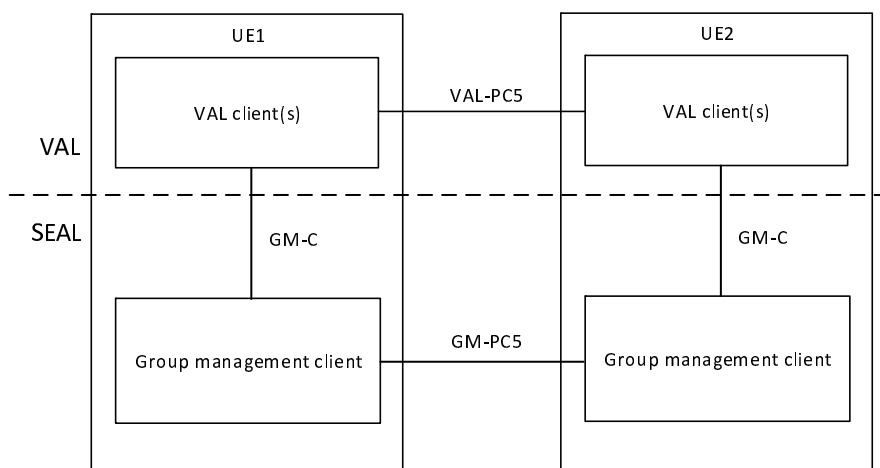
Figure 10.2.3-1: Off-network functional model for group management

The group management client of the UE1 communicates with the group management client of the UE2 over the GM-PC5 reference point.

10.2.4 Functional entities description

10.2.4.1 General

The functional entities for group management SEAL service are described in the following subclauses.

10.2.4.2 Group management client

The group management client functional entity acts as the application client for management of groups. A VAL system maintains groups corresponding to one or more vertical applications. The group management client interacts with the group management server. The group management client also supports interactions with the corresponding group management client between the two UEs.

The group management client functional entity is supported by the signalling user agent and HTTP client functional entities of the signalling control plane.

10.2.4.3 Group management server

The group management server functional entity provides for management of groups supported within the vertical application layer. The group management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The group management server also supports interactions with the corresponding group management server in distributed SEAL deployments.

The group management server functional entity is supported by the SIP AS and HTTP server functional entities of the signalling control plane.

All the group management clients supporting users belonging to a single group are required to use the same group management server for that group. A group management client supporting a user involved in multiple groups can have relationships with multiple group management servers.

10.2.5 Reference points description

10.2.5.1 General

The reference points for the functional model for group management are described in the following subclauses.

10.2.5.2 GM-UU

The interactions related to group management functions between the group management client and the group management server are supported by GM-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

GM-UU reference point is used for VAL service signalling for VAL service data management of the VAL service. The GM-UU reference point supports:

- Configuration of group related data at the group management client by the group management server; and

- Configuration of group related data at the group management server by the group management client.

The GM-UU reference point uses the HTTP-1/HTTP-2 reference points for transport and routing of group management related signalling. The GM-UU reference point uses the SIP-1/SIP-2 reference points for subscription/notification related signalling.

10.2.5.3 GM-PC5

The interactions related to group management functions between the group management clients located in different VAL UEs are supported by GM-PC5 reference point. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [12].

10.2.5.4 GM-C

The interactions related to group management functions between the VAL client(s) and the group management client within a VAL UE are supported by GM-C reference point.

10.2.5.5 GM-S

The interactions related to group management functions between the VAL server(s) and the group management server are supported by GM-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

GM-S reference point supports the VAL server to obtain group information corresponding to the VAL service. The GM-S reference point uses HTTP-1/HTTP-2 reference points for transport and routing of group management related signalling. The GM-S reference point uses SIP-2 reference point for subscription/notification related signalling.

10.2.5.6 GM-E

The interactions related to group management functions between the group management servers in a distributed deployment are supported by GM-E reference point.

Editor's Note: The functions enabled over GM-E reference point is FFS.

10.2.5.7 N33

For group management procedures pertaining to a 5GVN group the group management server interacts with the NEF of the underlying 3GPP network using the dynamic 5G Virtual Network group management procedures exposed by the NEF via the N33 reference point, as specified in TS 23.501 [10] and in TS 23.502 [11].

10.3 Procedures and information flows for group management

10.3.1 General

Group management procedures apply to on-network VAL service only.

Group creation provides a dedicated VAL group to individual VAL users to enable the required communication for one or multiple VAL services. This includes the normal group creation by administrators or by authorized user/UE. The

group management server supports the external group identifier within the VAL group document to enable the SEAL servers to consume the NEF services for the member UEs of the VAL group.

NOTE: If an authorized VAL user/UE wants to participate in a new group created by the authorized VAL user/UE, then the authorized VAL user/UE needs to have been included in the new group as a member.

10.3.2 Information flows for group management

10.3.2.1 Group creation request

Table 10.3.2.1-1 describes the information flow group creation request from the group management client to the group management server.

Table 10.3.2.1-1: Group creation request

Information element	Status	Description
Requester Identity	M	The identity of the group management client performing the request.
Identity list	M	List of VAL user IDs or VAL UE IDs that are part of the group to be created corresponding to the list of the configured services
VAL service ID list (see NOTE 1)	O	List of VAL services whose service communications are to be enabled on the group.
VAL service specific information (see NOTE 2)	O	Placeholder for VAL service specific information
NOTE 1: This information element shall be included in the message for creating a group configured for multiple VAL services.		
NOTE 2: The details of this information element are specified in VAL service specific specification and are out of scope of the present document.		

10.3.2.2 Group creation response

Table 10.3.2.2-1 describes the information flow group creation response from the group management server to the group management client.

Table 10.3.2.2-1: Group creation response

Information element	Status	Description
VAL group ID	M (see NOTE)	VAL group ID of the group
Result	M	Indicates the success or failure for the operation
NOTE: If the Result information element indicates failure then the value of VAL group ID information element has no meaning.		

10.3.2.3 Group creation notification

Table 10.3.2.3-1 describes the information flow group creation notification from the group management server to the VAL server(s) and the group management clients.

NOTE: When group is configured for multiple VAL services, the group creation notification message is sent from the group management server to the VAL servers configured for the group.

Table 10.3.2.3-1: Group creation notification

Information element	Status	Description
VAL group ID	M	VAL group ID that was created based on the VAL user ID list and the VAL services enabled on them
Identity list	M	List of VAL user IDs or VAL UE IDs that are part of the created group
VAL service specific information (see NOTE)	O	Placeholder for VAL service specific information
NOTE: The details of this information element are specified in VAL service specific specification and are out of scope of the present document.		

10.3.2.4 Group information query request

Table 10.3.2.4-1 describes the information group information query request from group management client to group management server.

Table 10.3.2.4-1: Group information query request

Information element	Status	Description
Identity	M	The identity of the VAL user or VAL UE performing the query.
VAL group ID	M	The identity of the VAL group to be queried.
Query type	M	It indicates the query type, i.e., membership information.

10.3.2.5 Group information query response

Table 10.3.2.5-1 describes the information flow group information query response from group management server to group management client.

Table 10.3.2.5-1: Group information query response

Information element	Status	Description
VAL group ID	M (see NOTE)	The identity of the VAL group to be queried.
Query type	M (see NOTE)	It indicates the query type, e.g. membership information.
Query result	M (see NOTE)	The group information retrieved from the group management server based on the query type, i.e., a list of group members.
Result	M	Indicates the success or failure for the operation
NOTE: If the Result information element indicates failure then the values of other information elements have no meaning.		

10.3.2.6 Group membership update request

Table 10.3.2.6-1 describes the information flow group membership update request from the group management client to the group management server.

Table 10.3.2.6-1: Group membership update request

Information element	Status	Description
Requester Identity	M	The identity of the group management client performing the request.
VAL group ID	M	Identity of the VAL group
Identity	M	List of identities of the VAL users and VAL UEs affected by this operation
Operations	M	Add to or delete from the group
VAL service specific information (see NOTE)	O	Placeholder for VAL service specific information
NOTE: The details of this information element are specified in VAL service specific specification and are out of scope of the present document.		

10.3.2.7 Group membership update response

Table 10.3.2.7-1 describes the information flow group membership update response from the group management server to the group management client.

Table 10.3.2.7-1: Group membership update response

Information element	Status	Description
VAL group ID	M	Identity of the VAL group
Result	M	Indicates the success or failure for the operation

10.3.2.8 Group membership notification

Table 10.3.2.8-1 describes the information flow group membership notification from the group management server to the VAL server.

Table 10.3.2.8-1: Group membership notification

Information element	Status	Description
VAL group ID	M	Identity of the VAL group
Identity	M	List of identities of the VAL users and VAL UEs affected by this operation
Operations	M	Add to or delete from the group
VAL service specific information (see NOTE)	O	Placeholder for VAL service specific information
NOTE: The details of this information element are specified in VAL service specific specification and are out of scope of the present document.		

Table 10.3.2.8-2 describes the information flow group membership notification from the group management server to the group management client.

Table 10.3.2.8-2: Group membership notification

Information element	Status	Description
VAL group ID	M	Identity of the VAL group
Operations	M	Add to or delete from the group

10.3.2.9 Group deletion request

Table 10.3.2.9-1 describes the information flow group deletion request from the group management client to the group management server.

Table 10.3.2.9-1: Group deletion request

Information element	Status	Description
Requester Identity	M	The identity of the group management client performing the request.
VAL group ID	M	VAL group ID of the group to delete

10.3.2.10 Group deletion response

Table 10.3.2.10-1 describes the information flow group deletion response from the group management server to the group management client.

Table 10.3.2.10-1: Group deletion response

Information element	Status	Description
VAL group ID	M	Identity of the VAL group requested to be deleted
Result	M	Indicates success (group no longer exists), or failure (group deletion did not occur, e.g. authorization failure).

10.3.2.11 Group deletion notification

Table 10.3.2.11-1 describes the information flow group deletion notification from the group management server to the VAL server, and from the group management server to the group management clients for VAL users which are members of the group.

Table 10.3.2.11-1: Group deletion notification

Information element	Status	Description
VAL group ID	M	VAL group ID has been deleted.

10.3.2.12 Group information request

Table 10.3.2.12-1 describes the information flow group information request from the group management server in the partner VAL system of the VAL group to the group management server in the primary VAL system of the VAL group.

Table 10.3.2.12-1: Group information request

Information element	Status	Description
Requester Identity	M	The identity of the group management server performing the request.
VAL group ID	M	VAL group ID of the group

10.3.2.13 Group information response

Table 10.3.2.13-1 describes the information flow group information response from the group management server in the primary VAL system of the VAL group to the group management server in the partner VAL system of the VAL group.

Table 10.3.2.13-1: Group information response

Information element	Status	Description
VAL group ID	M	VAL group ID of the group
VAL group configuration information	O (see NOTE 1)	Configuration information for the VAL group
Failure reason	O (see NOTE 2)	Indicates reason for failure to provide VAL group configuration information
NOTE 1: Shall be present if the request can be fulfilled by the group management server in the primary VAL system of the VAL group.		
NOTE 2: Shall be present if the request cannot be fulfilled by the group management server in the primary VAL system of the VAL group.		

10.3.2.14 Group information subscribe request

Table 10.3.2.14-1 describes the information flow group information subscribe request from the group management server in the partner VAL system of the VAL group to the group management server in the primary VAL system of the VAL group.

Table 10.3.2.14-1: Group information subscribe request

Information element	Status	Description
Requester Identity	M	The identity of the group management server performing the request.
VAL group ID	M	VAL group ID of the group

10.3.2.15 Group information subscribe response

Table 10.3.2.15-1 describes the information flow group information subscribe response from the group management server in the primary VAL system of the VAL group to the group management server in the partner VAL system of the VAL group.

Table 10.3.2.15-1: Group information subscribe response

Information element	Status	Description
VAL group ID	M	VAL group ID of the group
Result	M	Indicates success or failure of the subscribe request

10.3.2.16 Group information notify request

Table 10.3.2.16-1 describes the information flow group information notify request from the group management server in the primary VAL system of the VAL group to the group management server in the partner VAL system of the VAL group.

Table 10.3.2.16-1: Group information notify request

Information element	Status	Description
Requester Identity	M	The identity of the group management server performing the request.
VAL group ID	M	VAL group ID of the group
VAL group configuration information	M	Configuration information for the VAL group

10.3.2.17 Group information notify response

Table 10.3.2.17-1 describes the information flow group information notify response from the group management server in the partner VAL system of the VAL group to the group management server in the primary VAL system of the VAL group.

Table 10.3.2.17-1: Group information notify response

Information element	Status	Description
VAL group ID	M	VAL group ID of the group
Result	M	Indicates success or failure of the notification request

10.3.2.18 Store group configuration request

Table 10.3.2.18-1 describes the information flow store group configuration request from the group management client to the group management server.

Table 10.3.2.18-1: Store group configuration request

Information element	Status	Description
Requester Identity	M	The identity of the group management client performing the request.
VAL group ID	M	VAL group ID of the group
VAL group configuration data	M	VAL group configuration data

10.3.2.19 Store group configuration response

Table 10.3.2.19-1 describes the information flow store group configuration response from the group management server to the group management client.

Table 10.3.2.19-1: Store group configuration response

Information element	Status	Description
VAL group ID	M	VAL group ID of the group
Result	M	Indicates the success or failure for the result

10.3.2.20 Get group configuration request

Table 10.3.2.20-1 describes the information flow get group configuration request from the group management client to the group management server.

Table 10.3.2.20-1: Get group configuration request

Information element	Status	Description
Requester Identity	M	The identity of the group management client performing the request.
VAL group ID	M	VAL group ID of the group
VAL group information reference	M	Reference to configuration data for the VAL group
VAL services requested (see NOTE)	O	Service(s) for which group configuration is requested
NOTE: If 'VAL services requested' is not present, group configuration is requested for all services defined for the VAL group		

10.3.2.21 Get group configuration response

Table 10.3.2.21-1 describes the information flow get configuration response from the group management server to the group management client.

Table 10.3.2.21: Get group configuration response

Information element	Status	Description
VAL group ID	M	VAL group ID of the group
VAL group configuration data	M (see NOTE)	VAL group configuration data
Result	M	Indicates the success or failure for the operation
NOTE: If the Result information element indicates failure then the value of the VAL group configuration data information element has no meaning.		

10.3.2.22 Subscribe group configuration request

Table 10.3.2.22-1 describes the information flow subscribe group configuration request from the group management client to the group management server.

Table 10.3.2.22-1: Subscribe group configuration request

Information element	Status	Description
Requester Identity	M	The identity of the group management client performing the request.
VAL group ID	M	VAL group ID of the group
VAL services requested (see NOTE)	O	Service(s) for which group configuration is requested
Minimum time between consecutive notifications	O	Defaults to 0 if not provided, otherwise indicates the minimum time interval between consecutive notifications
NOTE: If 'VAL services requested' is not present, group configuration is requested for all services defined for the VAL group		

10.3.2.23 Subscribe group configuration response

Table 10.3.2.23-1 describes the information flow subscribe group configuration response from the group management server to the group management client.

Table 10.3.2.23-1: Subscribe group configuration response

Information element	Status	Description
VAL group ID	M	VAL group ID of the group
Result	M	Indicates the success or failure for the result

10.3.2.24 Notify group configuration request

Table 10.3.2.24-1 describes the information flow notify group configuration request from the group management server to the group management client.

Table 10.3.2.24-1: Notify group configuration request

Information element	Status	Description
Requester Identity	M	The identity of the group management server performing the request.
VAL group ID	M	VAL group ID of the group
VAL group information reference (see NOTE)	O	Reference to information stored relating to the VAL group
Group related key material (see NOTE)	O	Key material for use with the VAL group
NOTE: At least one of these information elements shall be present.		

10.3.2.25   Notify group configuration response

Table 10.3.2.25-1 describes the information flow notify group configuration response from the group management client to the group management server.

Table 10.3.2.25-1: Notify group configuration response

Information element	Status	Description
VAL group ID	M	VAL group ID of the group
Result	M	Indicates the success or failure for the result

10.3.2.26   Configure VAL group request

Table 10.3.2.26-1 describes the information flow for configure VAL group request from a VAL server to a group management server.

Table 10.3.2.26-1: Configure VAL group request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL group ID	M	The group ID used for the VAL group.
VAL group description (see NOTE 2)	M	Information related to the VAL group e.g. group definition including communication type, policy, group size, group leader.
VAL service ID list (see NOTE 1)	O	List of VAL services whose service communications are to be enabled on the group.
Geo ID list (see NOTE 1)	O	List of geographical areas to be addressed by the group.
Identity list (see NOTE 1)	O	List of VAL UE IDs who are invited to be member of the group.
Identity list subscription	O	Indicates interest to receive notifications of newly registered or de-registered VAL UE IDs.
NOTE 1: At least one of these IEs shall be present.		
NOTE 2: Group communication type may indicate 5G LAN-Type communication using either Ethernet or IP (IPv4 and/or IPv6) transport.		

10.3.2.27   Configure VAL group response

Table 10.3.2.27-1 describes the information flow for configure VAL group response from group management server to a VAL server.

Table 10.3.2.27-1: Configure VAL group response

Information element	Status	Description
Result	M	The result of the configure VAL group operation
Subscription result	O (see NOTE)	Indicates whether subscription to receive notifications of newly registered or de-registered VAL UE IDs is successful or not
NOTE: Shall be present only if there is a subscription in the configure VAL group request and successful.		

10.3.2.28   Group announcement

Table 10.3.2.28-1 describes the information flow for a group management server to announce a VAL group to the group management clients.

Table 10.3.2.28-1: Group announcement

Information element	Status	Description
VAL group ID	M	The group ID used for the VAL group.
VAL group description (see NOTE 3)	M	Information related to the VAL group e.g. group definition including communication type and connection parameters, policy, group size, group leader.
VAL service ID list (see NOTE 1)	O	List of VAL services whose service communications are to be enabled on the group.
Geo ID list (see NOTE 1)	O	List of geographical areas to be addressed by the group.
Identity list (see NOTE 1, NOTE 2)	O	List of VAL UE IDs who are invited to be member of the group.
NOTE 1: At least one of these IEs shall be present. NOTE 2: This element is not present if it results in privacy concerns. NOTE 3: Group communication type may indicate 5G LAN-Type communication using either Ethernet or IP (IPv4 and/or IPv6) transport. Group connection parameters may include DNN and S-NSSAI.			

10.3.2.29   Group registration request

Table 10.3.2.29-1 describes the information flow for a group management client to register to a VAL group in response to a group announcement from the group management server. Message filters for throttling messages and notifications is included in this request e.g. for limiting message exchange on a constrained UE, for receiving only improtant group communication.

Table 10.3.2.29-1: Group registration request

Information element	Status	Description
VAL UE ID	M	Identity of the VAL UE registering to the VAL group.
VAL Group ID	M	The group ID to be registered by the VAL UE for the VAL group.
Identity list subscription	M	Indicates interest to receive notifications of newly registered or de-registered VAL UE IDs
Message filters	O	Group message communication will be sent to the VAL UE after applying message filters as described in Table 10.3.2.29-2.

Table 10.3.2.29-2: Message filters

Information element	Status	Description
Identities	O	List of VAL UE identities whose messages will be send to the VAL UE being registered
Max number of messages (see NOTE 1)	O	Total number of messages allowed to be sent to the VAL UE in a given time frame as defined by the VAL service.
Time frame	O	Time frame associated to Max number of messages IE
Message Types (see NOTE 2)	O	List of message types which will be sent to the VAL UE being registered (e.g. high priority messages, or group configuration messages, etc.).
NOTE 1: Specifying value for max number of messages is outside the scope of SEAL and up to the implementation of a particular Vertical requirement. NOTE 2: Message types are as decided by the specific Vertical.			

Editor's note: Handling of updates to the "message filters" over the life of the group communication is FFS.

10.3.2.30 Group registration response

Table 10.3.2.30-1 describes the information flow for a group management server to respond for a group registration request from the group management client.

Table 10.3.2.30-1: Group registration response

Information element	Status	Description
Result	M	Result from the VAL server in response to VAL group registration request indicating success or failure
Subscription result	M	Indicates whether subscription to receive notifications of newly registered or de-registered VAL UE IDs is successful or not

10.3.2.31 Identity list notification

Table 10.3.2.31-1 describes the information flow identity list notification from the group management server to the group management client.

Table 10.3.2.31-1: Identity list notification

Information element	Status	Description
VAL group ID	M	Identity of the VAL group
Identity list	M	List of VAL UE IDs who are newly registered or de-registered members of the group

Table 10.3.2.31-2 describes the information flow identity list notification from the group management server to the VAL server.

Table 10.3.2.31-2: Identity list notification

Information element	Status	Description
VAL group ID	M	Identity of the VAL group
Identity list	M	List of VAL UE IDs who are newly registered or de-registered members of the group
Message filters list	O	List of Message filters per VAL UE ID who are newly registered.

10.3.2.32 Group de-registration request

Table 10.3.2.32-1 describes the information flow for a group management client to de-register to a VAL group.

Table 10.3.2.32-1: Group de-registration request

Information element	Status	Description
VAL UE ID	M	Identity of the VAL UE de-registering to the VAL group.
VAL Group ID	M	The group ID to be de-registered by the VAL UE for the VAL group.

10.3.2.33 Group de-registration response

Table 10.3.2.33-1 describes the information flow for a group management server to respond for a group de-registration request from the group management client.

Table 10.3.2.33-1: Group de-registration response

Information element	Status	Description
Result	M	Result from the group management server in response to VAL group de-registration request indicating success or failure

10.3.2.34 Location-based group creation request

Table 10.3.2.34-1 describes the information flow location-based group creation request from the group management client or VAL server to the group management server.

Table 10.3.2.34-1: location-based group creation request

Information element	Status	Description
Requester Identity	M	The identity of the group management client performing the request.
Location criteria	M	Criteria to combine Users or UEs in a location.
VAL service ID list (see NOTE 1)	O	List of VAL services whose service communications are to be enabled on the group.
VAL service specific information (see NOTE 2)	O	Placeholder for VAL service specific information
NOTE 1: This information element shall be included in the message for creating a group configured for multiple VAL services.		
NOTE 2: The details of this information element are specified in VAL service specific specification and are out of scope of the present document.		

10.3.2.35 Location-based group creation response

Table 10.3.2.35-1 describes the information flow location-based group creation response from the group management server to the group management client or VAL server.

Table 10.3.2.35-1: Location-based group creation response

Information element	Status	Description
VAL group ID	M (see NOTE)	VAL group ID of the group
Result	M	Indicates the success or failure for the operation
NOTE: If the Result information element indicates failure then the value of VAL group ID information element has no meaning.		

10.3.2.36 Group list fetch request

Table 10.3.2.36-1 describes the information flow for Group list fetch request from the group management client to the group management server.

Table 10.3.2.36-1: Group list fetch request

Information element	Status	Description
Identity	M	The identity of the VAL UE or VAL User performing the operation.
Period	O	Indicates to the group management server to provide list of the groups created between specified period.

10.3.2.37 Group list fetch response

Table 10.3.2.37-1 describes the information flow for Group list fetch response from the group management server to the group management client.

Table 10.3.2.37-1: Get group list fetch response

Information element	Status	Description
Result	M	Result from the group management server in response to group list fetch request indicating success or failure
VAL group IDs	M	The list of VAL groups for which the VAL User is a member

10.3.2.38 Temporary group formation request

Table 10.3.2.38-1 describes the information flow for the temporary group formation request from the group management client to the group management server.

Table 10.3.2.38-1: Temporary group formation request

Information element	Status	Description
VAL group ID list	M	List of VAL group IDs to be combined
VAL service list (see NOTE)	O	A subset of the common VAL service(s) to be applied for the temporary group
NOTE: If this information element is not present, all the VAL service(s) that are common to the groups being combined will be applicable for the temporary group.		

10.3.2.39 Temporary group formation response

Table 10.3.2.39-1 describes the information flow for the temporary group formation response from the group management server to the group management client.

Table 10.3.2.39-1: Temporary group formation response

Information element	Status	Description
VAL group ID	O (see NOTE)	VAL group ID of the temporary group
VAL service list	O	List of VAL services whose service communications are to be enabled on this temporary group
Result	M	Indicates the success or failure of temporary group formation.
NOTE: Shall be present if the Result information element indicates that the temporary group formation operation is successful. Otherwise VAL group ID shall not be present.		

10.3.2.40 Temporary group formation notify

Table 10.3.2.40-1 describes the information flow temporary group formation notify from the group management server to the VAL server.

Table 10.3.2.40-1: Temporary group formation notify

Information element	Status	Description
VAL group ID list	M	List of constituent VAL group IDs
VAL group ID	M	VAL group ID of the temporary group
VAL service list	O	List of VAL services whose service communications are to be enabled on this temporary group.

10.3.2.41 Temporary group formation notification

Table 10.3.2.41-1 describes the information flow temporary group formation notification from the group management server to the group management client.

Table 10.3.2.41-1: Temporary group formation notification

Information element	Status	Description
VAL group ID list	M	List of constituent VAL group IDs
VAL group ID	M	VAL group ID of the temporary group

10.3.2.42 Temporary group formation notification response

Table 10.3.2.42-1 describes the information flow temporary group formation notification response from the group management client to the group management server.

Table 10.3.2.42-1: Temporary group formation notification response

Information element	Status	Description
VAL group ID	M	VAL group ID of the temporary group

10.3.3 Group creation

Figure 10.3.3-1 below illustrates the group creation operations by authorized VAL user/UE/administrator to create a group. It applies to the scenario of normal group creation by a VAL administrator or by authorized user/UE.

Pre-conditions:

1. The group management client, group management server, VAL server and the VAL group members belong to the same VAL system.

2. The authorized VAL user/UE/administrator is aware of the users' identities which will be combined to form the VAL group.
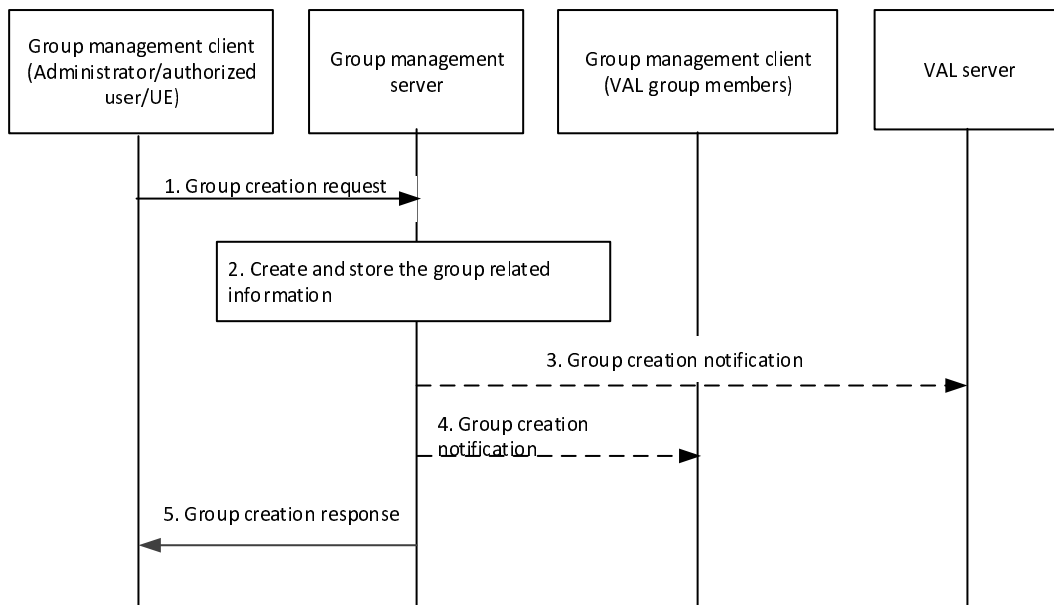
Figure 10.3.3-1: Group creation

1. The group management client of the authorized VAL user/UE/administrator requests group create operation to the group management server. The identities of the users or UEs being combined and the information of the VAL services that are enabled on the group shall be included in this message.

2. During the group creation, the group management server creates and stores the information of the group. The group management server performs the check on the policies e.g. maximum limit of the total number of VAL group members for the VAL group(s). The external group identifier, identifying the member UEs of the VAL group at the 3GPP core network, is stored in the newly created VAL group's configuration information.

NOTE: The exact policies are out of scope of the present document.

3. The group management server may conditionally notify the VAL server regarding the group creation with the information of the group members.

4. The VAL group members of the VAL group are notified about the newly created VAL group configuration data.

5. The group management server provides a group creation response to the group management client of the administrator/authorized VAL user/UE.

10.3.4 Group information query

10.3.4.1 General

A VAL user/UE can request the membership list on an VAL group regardless the user or UE's group membership.

10.3.4.2 Procedure

Figure 10.3.4.2-1 below illustrates the group information query on a VAL group.
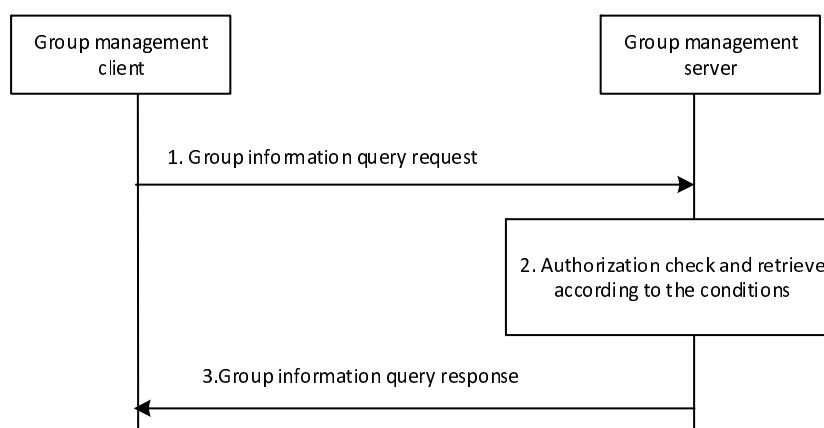
Figure 10.3.4.2-1: Group information query

1. The group management client of the VAL user/UE requests the group information on the VAL group from the group management server by sending a group information query request. The query type is included.

2. The group management server checks whether the VAL user/UE is authorized to perform the query. If authorized, then the group management server retrieves the requested group information based on the query type.

3. The group management server sends a group information query response including the retrieved group information to the group management client.

10.3.5 Group membership

10.3.5.1 Group membership notification

Figure 10.3.5.1-1 illustrates the group membership notification operations to the VAL server(s) and group management clients upon the group membership change at group management server.

Pre-conditions:

1. VAL group is created on the group management server.
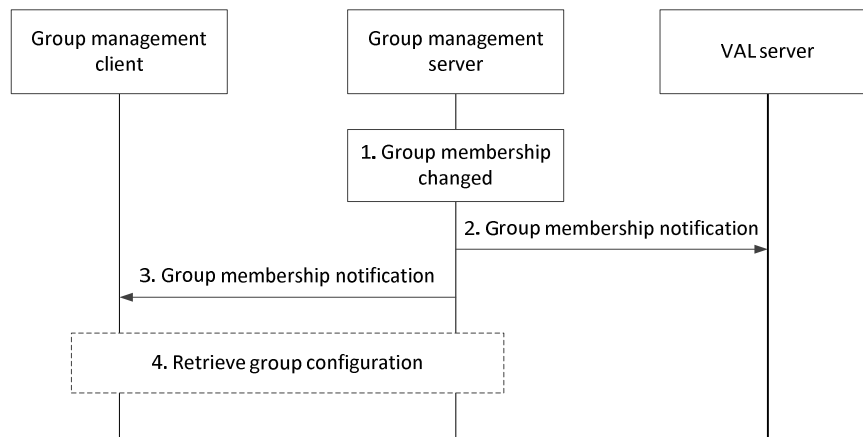
Figure 10.3.5.1-1: group membership notification

1. The membership of a specific VAL group is changed at group management server.

2. The group management server notifies the VAL server(s) regarding the group membership change with the information of the updated group members.

3. The group management server updates the group management clients of the VAL users/UEs who have been added to or removed from the group.

4. The group management client requests to retrieve the relevant group configurations from group management server, if the user or UE is added to the group. If the user or UE is deleted from the group, the locally stored group configurations in the VAL UE may be removed.

10.3.5.2   Group membership update by authorized user/UE/VAL server

Figure 10.3.5.2-1 below illustrates the group membership update operations by an authorized user/UE/administrator/VAL server to change the membership of a VAL group (e.g. to add or delete group members).

Pre-conditions:

1. The group management server and VAL server serve the same VAL system;

2. The initiator of this operation is aware of the current group membership of the VAL group;

3. The authorized user/UE/administrator/VAL server is aware of the users' identities which will be added to or deleted from the VAL group.
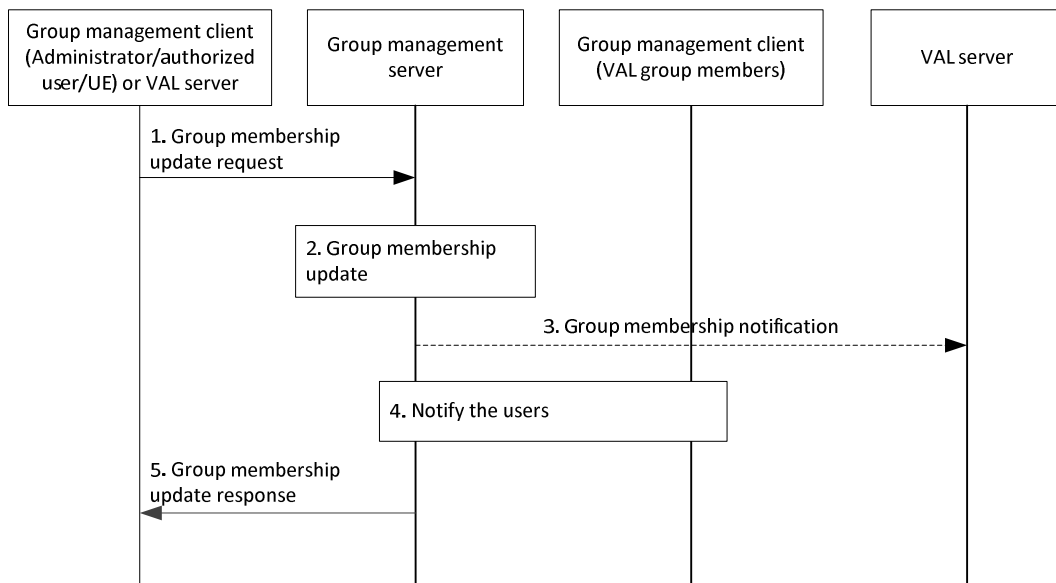
Figure 10.3.5.2-1: Group membership update by authorized user/UE/VAL server

1. The group management client of the authorized user/UE/administrator or VAL server requests group membership update operation to the group management server.

2. The group management server updates the group membership information. The group management server may perform the check on policies e.g. the maximum limit of the total number of VAL group members.

NOTE 1: The exact policies are out of scope of the present document.

3. The group management server notifies the VAL server(s) regarding the group membership change with the information of the updated group members.

NOTE 2: Step 3 does not happen when the VAL server is requesting group membership update operation.

4. The group members that are added to or deleted from the group by this operation are notified about the group membership change. This step may be followed by retrieving group configurations.

5. The group management server provides a group membership response to the group management client of the authorized user/UE/administrator or the VAL server.

10.3.6 Group configuration management

10.3.6.1 Store group configurations at the group management server

The procedure for store group configurations at the group management server is described in figure 10.3.6.1-1.

Pre-conditions:

- The group management server may have some pre-configuration data which can be used for online group configuration validation;
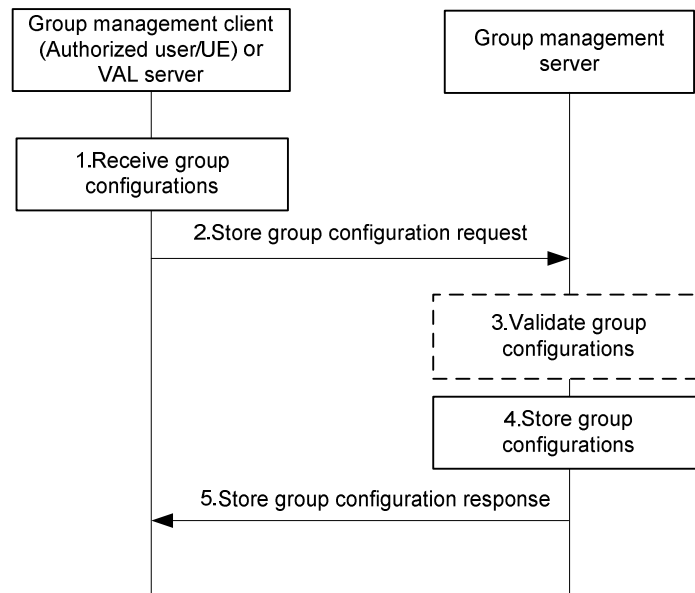
Figure 10.3.6.1-1: Store group configurations at group management server

1. The group configurations are received by the group management client of an authorized user/UE or VAL server.

2. The received group configurations are sent to the group management server for storage using a store group configuration request.

3. The group management server may validate the group configurations before storage.

4. The group management server stores the group configurations.

5. The group management server provides a store group configuration response indicating success or failure. If any validation or storage fails, the group management server provides a failure indication in the store group configuration response.

10.3.6.2   Retrieve group configurations

The procedure for retrieve group configurations at the group management client or the VAL server is described in figure 10.3.6.2-1. This procedure can be used following service authorisation when the configuration management client has received the list of groups and the group management client needs to obtain the group configurations, or following a notification from the group management server that new group configuration information is available.

Pre-conditions:

-   The group management server has received configuration data for groups, and has stored this configuration data;

-   The VAL UE has registered for service and the group management client or the VAL server needs to download group configuration data applicable to the user/UE.
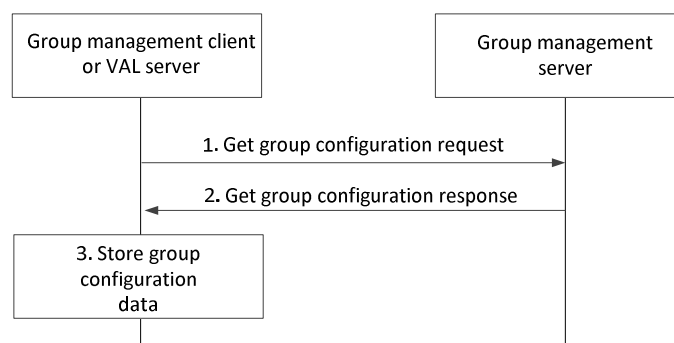
Figure 10.3.6.2-1: Retrieve group configurations

1. The group management client or the VAL server requests the group configuration data.

2. The group management server provides the group configuration data to the client or the VAL user.

3. The group management client or the VAL server stores the group configuration information.

10.3.6.3 Subscription and notification for group configuration data

The procedure for subscription for group configuration data as described in figure 10.3.6.3-1 is used by the group management client to indicate to the group management server that it wishes to receive updates of group configuration data for groups for which it is authorized.

Pre-conditions:

- The group management server has some group configurations stored.
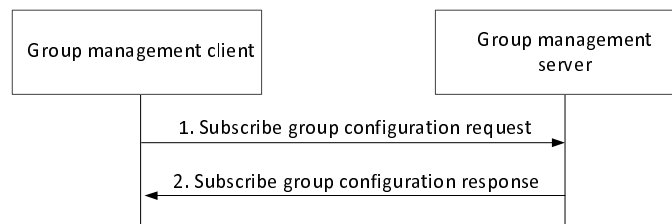
Figure 10.3.6.3-1: Subscription for group configurations

1. The group management client subscribes to the group configuration information stored at the group management server using the subscribe group configuration request.

2. The group management server provides a subscribe group configuration response to the group management client indicating success or failure of the request.

The procedure for notification of group configuration data as described in figure 10.3.6.3-2 is used by the group management server to inform the group management client that new group configuration data is available. It can also be used by the group management server to provide new group related key material to the group management client.

Pre-conditions:

- The group management client has subscribed to the group configuration information

- The group management server has received and stored new group configuration information, or the group management server has generated and stored new key material, or both of these have occurred.
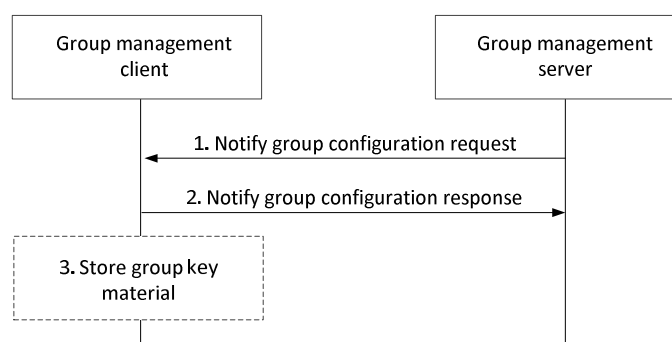
Figure 10.3.6.3-2: Notification of group configurations

1. The group management server provides the notification to the group management client, who previously subscribed for the group configuration information. Optionally, the notify group configuration request may contain group related key material for the group management client.

2. The group management client provides a notify group configuration response to the group management server.

3. If the group management server had provided group related key material to the group management client, the group management client stores the key material.

If the group management server has notified the group management client about new group configuration information through this procedure, the group management client may then follow the procedure described in subclause 10.3.6.2 in order to retrieve that group configuration information.

10.3.6.4 Structure of group configuration data

The group configuration data contains group configuration data common to all VAL services and group configuration data specific to each VAL service.

NOTE: For a VAL service, the VAL group configuration data is listed in the corresponding VAL service specification and is outside the scope of the present document.

10.3.7 Location-based group creation

Figure 10.3.7-1 below illustrates the location-based group creation.

Pre-conditions:

1. The group management client, group management server, VAL server, location management server and the VAL group members belong to the same VAL system.

2. The authorized VAL user/UE/administrator is not aware of the users' or UE identities which will be combined to form the VAL group.
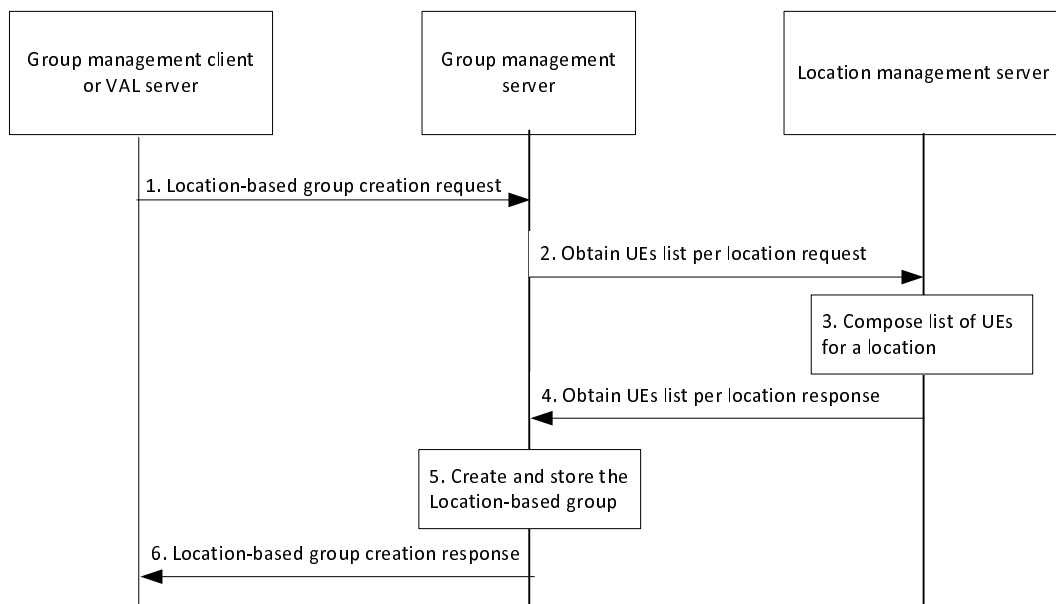
Figure 10.3.7-1: Location-based group creation

1. The group management client or the VAL server requests location-based group create operation to the group management server. The location criteria for determining the identities of the users or UEs to be combined shall be included in this message.

2. The group management server requests the location management server for obtaining the users or UEs corresponding to the location information.

3. The location management server composes the list of users or UEs within the requested location.

4. The group management server receives the composed list of users or UEs from the location management server.

5. During the group creation, the group management server creates and stores the information of the location-based group. The group management server performs the check on the policies e.g. maximum limit of the total number of VAL group members for the VAL group(s). If an external group identifier, identifying the member UEs of the VAL group at the 3GPP core network is available, then the external group ID is stored in the newly created VAL group's configuration information.

NOTE: The exact policies are out of scope of the present document.

6. The group management server provides a location-based group creation response to the group management client or the VAL server.

10.3.8 Group announcement and join

10.3.8.1 General

This subclause describes the procedures for establishing group communication from the group management server to the group management clients.

10.3.8.2 Procedure

Pre-conditions:

1. The group management client, group management server, VAL server and the VAL clients belong to the same VAL system.

2. The VAL server is aware of the users' identities and is authorized to form a VAL group.
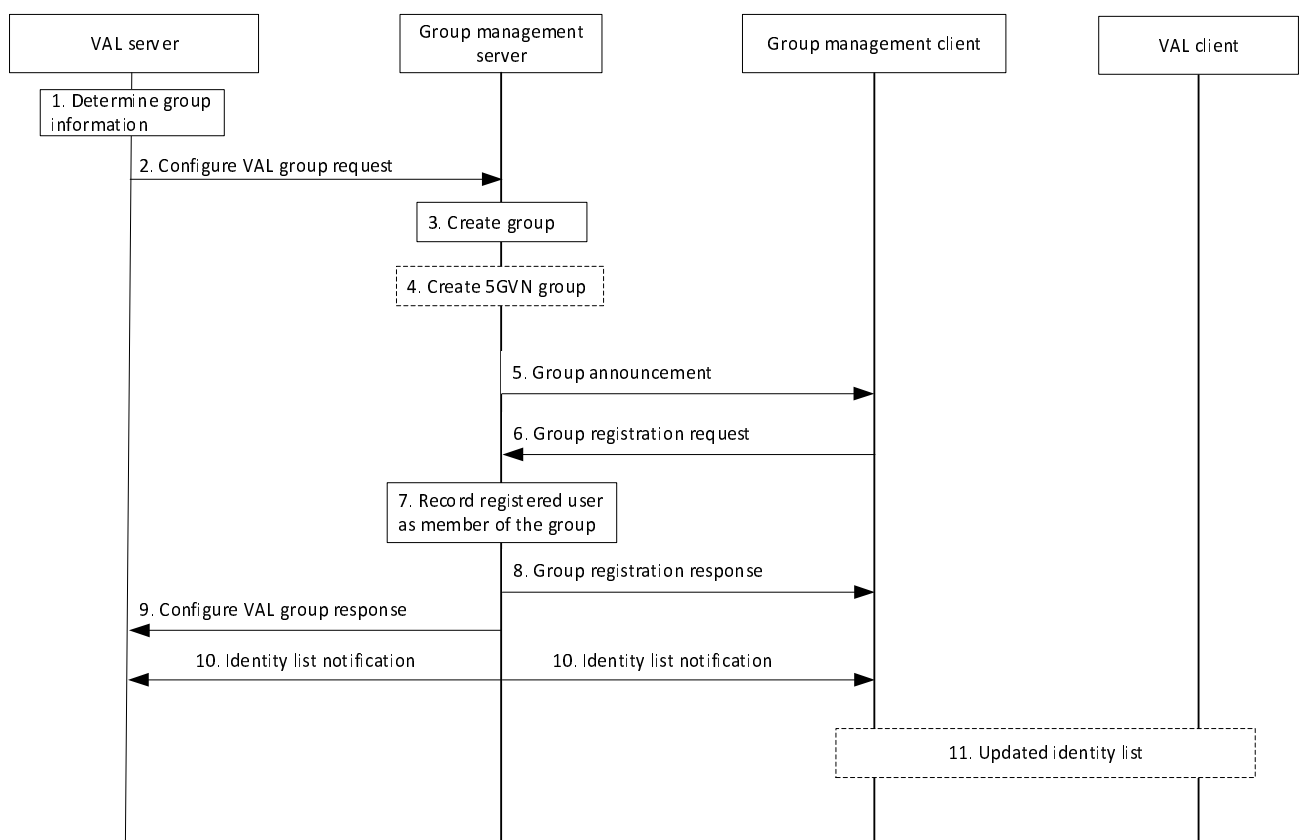
Figure 10.3.8.2-1: Procedure for establishing VAL group communication between the group management server and group management client1.

1. The VAL server determines group information and the identity list to which the group announcement shall be sent. The decision can be based on the list of authorized UEs and other criteria (e.g. user consent, service, or vehicle driving profile).

2. The VAL server configures VAL group for Uu communication defined by VAL Group ID for one or more VAL services with list of VAL Service ID with the group management server.

3. The group management server creates an empty group based on the information provided in the Configure VAL group request. The group management server stores the mapping between the VAL group ID and the external Group Id in the VAL group document, along with a list of GPSIs corresponding to the identity list provided by the VAL server. The group management server also determines whether the group is for 5G LAN-Type communication and whether Ethernet or IP (IPv4 and/or IPv6) transport shall be used for the 5G LAN-Type communication.

4. If 5G LAN-Type communication is to be used, the group management server creates a 5GVN group in the 5GS via N33 using the create group procedure specified in 3GPP TS 23.501 [10] clause 5.29.2 and 3GPP TS 23.502 [11] clause 4.15.6. The group management server creates the 5GVN group data and the 5GVN group membership data defined in 3GPP TS 23.502 [11] clause 4.15.6.3b to be configured in the 5GS. To create the 5GVN group data the group management server uses the 5G LAN-Type communication type information provided by the VAL server to set the PDU session type (Ethernet or IP) and maps the VAL service IDs to Application descriptors. To create the 5GVN group membership data the group management server maps the VAL group ID to the External Group ID and makes a list of GPSIs corresponding to the identity list provided by the VAL server.

NOTE 1: This step is skipped for the case that a 5G LAN-Type communication is not being used.

NOTE 2: The PDU session type, DNN, S-NSSAI provided within 5GVN group data cannot be modified in the 5GS after the create procedure.

NOTE 3: The 5GS supports only a 1:1 mapping between DNN/S-NSSAI combination and 5GVN group.

NOTE 4: The group management server maintains a mapping between DNN and S-NSSAI of the 5GVN group and the VAL server requester identity based on operator policy. How such mapping is configured is implementation specific and out of the scope of this specification.

5. The group management server announces the VAL group to the group management clients. For a 5GVN group the announcement includes the communication type (IP or Ethernet), DNN, and S-NSSAI corresponding to the 5GVN group.

6. The group management client registers to VAL group communication using the VAL Group ID.

7. The group management server records the users who have registered to be the members of the group.

8. The group management server sends a VAL group registration response to the group management client.

9. The group management server sends a configure VAL group response to the VAL server.

NOTE 5: Step 9 may occur any time after step 5.

10. The group management server sends identity list notification about the newly registered users to the other members of the group and VAL server, whose subscription to receive notifications of newly registered VAL UE IDs is successful in step 8 and step 9 respectively.

11. The group management client may inform VAL client about the updated identity list.

10.3.9 Group member leave

10.3.9.1 General

This subclause describes the procedures for group member to leave the group by de-registering.

10.3.9.2 Procedure

Pre-conditions:

1. Group is previously defined on the group management server including the list of registered users and each member of the group and VAL server is aware of it.
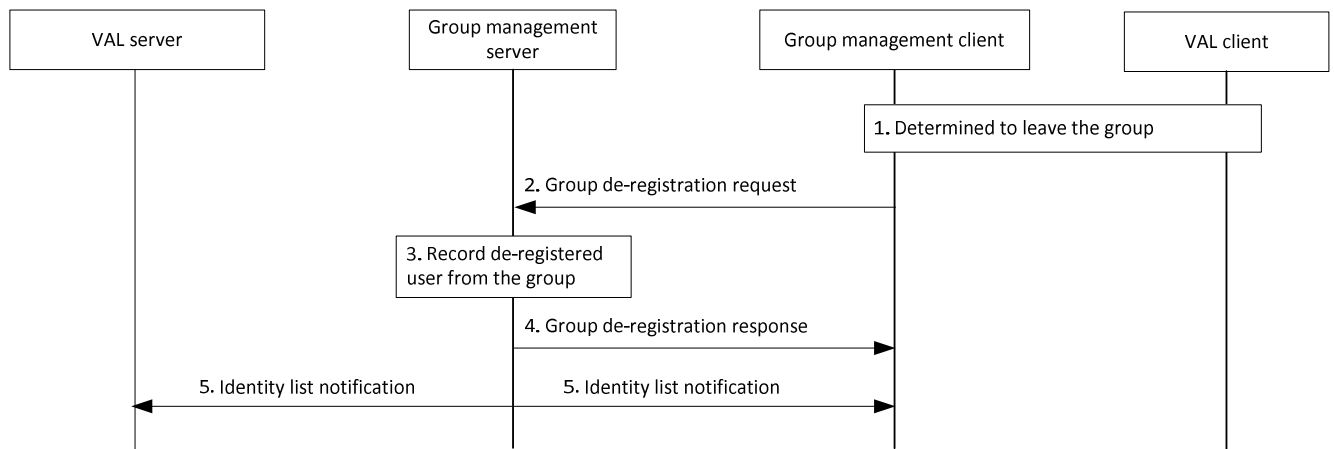
Figure 10.3.9.2-1: Procedure for group member leaving the group.

1. The VAL client determines to de-register member from the group and group management client is aware of it.

2. The group management client initiates the group de-registration request towards the group management server.

3. The group management server checks the authorization of group de-registration request and updates the group member list.

4. The group management server sends a group de-registration response to the group management client.

5. The group management server sends identity list notification about the leaving registered user to the other members of the group and the VAL server, whose subscription to receive notifications of de-registered VAL UE IDs is successful in step 7 and step 8 of the procedure in clause 10.3.8.2 respectively.

10.3.10 Temporary groups

10.3.10.1 Temporary group formation within a VAL system

Figure 10.3.10.1-1 below illustrates the temporary group formation within a VAL system.

Temporary groups are formed by combining two or more groups. The temporary group formation is applicable only for groups configured with at least one common VAL service. The temporary group formation shall be rejected if any of the requested VAL services are not common to all the constituent VAL service groups.

Pre-conditions:

1. The group management client, group management server, VAL server and the VAL group members belong to the same VAL system.

2. The group management client has retrieved the group configurations of the groups.

3. The VAL server has subscribed to receive group management event notifications.
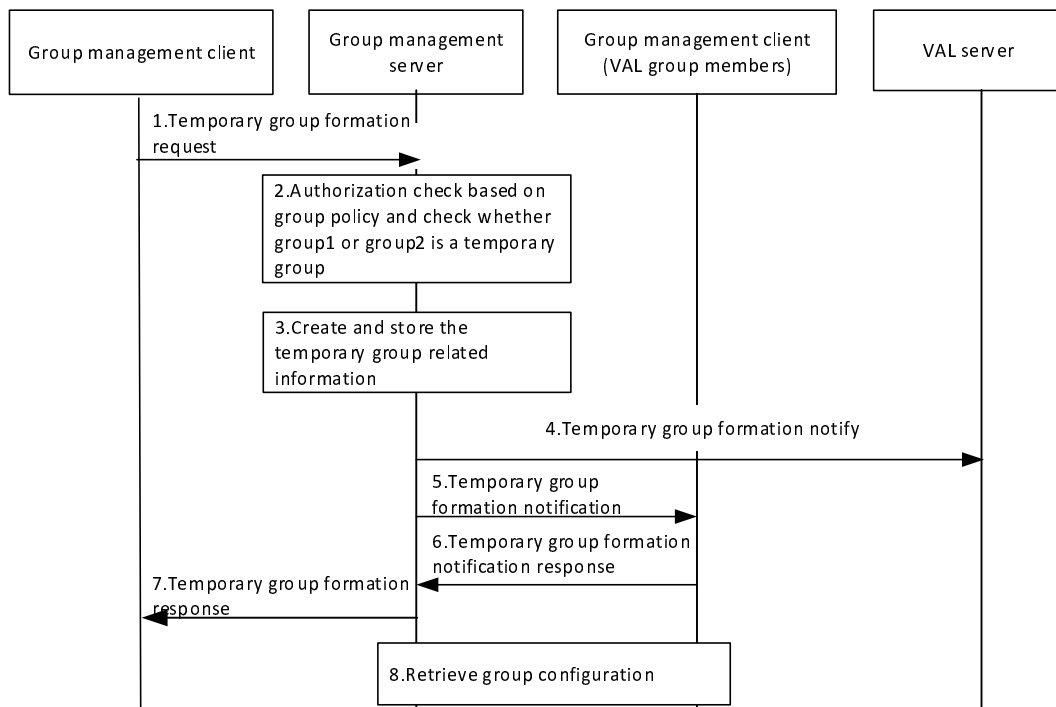
Figure 10.3.10.1-1: Temporary group formation within a VAL system

1. The group management client of the VAL user requests temporary group formation operation to the group management server, which is the group management server of one of the groups to be regrouped. The identities of the groups being combined shall be included in this message. The group management client may indicate the security level required for the temporary group. The group management client may indicate the priority level required for the temporary group.

2. The group management server checks whether temporary group formation operation is performed by an authorized VAL user, based on group policy. The group management server checks whether group1 or group2 is a temporary group. If group 1 or group2 is a temporary group, then the group regrouping will be rejected, otherwise the group regrouping can proceed.

3. The group management server creates and stores the information of the temporary group, including the temporary VAL group ID, the VAL group ID of the groups being combined, the priority level of the temporary group and the security level of the temporary group. If the authorized VAL user does not specify the security level and the priority level, the group management server shall set the lowest security level and the highest priority of the constituent groups. If VAL service types of the groups being combined are not identical, group management server determines the overlapping part and stores the VAL service list for the temporary group.

4. The group management server notifies the VAL server regarding the temporary group creation with the information of the constituent groups, i.e. temporary VAL group ID, group1's VAL group ID and group2's VAL group ID. If VAL service list is included, VAL server stores it and provides VAL service types accordingly.

5. The group management server notifies the VAL group members of the constituent VAL groups by sending temporary group formation notification messages.

6. The VAL group members of the constituent VAL groups send individual temporary group formation notification response messages.

7. The group management server provides a temporary group formation response to the group management client of the authorized VAL user. If VAL service list is included, group management client stores it and initiates VAL service types accordingly.

8. The VAL group members of the constituent VAL groups individually request group configuration data from the group management server for the temporary group. The group configuration data includes security, priority, and other parameters.

10.3.11 Group List Fetch

Figure 10.3.11-1 illustrates the group list fetch operations to fetch list of groups by the group management client.

Pre-conditions:

1) List of groups to which a VAL UE/ VAL User belongs to is known to the Group management server for each of the VAL UE/ VAL User.

2) VAL user has not received group announcement message as it was offline previously.
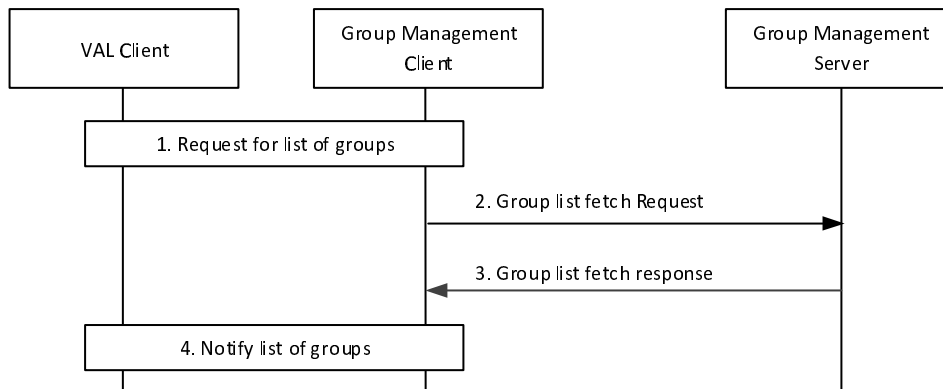
Figure 10.3.11-1: Group list fetch

1) The VAL client requests group management client to provide the list of groups in which the VAL UE or VAL User is a member.

2) The group management client initiates the group list fetch request towards the Group management server. The information elements described in clause 10.3.2.36 are included in the group list fetch request.

3) The group management server checks the authorization of group list fetch request and if authorized, sends the group list fetch response containing list of groups in which the VAL user is member. The information elements described in clause 10.3.2.37 are included in the group list fetch response.

4) The group management client notifies the list of groups to the VAL client.

10.3.12 Location-based group update

Figure 10.3.12-1 below illustrates the location-based group update.

Pre-conditions:

1. The group management client, group management server, VAL server, location management server and the VAL group members belong to the same VAL system.

2. The location based group has been created as specified in clause 10.3.7.

3. The group management server has subscribed to monitor UEs moving in or out of the fixed location area as specified in clause 9.3.12.
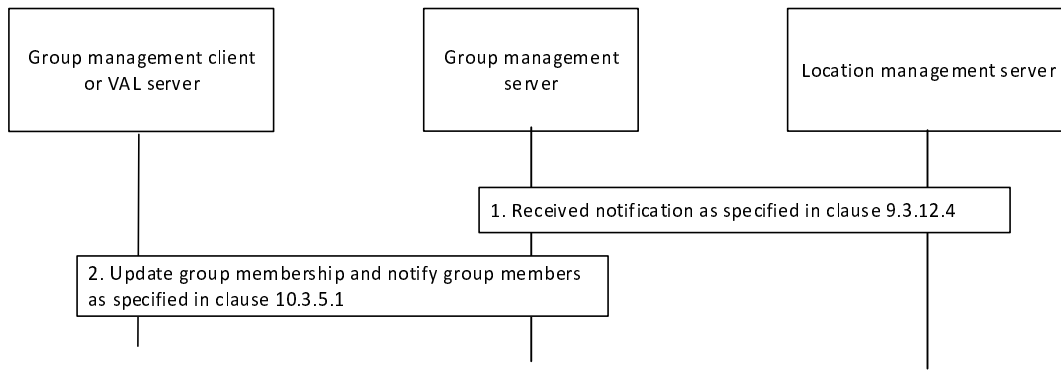
Figure 10.3.12-1: Location-based group update

1. The group management server receives location area monitoring notification from location management server as specified in clause 9.3.12.4.

2. The group management server updates the group members and sends notification as specified in clause 10.3.5.1.

10.3.13 Group deletion

Figure 10.3.13-1 below illustrates the group deletion operation by authorized VAL user/UE/administrator to delete a group. It applies to group deletion by a VAL administrator or by authorized user/UE.

Pre-conditions:

1. The group management client, group management server, VAL server and the VAL group members belong to the same VAL system.

2. The authorized VAL user/UE/administrator is aware of the group identity which needs to be deleted.
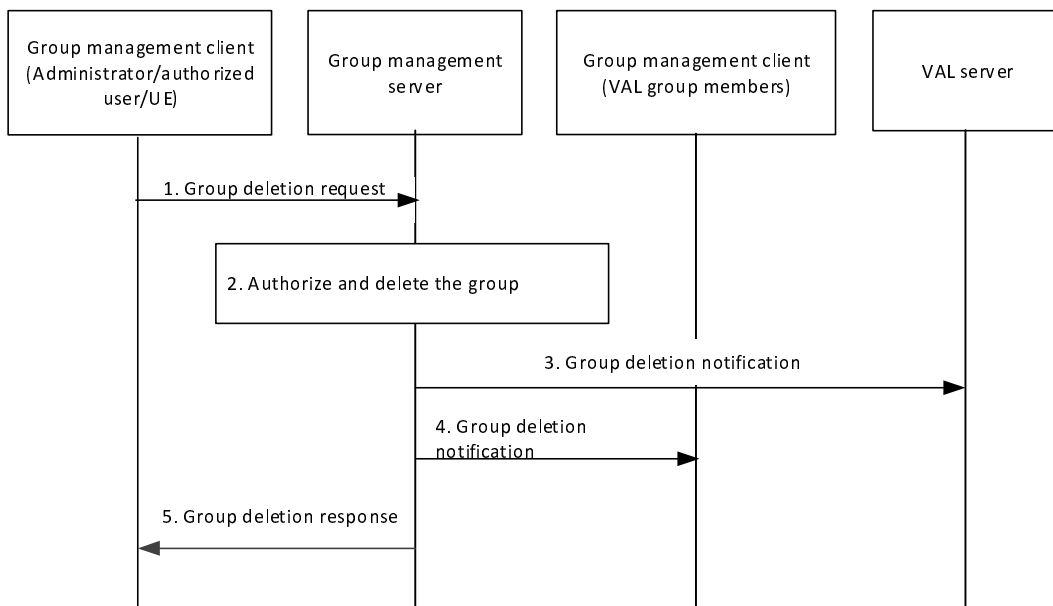
Figure 10.3.13-1: Group deletion

1. The group management client of the authorized VAL user/UE/administrator requests group deletion operation to the group management server. The identity of the group to be deleted shall be included in this message.

2. The group management server authorizes the request and if authorized, deletes the group.

3. The group management server notifies the VAL server regarding the group deletion.

4. The group members of the VAL group are notified about the deleted VAL group.

5. The group management server provides a group deletion response to the group management client of the administrator/authorized VAL user/UE.

10.4 SEAL APIs for group management

10.4.1 General

Table 10.4.1-1 illustrates the SEAL APIs for group management.

Table 10.4.1-1: List of SEAL APIs for group management

API Name	API Operations	Known Consumer(s)	Communication Type
SS_GroupManagement	Query_Group_Info	VAL server	Request /Response
	Create_LocationBasedGroup_Info	VAL server	Request/Response
	Update_Group_Info	VAL server	Request /Response
SS_GroupManagementEvent	Subscribe_ Group_Info_Modification	VAL server	Subscribe/Notify
	Notify_Group_Info_Modification	VAL server	
	Notify_Group_Creation	VAL server	
	Notify_TempGroupFormation	VAL server	

10.4.2 SS_GroupManagement API

10.4.2.1 General

API description: This API enables the VAL server to communicate with the group management server for querying group information, obtaining stored group configuration, modify the group membership and configuration information on the group management server over GM-S.

10.4.2.2 Query_Group_Info operation

API operation name: Query_Group_Info

Description: Query group information and obtaining group configuration information.

Known Consumers: VAL server.

Inputs: See subclause 10.3.2.4, 10.3.2.20

Outputs: See subclause 10.3.2.5, 10.3.2.21

See subclause 10.3.4 and 10.3.6.2 for the details of usage of this API operation.

10.4.2.3 Update_Group_Info operation

API operation name: Update_Group_Info

Description: Storing group membership and configuration information.

Known Consumers: VAL server.

Inputs: See subclause 10.3.2.6, 10.3.2.18

Outputs: See subclause 10.3.2.7, 10.3.2.19

See subclause 10.3.6.5 and 10.3.6.1 for the details of usage of this API operation.

10.4.2.4 Create_LocationBasedGroup_Info operation

API operation name: Create_LocationBasedGroup_Info

Description: Create location-based group

Known Consumers: VAL server.

Inputs: See subclause 10.3.2.34

Outputs: See subclause 10.3.2.35

See subclause 10.3.7 for the details of usage of this API operation.

10.4.3 Void

10.4.3.1 Void

10.4.3.2 Void

10.4.4 Void

10.4.4.1 Void

10.4.4.2 Void

10.4.5 SS_Group_Management_Event API

10.4.5.1 General

API description: This API enables the VAL server to communicate with the group management server to subscribe and receive subsequent notification events over GM-S.

10.4.5.2 Subscribe_ Group_Info_Modification operation

API operation name: Subscribe_ Group_Info_Modification

Description: Subscribing to changes to group membership and configuration information.

Known Consumers: VAL server.

Inputs: See subclause 10.3.2.14

Outputs: See subclause 10.3.2.15

See subclause 10.3.6.3 for the details of usage of this API operation.

10.4.5.3 Notify_Group_Info_Modification operation

API operation name: Notify_Group_Info_Modification

Description: Notification for changes to group membership and configuration information.

Known Consumers: VAL server.

Inputs: See subclause 10.3.2.8

Outputs: See subclause 10.3.2.8

See subclause 10.3.5.1 and 10.3.5.2 for the details of usage of this API operation.

10.4.5.4 Notify_Group_Creation operation

API operation name: Notify_Group_Creation

Description: Notification for new group creation.

Known Consumers: VAL server.

Inputs: See subclause 10.3.2.3

Outputs: See subclause 10.3.2.3

See subclause 10.3.3 for the details of usage of this API operation.

10.4.5.5 Notify_TempGroupFormation operation

API operation name: Notify_TempGroupFormation

Description: Notification of the new temporary group formed at the group management server.

Known Consumers: VAL server.

Inputs: See clause 10.3.2.40

Outputs: None

See subclause 10.3.10.1 for the details of usage of this API operation.

11 Configuration management

11.1 General

The configuration management is a SEAL service that offers the configuration management related capabilities to one or more vertical applications.

11.2 Functional model for configuration management

11.2.1 General

The functional model for the configuration management is based on the generic functional model specified in clause 6. It is organized into functional entities to describe a functional architecture which addresses the support for configuration management aspects for vertical applications. The on-network and off-network functional model is specified in this clause.

11.2.2 On-network functional model description

Figure 11.2.2-1 illustrates the generic on-network functional model for configuration management.
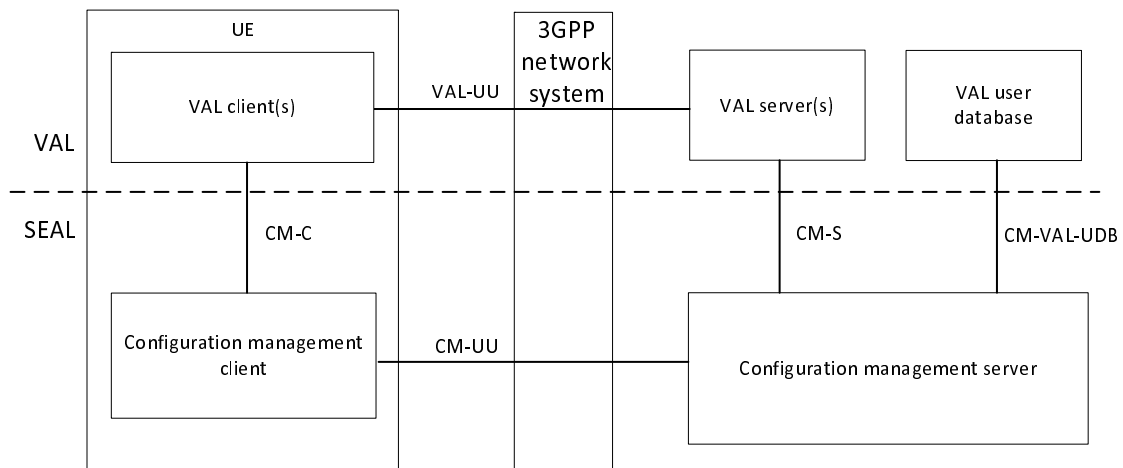
Figure 11.2.2-1: On-network functional model for configuration management

The configuration management client communicates with the configuration management server over the CM-UU reference point. The configuration management client provides the support for configuration management functions to the VAL client(s) over CM-C reference point. The VAL server(s) communicate with the configuration management server over the CM-S reference point. The configuration management server communicates with the VAL user database over the CM-VAL-UDB reference point.

11.2.3 Off-network functional model description

Figure 11.2.3-1 illustrates the off-network functional model for configuration management.
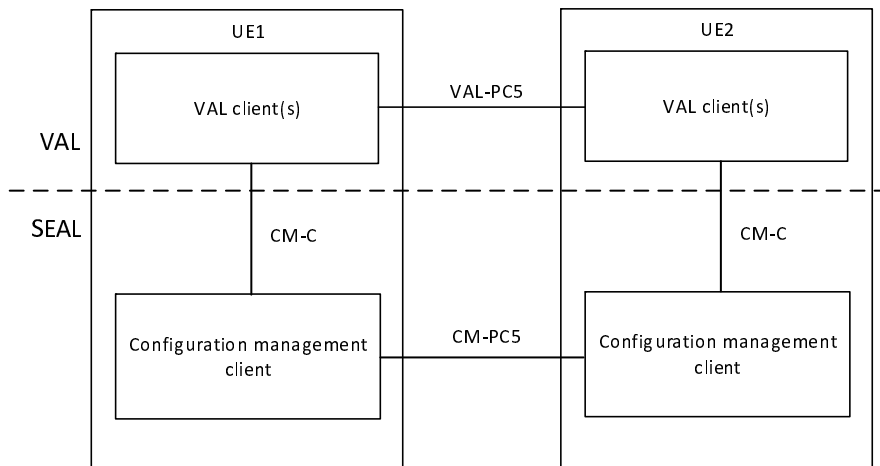
Figure 11.2.3-1: Off-network functional model for configuration management

The configuration management client of the UE1 communicates with the configuration management client of the UE2 over the CM-PC5 reference point.

11.2.4 Functional entities description

11.2.4.1 General

The functional entities for configuration management SEAL service are described in the following subclauses.

11.2.4.2 Configuration management client

The configuration management client functional entity acts as the application client for configuration related transactions. The configuration management client interacts with the configuration management server and provides and receives configuration data. The configuration management client also supports interactions with the corresponding configuration management client between the two UEs.

The configuration management client functional entity is supported by the signalling user agent and HTTP client functional entities of the signalling control plane.

11.2.4.3 Configuration management server

The configuration management server is a functional entity used to configure one or more vertical applications with 3GPP system related vertical applications provisioning information and configure data on the configuration management client. The configuration management server manages vertical application configuration supported within the vertical's service provider. The configuration management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The configuration management server also supports interactions with the corresponding configuration management server in distributed SEAL deployments.

The configuration management server functional entity is supported by the SIP AS and HTTP server functional entities of the signalling control plane.

11.2.5 Reference points description

11.2.5.1 General

The reference points for the functional model for configuration management are described in the following subclauses.

11.2.5.2 CM-UU

The interactions related to configuration management functions between the configuration management client and the configuration management server are supported by CM-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

The CM-UU reference point provides the configuration information required for VAL services and supports:

- configuration of the VAL UE by the VAL service; and

- configuration of the VAL application with the VAL service related information e.g. policy information by the VAL UE.

The CM-UU reference point shall use the HTTP-1/HTTP-2 reference points for transport and routing of configuration management related signalling. The CM-UU reference point shall use SIP-1/SIP-2 reference points for subscription/notification related signalling.

11.2.5.3 CM-PC5

The interactions related to configuration management functions between the configuration management clients located in different VAL UEs are supported by CM-PC5 reference point. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [12].

11.2.5.4 CM-C

The interactions related to configuration management functions between the VAL client(s) and the configuration management client within a VAL UE are supported by CM-C reference point.

11.2.5.5 CM-S

The interactions related to configuration management functions between the VAL server(s) and the configuration management server are supported by CM-S reference point. The CM-S reference point supports VAL server to obtain

the VAL service related vertical applications provisioning information. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

The CM-S reference point shall use HTTP-1/ HTTP-2 reference points for transport and routing of configuration management related signalling. The CM-S reference point shall use SIP-2 reference point for subscription/notification related signalling.

11.2.5.6 CM-E

The interactions related to configuration management functions between the configuration management servers in a distributed deployment are supported by CM-E reference point.

Editor's Note: The functions enabled over CM-E reference point is FFS.

11.2.5.7 Reference point CM-VAL-UDB (between the configuration management server and the VAL user database)

The CM-VAL-UDB reference point is an instance of VAL-UDB reference point, which exists between the VAL user database and the configuration management server, is used for:

- the configuration management server to store the user profile data in the specific VAL user database; and

- the configuration management server to obtain the user profile from the specific VAL user database for further configuration in the VAL UE.

11.3 Procedures and information flows for configuration management

11.3.1 General

The procedures related to the configuration management are described in the following subclauses.

11.3.2 Information flows

11.3.2.1 Get VAL UE configuration request

Table 11.3.2.1-1 describes the information flow get VAL UE configuration request from the configuration management client to the configuration management server.

Table 11.3.2.1-1: Get VAL UE configuration request

Information element	Status	Description
VAL UE ID	M	Identify of the VAL UE requesting the configuration information.
VAL service ID	O (see NOTE 1)	Identify of the VAL service for which the configuration information is requested.
VAL UE Information (see NOTE 2)	O	Additional UE related information required to identify the configuration data (e.g. device type, device vendor, etc)
NOTE 1: If the VAL service ID information element is not present, then the default service is service. NOTE 2: The VAL service provider can configure the VAL UE with different configuration data based on this IE.		

11.3.2.2 Get VAL UE configuration response

Table 11.3.2.2-1 describes the information flow get VAL UE configuration response from the configuration management server to the configuration management client.

Table 11.3.2.2-1: Get VAL UE configuration response

Information element	Status	Description
Result	M	Indicates the success or failure of getting the configuration information
VAL UE configuration data	O (see NOTE)	The VAL UE configuration data as specified in the corresponding VAL service specification and outside the scope of the present document
NOTE: If the Result information element indicates failure then VAL UE configuration data information element is not included.		

11.3.2.3 Get VAL user profile request

Table 11.3.2.3-1 describes the information flow get VAL user profile request from the configuration management client to the configuration management server.

Table 11.3.2.3-1: Get VAL user profile request

Information element	Status	Description
Requester Identity	M	The identity of the configuration management client performing the request.
Identity	M	The VAL user ID of the VAL user or VAL UE ID.

11.3.2.4 Get VAL user profile response

Table 11.3.2.4-1 describes the information flow get VAL user profile response from the configuration management server to the configuration management client.

Table 11.3.2.4-1: Get VAL user profile response

Information element	Status	Description
VAL user profile data	M (see NOTE)	One or more VAL user profiles associated with the VAL user ID or VAL UE ID provided in the associated get VAL user profile request.
Result	M	Indicates the success or failure for the operation
NOTE: If the Result information element indicates failure then the value of VAL user profile data information element has no meaning.		

11.3.2.5 Notification for VAL user profile data update

Table 11.3.2.5-1 describes the information flow notification for VAL user profile data update from the configuration management server to the configuration management client.

Table 11.3.2.5-1: Notification for VAL user profile data update

Information element	Status	Description
Pointer to modified VAL user profile data.	M	Pointer to the modified VAL user profile data.

11.3.2.6 Get updated VAL user profile data request

Table 11.3.2.6-1 describes the information flow get updated VAL user profile data request from the configuration management client to the configuration management server.

Table 11.3.2.6-1: Get updated VAL user profile data request

Information element	Status	Description
Identity	M	The VAL user ID of the originating VAL user or VAL UE ID.
Pointer to modified VAL user profile data.	M	Pointer to the modified VAL user profile data.

11.3.2.7 Get updated VAL user profile data response

Table 11.3.2.7-1 describes the information flow get updated VAL user profile data response from the configuration management server to the configuration management client.

Table 11.3.2.7-1: Get updated VAL user profile data response

Information element	Status	Description
Updated VAL user profile data	M (see NOTE)	VAL user profile data that has been modified.
Result	M	Indicates the success or failure for the operation
NOTE: If the Result information element indicates failure then the value of Updated VAL user profile data information element has no meaning.		

11.3.2.8 Update VAL user profile data request

Table 11.3.2.8-1 describes the information flow update VAL user profile data request from the configuration management client to the configuration management server.

Table 11.3.2.8-1: Update VAL user profile data request

Information element	Status	Description
Identity	M	The VAL user ID of the originating VAL user or VAL UE ID.
Updated VAL user profile data	M	The contents of the user profile data to be updated.

11.3.2.9 Update VAL user profile data response

Table 11.3.2.9-1 describes the information flow update VAL user profile data response from the configuration management server to the configuration management client.

Table 11.3.2.9-1: Update VAL user profile data response

Information element	Status	Description
Result	M	Indicates the success or failure

11.3.2.10 Updated user profile subscription request

Table 11.3.2.10-1 describes the information flow from the VAL server to the configuration management server for updated user profile subscription request.

Table 11.3.2.10-1: Updated user profile subscription request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
Identities list	M	List of VAL users or VAL UEs whose updates on user profile is requested.
Time between consecutive user profile updates	M	It indicates the interval time between consecutive user profile updates

11.3.2.11 Updated user profile subscription response

Table 11.3.2.11-1 describes the information flow from the configuration management server to the VAL server for updated user profile subscription response.

Table 11.3.2.11-1: Updated user profile subscription response

Information element	Status	Description
Subscription status	M (see NOTE)	It indicates the subscription result
Result	M	Indicates the success or failure for the operation
NOTE: If the Result information element indicates failure then the value of the Subscription status information element has no meaning.		

11.3.2.12 Updated user profile notification

Table 11.3.2.12-1 describes the information flow updated user profile notification from the configuration management server to the VAL server.

Table 11.3.2.12-1: Notify updated user profile event

Information element	Status	Description
Identities list	M	List of VAL users or VAL UEs whose user profile is modified.
Updated user profile data	M	User profile data that has been modified.

11.3.3 VAL UE configuration data

11.3.3.1 General

The VAL UE configuration data has to be known by the VAL UE before it can use the VAL service.

11.3.3.2 Procedures

The procedure for VAL UE obtaining the VAL UE related configuration data is illustrated in figure 11.3.3.2-1.

Pre-conditions:

- The VAL UE has the secure access to the configuration management server.
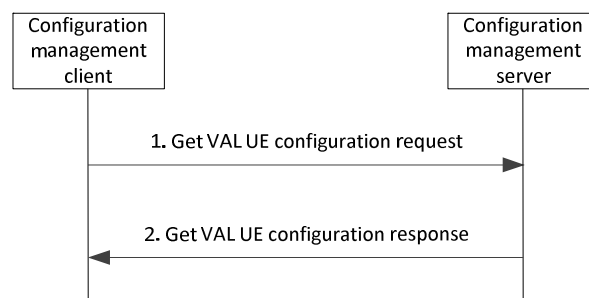
Figure 11.3.3.2-1: VAL UE obtains the configuration data

1. The configuration management client sends a get VAL UE configuration request to the configuration management server for obtaining VAL UE configuration data.

2. The configuration management server sends get VAL UE configuration response to the configuration management client. This message carries the VAL UE configuration data.

11.3.3.3 Structure of VAL UE configuration data

NOTE: For a VAL service, the VAL UE configuration data is listed in the corresponding VAL service specification and outside the scope of the present document.

11.3.4 VAL user profile data

11.3.4.1 General

The VAL user profile procedures are described in the following subclauses.

11.3.4.2 Obtaining the VAL user profile(s) from the network

11.3.4.2.1 Obtaining the VAL user profile(s) in primary VAL system

The procedure for the VAL user or VAL server obtaining VAL user profiles in the primary VAL system of that VAL user is illustrated in figure 11.3.4.2.1-1.

Pre-conditions:

- The VAL user has performed user authentication in the identity management server.

- The VAL UE or VAL server has secure access to the configuration management server.
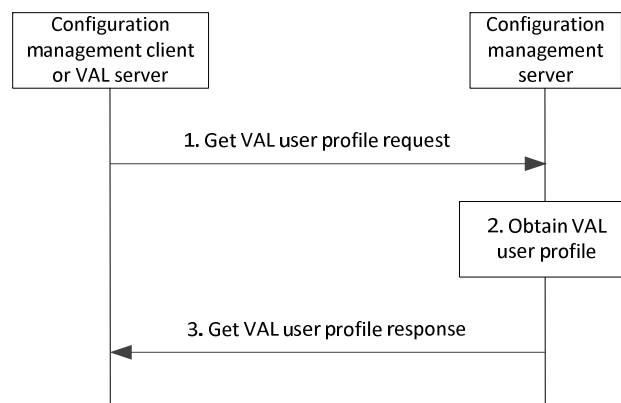
Figure 11.3.4.2.1-1: VAL user obtains the VAL user profile(s) from the network

1. The configuration management client or VAL server sends a get VAL user profile request message to the configuration management server, which includes the VAL user ID or VAL UE ID.

2. The configuration management server obtains the VAL user profile information.

3. The configuration management server sends get VAL user profile response message to the configuration management client or VAL server. When a download is necessary, this message includes all VAL user profiles that are associated with the VAL user ID or VAL UE ID.

11.3.4.2.2 VAL user receiving VAL service from a partner VAL system

Figure 11.3.4.2.2-1 below illustrates mechanism for the configuration management client to retrieve the VAL user profile for the migrating VAL user from the partner VAL system.

NOTE: Any proxy servers at the edges of the primary and partner VAL systems which are used to hide the topology of the VAL systems from external entities are not shown in this procedure.

Preconditions

- The VAL user is permitted to migrate to the partner VAL system, and the relevant authorizations are configured in both the primary and partner VAL systems of that VAL user

- The VAL user has performed VAL user authentication in the partner VAL system, and has received the necessary credentials to retrieve configuration information and to request service authorization.

- The VAL UE has been provided with addressing information to allow the configuration management client in the VAL UE to access the configuration management server in the partner VAL system.
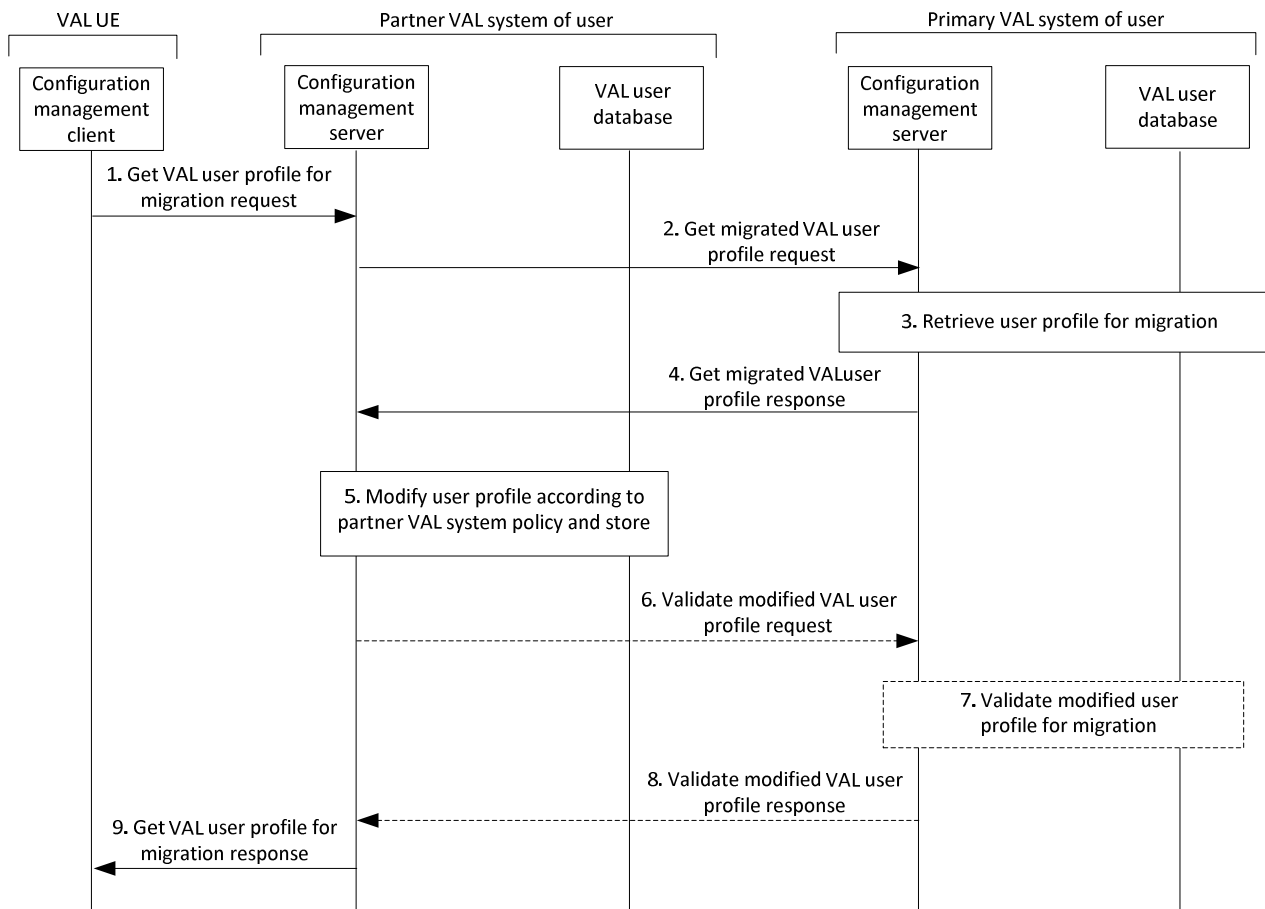
Figure 11.3.4.2.2-1: Retrieval of user profile in partner VAL system

1. The configuration management client in the VAL UE of the migrating VAL user requests the VAL user profile for migration from the configuration management server in the partner VAL system.

2. The configuration management server in the partner VAL system requests the VAL user profile from the configuration management server in the primary VAL system of the VAL user.

3. The configuration management server in the primary VAL system of the VAL user retrieves the VAL user profile from the VAL user database in that primary VAL system. The identification of the partner VAL system to which the VAL user is attempting to migrate is used to determine which VAL user profile is retrieved for that VAL user for migration to that partner VAL system.

4. The configuration management server in the primary VAL system provides the VAL user profile to the configuration management server in the partner VAL system of the VAL user, optionally requesting validation of the modified VAL user profile.

5. The partner VAL system of the VAL user modifies the VAL user profile according to local configuration information and stores the modified VAL user profile in the VAL user database in the partner VAL system.

6. If the primary VAL system requested validation of the VAL user profile in step 4, the configuration management server in the partner VAL system of the migrating VAL user may send the modified VAL user profile to the configuration management server of the primary VAL system of the VAL user to allow the primary VAL system of the VAL user to validate the modified VAL user profile.

7. The primary VAL system of the migrated VAL user validates the modified VAL service profile of the migrated VAL user.

8. The primary VAL system of the migrated VAL user responds to the partner VAL system with the results of the validation process.

9. The configuration management server in the partner VAL system provides the VAL user profile to the configuration management client of the migrating VAL user,

NOTE: Step 9 is not followed if the validation process fails.

11.3.4.3 VAL user receives updated VAL user profile data from the network

The procedure for VAL user obtaining updated VAL user profile data that is initiated by the network is illustrated in figure 11.3.4.3-1.

Pre-conditions:

- The VAL user has performed user authentication in identity management server.

- The VAL UE has secure access to the configuration management server.

- The VAL UE has already obtained one or more VAL user profiles.

- The configuration management server has access to the VAL user profile(s) associated with the VAL user ID of the VAL user or VAL UE ID.
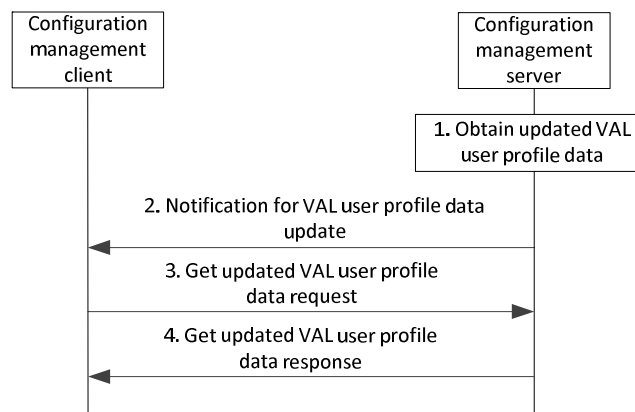
Figure 11.3.4.3-1: VAL user receives updated VAL user profile data from the network

1. The configuration management server obtains updated VAL user profile data.

2. The configuration management server sends a notification for VAL user profile data update to the configuration management client.

3. The configuration management client sends get updated VAL user profile data request to the configuration management server, which includes the VAL user ID or VAL UE ID.

4. The configuration management server sends get updated VAL user profile data response to the configuration management client which includes the updated VAL user profile data requested in step 3.

NOTE: The updated VAL user profile data could be for a specific VAL user profile, a specific parameter in an VAL user profile, a set of VAL user profiles, or all the VAL user profiles for the VAL user ID or VAL UE ID. VAL user profile data is defined per VAL service.

11.3.4.4 VAL user updates VAL user profile data to the network

The procedure for VAL user updating the VAL user profile data is illustrated in figure 11.3.4.4-1.

Pre-conditions:

- The VAL user has performed user authentication in identity management server.

- The VAL UE has secure access to the configuration management server.

- The VAL UE has already obtained one or more VAL user profiles.
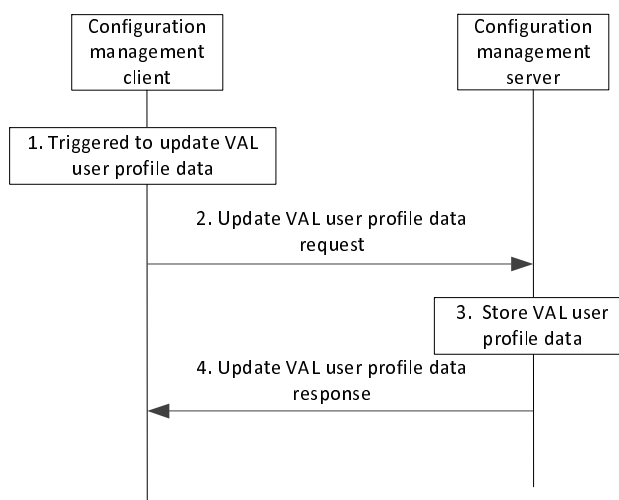
Figure 11.3.4.4-1: VAL user updates VAL user profile data to the network

1. The configuration management client is triggered (e.g. by user interaction operation) to update the VAL user profile data on the configuration management server.

2. The configuration management client sends update VAL user profile data request to the configuration management server, which includes the VAL user profile data to be updated.

3. The configuration management server stores the received VAL user profile data.

4. The configuration management server sends update VAL user profile data response to the configuration management client to confirm the VAL user profile data update is complete.

NOTE: The updated VAL user profile data could be for a specific VAL user profile, a specific parameter in an VAL user profile, a set of VAL user profiles, or all the VAL user profiles for the VAL user ID and VAL UE ID. VAL user profile data is defined per VAL service.

11.3.4.5 Updated user profile subscription procedure

Figure 11.3.4.5-1 illustrates the high level procedure for obtaining updated user profile data based on subscription request.
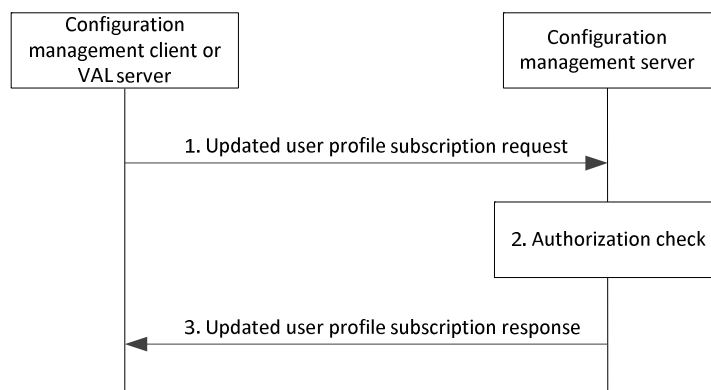
Figure 11.3.4.5-1: Updated user profile subscription procedure

1. Configuration management client or VAL server sends an updated user profile subscription request to the configuration management server to subscribe any updates to user profile of one or more VAL users or VAL UEs.

2. The configuration management server shall check if the configuration management client or VAL server is authorized to initiate the updated user profile subscription request.

3. The configuration management server replies with a updated user profile subscription response indicating the subscription status.

Figure 11.3.4.5-2 illustrates the high level procedure of updated user profile notification event.
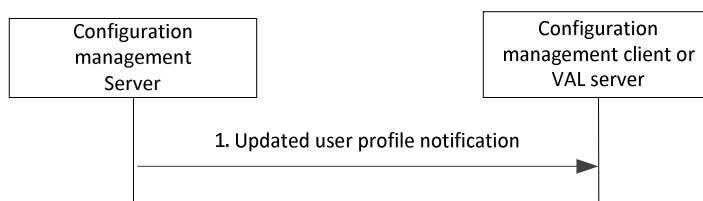
Figure 11.3.4.5-2: Updated user profile notification

1. The configuration management server sends the updated user profile notification including the changes to user profile of one or more VAL users or VAL UEs to the configuration management client or VAL server.

NOTE: Updated user profile notification is based on the subscription.

11.4   SEAL APIs for configuration management

11.4.1   General

Table 11.4.1-1 illustrates the SEAL APIs for configuration management.

Table 11.4.1-1: List of SEAL APIs for configuration management

API Name	API Operations	Known Consumer(s)	Communication Type
SS_UserProfileRetrieval	Obtain_User_Profile	VAL server	Request /Response
SS_UserProfileEvent	Subscribe_User_Profile_Update	VAL server	Subscribe/Notify
	Notify_User_Profile_Update	VAL server	

11.4.2   SS_UserProfileRetrieval API

11.4.2.1   General

API description: This API enables the VAL server to communicate with the configuration management server for obtaining user profile over CM-S.

11.4.2.2   Obtain_User_Profile operation

API operation name: Obtain_User_Profile

Description: Obtaining user profile.

Known Consumers: VAL server.

Inputs: See subclause 11.3.2.3

Outputs: See subclause 11.3.2.4

See subclause 11.3.4.2 for the details of usage of this API operation.

11.4.3   SS_UserProfileEvent API

11.4.3.1   General

API description: This API enables the VAL server to communicate with the configuration management server for obtaining updated user profile over CM-S.

11.4.3.2   Subscribe_User_Profile_Update operation

API operation name: Subscribe_User_Profile_Update

Description: Subscribing to changes to user profile.

Known Consumers: VAL server.

Inputs: See subclause 11.3.2.10

Outputs: See subclause 11.3.2.11

See subclause 11.3.4.5 for the details of usage of this API operation.

11.4.3.3   Notify_User_Profile_Update operation

API operation name: Notify_User_Profile_Update

Description: Notification for changes to user profile.

Known Consumers: VAL server.

Inputs: See subclause 11.3.2.12

Outputs: See subclause 11.3.2.12

See subclause 11.3.4.5 for the details of usage of this API operation.

12 Identity management

12.1 General

The identity management is a SEAL service that offers the identity management related capabilities to one or more vertical applications.

12.2 Functional model for identity management

12.2.1 General

The functional model for the identity management is based on the generic functional model specified in clause 6. It is organized into functional entities to describe a functional architecture which addresses the support for identity management aspects for vertical applications. The on-network and off-network functional model is specified in this clause.

12.2.2 On-network functional model description

Figure 12.2.2-1 illustrates the generic on-network functional model for identity management.
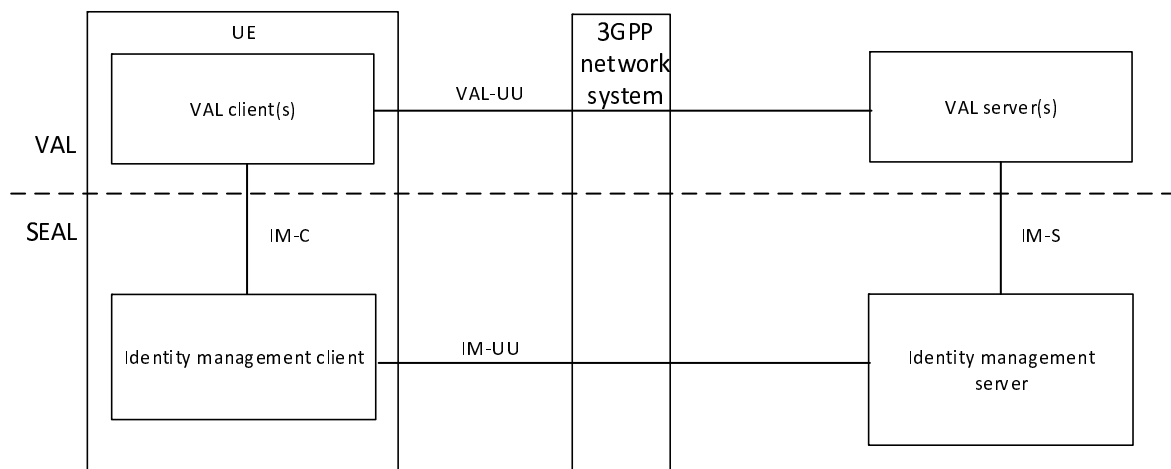
Figure 12.2.2-1: On-network functional model for identity management

The identity management client communicates with the identity management server over the IM-UU reference point. The identity management client provides the support for identity management functions to the VAL client(s) over IM-C reference point. The VAL server(s) communicate with the identity management server over the IM-S reference point.

Editor's Note: The role of VAL-UU in the context of identity management is FFS.

12.2.3 Off-network functional model description

Figure 12.2.3-1 illustrates the off-network functional model for identity management.
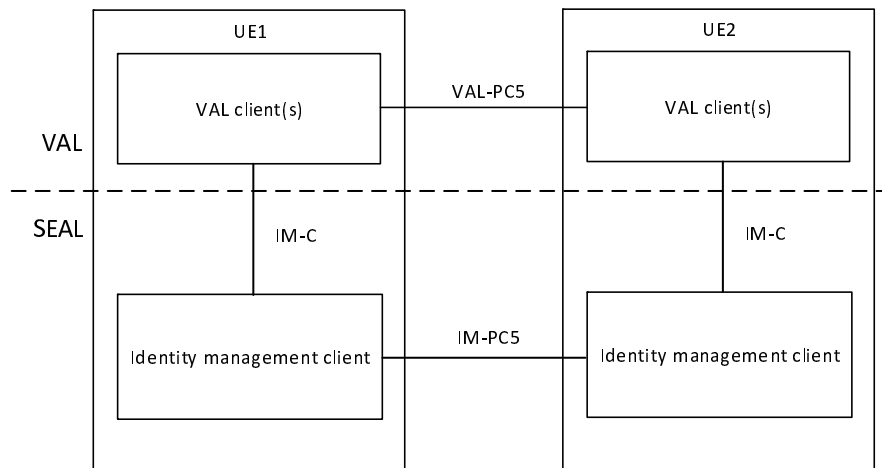
Figure 12.2.3-1: Off-network functional model for identity management

The identity management client of the UE1 communicates with the identity management client of the UE2 over the IM-PC5 reference point.

12.2.4　Functional entities description

12.2.4.1　General

The functional entities for identity management SEAL service are described in the following subclauses.

12.2.4.2　Identity management client

The identity management client functional entity acts as the application client for vertical applications layer user identity related transactions. The identity management client interacts with the identity management server. The identity management client also supports interactions with the corresponding identity management client between the two UEs.

12.2.4.3　Identity management server

The identity management server is a functional entity that authenticates the vertical application layer user identity. The authentication is performed by verifying the credentials provided by the vertical applications' user. The identity management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The identity management server also supports interactions with the corresponding identity management server in distributed SEAL deployments.

12.2.5　Reference points description

12.2.5.1　General

The reference points for the functional model for identity management are described in the following subclauses.

12.2.5.2　IM-UU

The interactions related to identity management functions between the identity management client and the identity management server are supported by IM-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

12.2.5.3　IM-PC5

The interactions related to identity management functions between the identity management clients located in different VAL UEs are supported by IM-PC5 reference point. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [12].

12.2.5.4 IM-C

The interactions related to identity management functions between the VAL client(s) and the identity management client within a VAL UE are supported by IM-C reference point.

12.2.5.5 IM-S

The interactions related to identity management functions between the VAL server(s) and the identity management server are supported by IM-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

12.2.5.6 IM-E

The interactions related to identity management functions between the identity management servers in a distributed deployment are supported by IM-E reference point.

> Editor's Note: The functions enabled over IM-E reference point is FFS.

12.3 Procedures and information flows for identity management

12.3.1 General

The procedures related to the identity management are described in the following subclauses.

12.3.2 Information flows

> NOTE: The procedure for identity management is specified in subclause 5.2.3 and 5.2.4 of 3GPP TS 33.434 [29].

12.3.3 General user authentication and authorization for VAL services

12.3.3.1 General

The high level user authentication and authorization procedure is described in the following subclause.

12.3.3.2 Primary VAL system

Figure 12.3.3.2-1 is a high level user authentication and authorization flow.

> NOTE: The specific user authentication and authorization architecture required by the VAL services in order to realize the VAL user authentication and authorization is specified in subclauses 5.2.3, 5.2.4 and 5.2.5 of 3GPP TS 33.434 [29].

The user authentication process shown in figure 12.3.3.2-1 may take place in some scenarios as a separate step independently from a SIP registration phase, for example if the SIP core is outside the domain of the VAL server.

> Editor's note: The procedure described in this subclause as shown in Figure 12.3.3.2-1 may require further study.

A procedure for user authentication is illustrated in figure 12.3.3.2-1. Other alternatives may be possible, such as authenticating the user within the SIP registration phase.
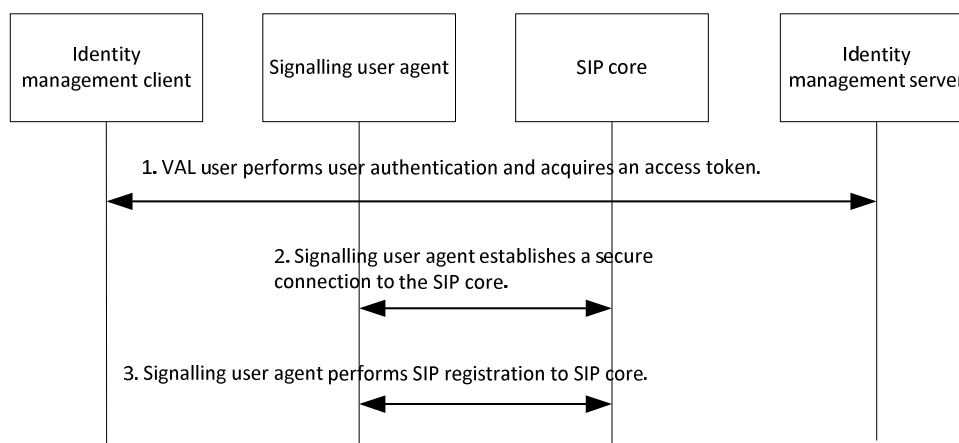
Figure 12.3.3.2-1: VAL user authentication and registration with Primary VAL system, single domain

1. In this step the identity management client begins the user authorization procedure. The VAL user supplies the user credentials (e.g. biometrics, secureID, username/password) for verification with the identity management server. This step may occur before or after step 3. In a VAL system with multiple VAL services, a single user authentication as in step 1 can be used for multiple VAL service authorizations for the user.

2. The signalling user agent establishes a secure connection to the SIP core for the purpose of SIP level authentication and registration.

3. The signalling user agent completes the SIP level registration with the SIP core (and an optional third-party registration with the VAL service server(s)).

NOTE 1: The VAL client(s) perform the corresponding VAL service authorization for the user by utilizing the result of this procedure.

NOTE 2: Steps 2 and 3 are not required to be performed if the VAL service does not use SIP.

12.3.3.3 Interconnection partner VAL system

Where communications with a partner VAL system using interconnection are required, user authorization takes place in the serving VAL system of the VAL service user, using the VAL user service authorization procedure specified in subclauses 5.2.5 and 5.2.6 of 3GPP TS 33.434 [29].

12.4 SEAL APIs for identity management

12.4.1 General

There are no APIs defined for SEAL Identity Management.

12.4.2 Void

12.4.2.1 Void

12.4.2.2 Void

13 Key management

13.1 General

The key management is a SEAL service that offers the key management related capabilities to one or more vertical applications.

13.2 Functional model for key management

13.2.1 General

The functional model for the key management is based on the generic functional model specified in clause 6. It is organized into functional entities to describe a functional architecture which addresses the support for key management aspects for vertical applications. The on-network and off-network functional model is specified in this clause.

13.2.2 On-network functional model description

Figure 13.2.2-1 illustrates the generic on-network functional model for key management.
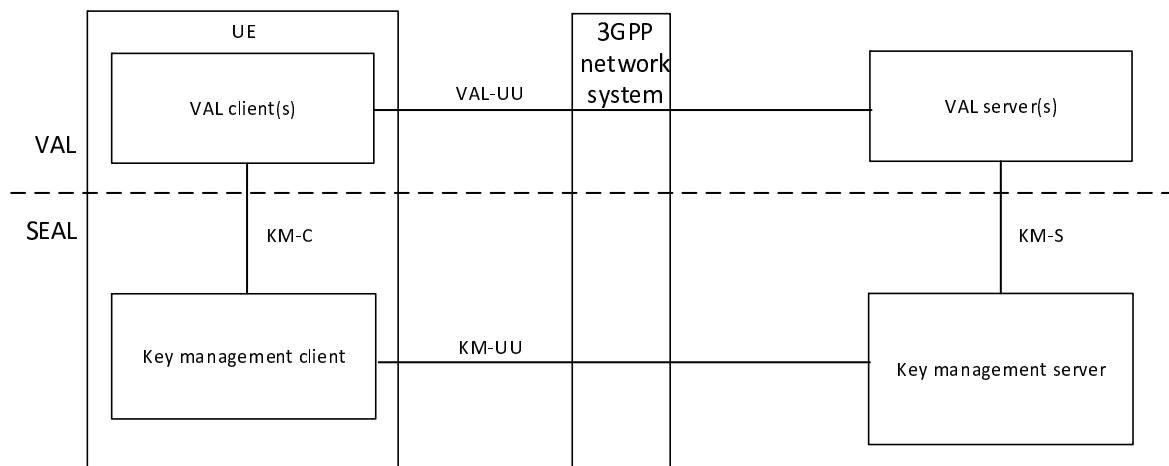
Figure 13.2.2-1: On-network functional model for key management

The key management client communicates with the key management server over the KM-UU reference point. The key management client provides the support for key management functions to the VAL client(s) over KM-C reference point. The VAL server(s) communicate with the key management server over the KM-S reference point.

13.2.3 Off-network functional model description

Figure 13.2.3-1 illustrates the off-network functional model for key management.
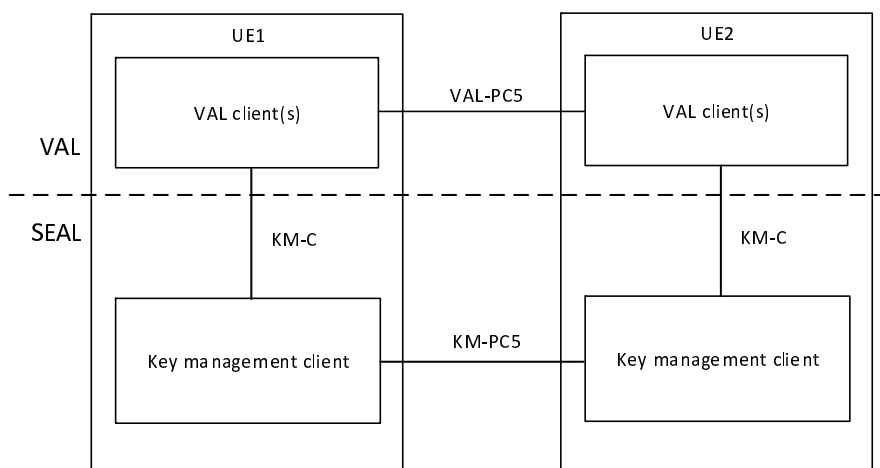
Figure 13.2.3-1: Off-network functional model for key management

The key management client of the UE1 communicates with the key management client of the UE2 over the KM-PC5 reference point.

13.2.4 Functional entities description

13.2.4.1 General

The functional entities for key management SEAL service are described in the following subclauses.

13.2.4.2 Key management client

The key management functional entity acts as the application client for key management functions. It interacts with the key management server. The key management client also supports interactions with the corresponding key management client between the two UEs.

 NOTE: The functionality of the key management client is specified in subclause 5.3 of 3GPP TS 33. 434 [29].

13.2.4.3 Key management server

The key management server is a functional entity that stores and provides security related information (e.g. encryption keys) to the key management client, group management server and vertical application server to achieve the security goals of confidentiality and integrity of media and signalling. The key management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The key management server also supports interactions with the corresponding key management server in distributed SEAL deployments.

 NOTE: The functionality of the key management server is specified in subclause 5.3 of 3GPP TS 33.434 [29].

13.2.5 Reference points description

13.2.5.1 General

The reference points for the functional model for key management are described in the following subclauses.

13.2.5.2 KM-UU

The interactions related to key management functions between the key management client and the key management server are supported by KM-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

KM-UU reference point provides a means for the key management server to provide security related information (e.g. encryption keys) to the key management client. The KM-UU reference point shall use the HTTP-1 and HTTP-2

signalling control plane reference points for transport and routing of security related information to the key management client.

NOTE: KM-UU reference point is specified in subclause 5.1.1.4 of 3GPP TS 33.434 [29].

13.2.5.3 KM-PC5

The interactions related to key management functions between the key management clients located in different VAL UEs are supported by KM-PC5 reference point. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [12].

13.2.5.4 KM-C

The interactions related to key management functions between the VAL client(s) and the key management client within a VAL UE are supported by KM-C reference point.

13.2.5.5 KM-S

The interactions related to key management functions between the VAL server(s) and the key management server are supported by KM-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

KM-S reference point provides a means for the key management server to provide security related information (e.g. encryption keys) to the VAL server. The KM-S reference point shall use the HTTP-1 and HTTP-2 signalling control plane reference points for transport and routing of security related information to the VAL server.

NOTE: KM-S is specified in subclause 5.1.1.4 of 3GPP TS 33.434 [29].

13.2.5.6 KM-E

The interactions related to key management functions between the key management servers in a distributed deployment are supported by KM-E reference point.

Editor's Note: The functions enabled over KM-E reference point is FFS.

13.2.5.7 SEAL-X1

NOTE: SEAL-X1 reference point between the key management server and the group management server is described in subclause 6.5.9.2.

13.3 Procedures and information flows for key management

NOTE: The procedure for key management is specified in subclause 5.3 of 3GPP TS 33.434 [29].

13.4 SEAL APIs for key management

13.4.1 General

The SEAL APIs for Key Management are specified in subclauses 5.7.1 and 7.6.1 of 3GPP TS 29.549 [30].

13.4.2　Void

13.4.2.1　Void

13.4.2.2　Void

14　Network resource management

14.1　General

The network resource management is a SEAL service that offers the network resource management (e.g. unicast and multicast network resources) and monitoring related capabilities to one or more vertical applications.

14.2　Functional model for network resource management

14.2.1　General

The functional model for the network resource management is based on the generic functional model specified in clause 6. It is organized into functional entities to describe a functional architecture which addresses the support for network resource management aspects for vertical applications. The on-network and off-network functional model is specified in this clause.

14.2.2　On-network functional model description

14.2.2.1　Generic on-network functional model for network resource management

Figure 14.2.2-1 illustrates the generic on-network functional model for network resource management.
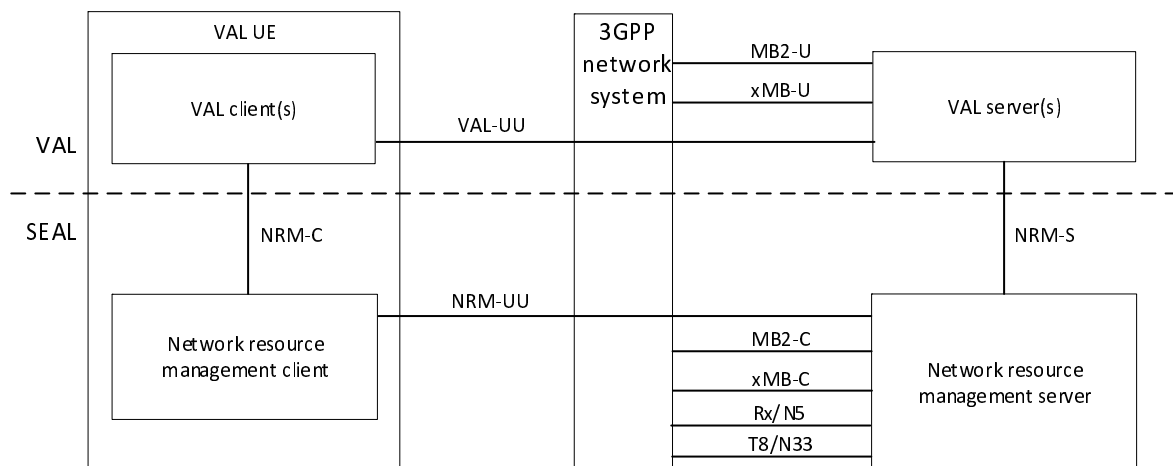
Figure 14.2.2.1-1: On-network functional model for network resource management

The network resource management client communicates with the network resource management server over the NRM-UU reference point. The network resource management client provides the support for network resource management functions to the VAL client(s) over NRM-C reference point. The VAL server(s) communicate with the network resource management server over the NRM-S reference point.

The network resource management server communicates with the BM-SC via MB2-C and xMB-C reference points to obtain and control the multicast resources from the underlying 3GPP network system. The network resource management server communicates with the PCRF via Rx reference point or communicates with the PCF via N5 reference point to control the unicast resources from the underlying 3GPP network system. The network resource

management server communicates with the SCEF via T8 reference point or communicates with the NEF via N33 reference point to perform event monitoring procedures from the underlying 3GPP network system. The network resource management server interacts with NEF via N33 to obtain QoS monitoring information from the 5GS.

14.2.2.2 On-network functional model for network resource management for TSN

The architecture for integration of the 5G with TSN [36] is depicted in Figure 14.2.2.2-1. The SEAL Network Resource Management (NRM) server acts as a TSN AF (defined in [10] in clause 5.28.1). TSN CNC (defined in [35]) via the NRM-S reference point configures the TSN flows in the 5GS. In this case the NRM-S supports the IEEE 802.1Qcc management protocol. As a TSN AF the SEAL NRM server interacts with the 5GS PCF over the N5 reference point to configure the 5G QoS and TSCAI parameters in the 5GS.
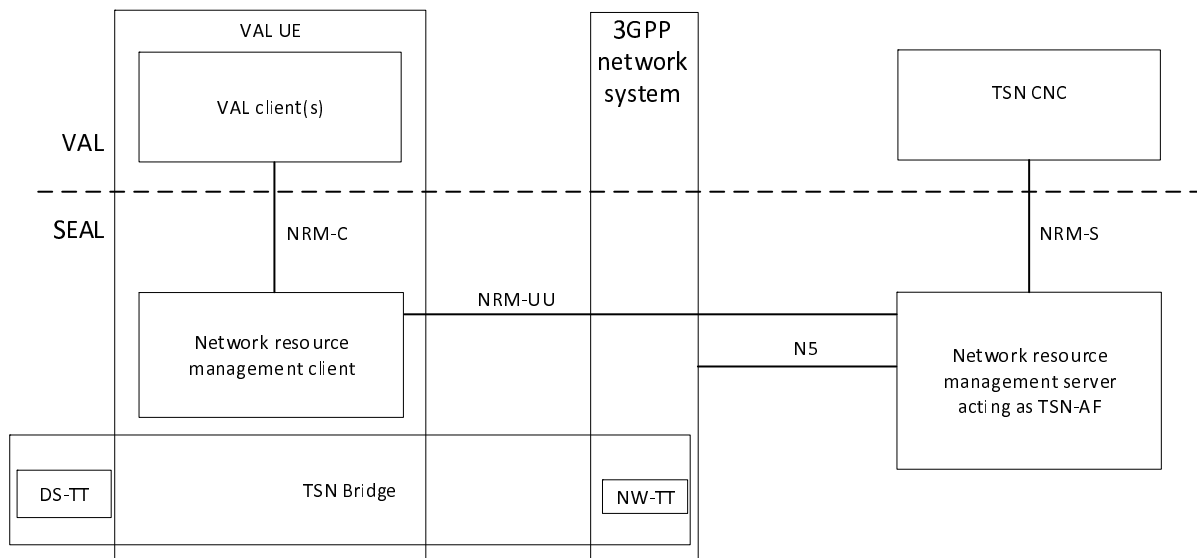
Figure 14.2.2.2-1: On-network functional model for network resource management for TSN

NOTE: Whether DS-TT and UE are combined or are separate is up to implementation.

Acting as the TSN AF the NRM server collects 5GS TSN Bridge information by interaction with the 5GS via the N5 reference point, as described in in TS 23.502 [11] Annex F.1.

NRM server triggers via N5 the AF request procedure as described in 3GPP TS 23.502 [11] Annex F.2.

14.2.2.3 On-network functional model for network resource management for 5G TSC

5G TSC refers to time sensitive communication service offered within the 5G system (i.e. without integration with a TSN system) by the 5GS for the UEs connected to the 5GS. The architecture for the 5G TSC is depicted in Figure 14.2.2.3-1. The SEAL NRM server acts as an AF towards the 5G Core Network and performs coordination of QoS flows to fulfill the end-to-end QoS requirements for the UEs involved in the TSC communication. It combines the roles of TSCTSF and TSC CNC (similar to the TSN CNC in the TSN integration case), which means that it controls the allocation of resources of TSC communication within the boundaries of the 5G domain.

Upon request from a VAL server via the NRM-S reference point it configures the TSC end-to-end QoS flows in the 5GS. In line with other SEAL service enablers the SEAL NRM server provides a RESTful interface on the NRM-S reference point. As a TSCTSF the SEAL NRM server interacts with the 5GS PCF over the N5 reference point to configure the 5G QoS and TSCAI parameters in the 5GS.
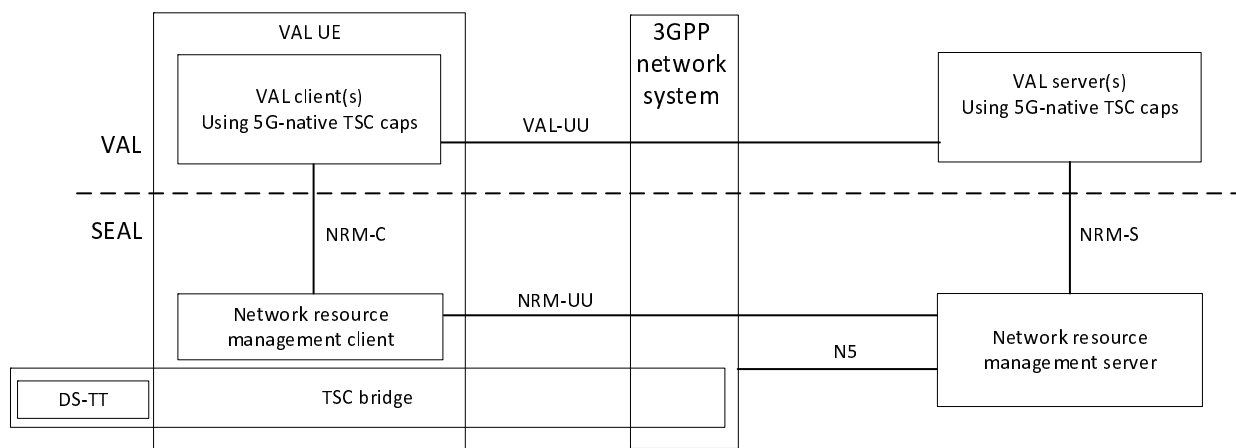
Figure 14.2.2.3-1: On-network functional model for network resource management for 5G TSC

14.2.3 Off-network functional model description

Figure 14.2.3-1 illustrates the off-network functional model for network resource management.
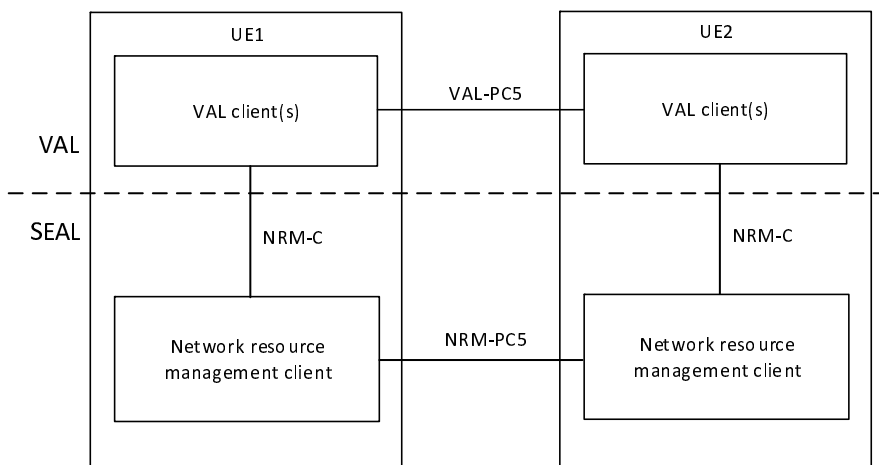
Figure 14.2.3-1: Off-network functional model for network resource management

The network resource management client of the UE1 communicates with the network resource management client of the UE2 over the NRM-PC5 reference point.

Editor's note: Whether off-network support is required for network resource management is FFS.

14.2.4 Functional entities description

14.2.4.1 General

The functional entities for network resource management SEAL service are described in the following subclauses.

14.2.4.2 Network resource management client

The network resource management client functional entity acts as the application client for the management of network resources. The network resource management client interacts with the network resource management server.

14.2.4.3   Network resource management server

The network resource management server functional entity provides for management of 3GPP system network resources (e.g. unicast, multicast) and monitoring events to support the VAL applications. The network resource management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The network resource management server also supports interactions with the corresponding network resource management server in distributed SEAL deployments. The NRM server's role may be assumed by the VAL server in some deployments, in which case, the VAL server performs the procedures for network resource management of the NRM server.

14.2.5   Reference points description

14.2.5.1   General

The reference points for the functional model for network resource management are described in the following subclauses.

14.2.5.2   NRM-UU

The interactions related to network resource management functions between the network resource management client and the network resource management server are supported by NRM-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

14.2.5.3   NRM-PC5

The interactions related to network resource management functions between the network resource management clients located in different VAL UEs are supported by the NRM-PC5 reference point. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [12].

> Editor's note: Whether NRM-PC5 reference point is required for network resource management is FFS.

14.2.5.4   NRM-C

The interactions related to network resource management functions between the VAL client(s) and the network resource management client within a VAL UE are supported by the NRM-C reference point.

> Editor's note: Whether NRM-C reference point is required for network resource management is FFS.

14.2.5.5   NRM-S

The interactions related to network resource management functions between the VAL server(s) and the network resource management server are supported by the NRM-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

14.2.5.6   NRM-E

The interactions related to network resource management functions between the network resource management servers in a distributed deployment are supported by NRM-E reference point.

> Editor's Note: The functions enabled over NRM-E reference point is FFS.

14.2.5.7   MB2-C

The reference point MB2-C supports the control plane interactions between the network resource management server and the BM-SC and is specified in 3GPP TS 29.468 [22].

14.2.5.8   xMB-C

The reference point xMB-C supports the control plane interactions between the network resource management server and the BM-SC and is specified in 3GPP TS 26.348 [20].

14.2.5.9   Rx

The reference point Rx supports the interactions between the network resource management server and the PCRF and is specified in 3GPP TS 29.214 [21].

14.2.5.10   N5

The reference point N5 supports the interactions between the network resource management server and the PCF and is specified in 3GPP TS 23.501 [10].

14.2.5.11   N33

The reference point N33 supports the interactions between the network resource management server and the NEF and is specified in 3GPP TS 23.501 [10].

14.3   Procedures and information flows for network resource management

14.3.1   General

The procedures related to the network resource management are described in the following subclauses.

14.3.2   Information flows

14.3.2.1   Network resource adaptation request

Table 14.3.2.1-1 describes the information flow network resource adaptation request from the VAL server to the NRM server.

Table 14.3.2.1-1: Network resource adaptation request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
List of VAL UE IDs	O (see NOTE)	List consisting of one or more VAL UE IDs for whom the network resource adaptation occurs.
VAL group ID	O (see NOTE)	The VAL group ID for whom the network resource adaptation occurs.
Resource adaptation requirement	M	The resource adaptation requirement corresponds to the VAL service QoS requirements as applied for a UE or group of UEs (E.g. bandwidth, resource).
NOTE: Either of the information elements should be present.		

14.3.2.2   Network resource adaptation response

Table 14.3.2.2-1 describes the information flow network resource adaptation response from the NRM server to the VAL server.

Table 14.3.2.2-1: Network resource adaptation response

Information element	Status	Description
Result	M	Result includes success or failure of the network resource adaptation with the underlying network. The response can also include an updated value for some of the parameters included in the network resource adaptation request (e.g. negotiation of resource offering)

14.3.2.3   MBMS bearer announcement

Table 14.3.2.3-1 describes the information flow MBMS bearer announcement from the NRM server to the NRM client.

Table 14.3.2.3-1: MBMS bearer announcement

Information element	Status	Description
TMGI	M	TMGI information
Alternative TMGI	O	A list of additional alternative TMGI may be included and used in roaming scenarios.
QCI	O	QCI information used by the ProSe UE-Network Relay to determine the ProSe Per-Packet Priority value to be applied for the multicast packets relayed to Remote UE over PC5
List of service area identifier	M	A list of service area identifier for the applicable MBMS broadcast area.
Frequency	O	Identification of frequency if multi carrier support is provided
SDP information	M	SDP with media and application control information applicable to groups that can use this bearer (e.g. codec, protocol id, FEC information)
Monitoring state	O	The monitoring state is used to control if the client is actively monitoring the MBMS bearer quality or not.
Announcement acknowledgment	O	Indicate if the NRM server requires an acknowledgement of the MBMS bearer announcement.
Unicast status	O	An indication that the listening status of the unicast bearer is requested.
ROHC information	O	Indicate the usage of ROHC and provide the parameters of the ROHC channel to signal to the ROHC decoder.
NOTE: When MBMS bearer announcement is done on a MBMS bearer all attributes above are optional except the TMGI.		

14.3.2.4   MBMS listening status report

Table 14.3.2.4-1 describes the information flow for the MBMS listening status report from NRM client to NRM server.

Table 14.3.2.4-1: MBMS listening status report

Information element	Status	Description
VAL user ID or VAL UE ID	M	The identity of the VAL user or VAL UE who wants to report the MBMS listening status.
TMGI(s)	M	TMGI(s) information.
MBMS listening status(s)	M	The MBMS listening status per TMGI.
MBMS reception quality level	O	The reception quality level per TMGI (see NOTE)
Unicast listening status	O	The unicast listening status.
NOTE: The set of quality levels helps service continuity in MBMS scenarios. A reception quality level may help to make an efficient switching decision to another bearer. How these levels are used is implementation specific.		

14.3.2.5   MBMS suspension reporting instruction

Table 14.3.2.5-1 describes the information flow for the MBMS suspension reporting instruction from NRM server to NRM client in a unicast bearer for MBMS suspension reporting.

Table 14.3.2.5-1: MBMS suspension reporting instruction (unicast)

Information element	Status	Description
VAL user ID or VAL UE ID	M	The identity of the VAL user or VAL UE.
Suspension reporting	M	Enables or disable the suspension reporting for a specific NRM client

Table 14.3.2.5-2 describes the information flow for the MBMS suspension reporting instruction from NRM server to NRM client in a multicast bearer for MBMS suspension reporting.

Table 14.3.2.5-2: MBMS suspension reporting instruction (multicast)

Information element	Status	Description
Suspension reporting client subset	M	Contains a uniquely defined subset of NRM clients that shall report MBMS suspension

14.3.2.6 Resource request

Table 14.3.2.6-1 describes the information flow for the resource request from VAL server to NRM server for unicast resources.

Table 14.3.2.6-1: Resource request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL user ID or VAL UE ID	M	The identity of the VAL user or VAL UE.
VAL service requirement information (see NOTE)	O	VAL service requirements for unicast resource (e.g. VAL service ID, Bitrate)
NOTE: When this information element is not included, the NRM server considers default VAL service requirement for the unicast resources.		

14.3.2.7 Resource response

Table 14.3.2.7-1 describes the information flow for the resource response from NRM server to VAL server for unicast resources.

Table 14.3.2.6-1: Resource response

Information element	Status	Description
Result	M	The result indicates success or failure of the resource request operation.

14.3.2.8 Resource modification request

Table 14.3.2.8-1 describes the information flow for the resource modification request from VAL server to NRM server for unicast resources.

Table 14.3.2.8-1: Resource modification request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL user ID or VAL UE ID	M	The identity of the VAL user or VAL UE.
VAL service requirement information	M	VAL service requirements for unicast resource (e.g. VAL sevice ID, Bitrate)

14.3.2.9 Resource modification response

Table 14.3.2.9-1 describes the information flow for the resource modification response from NRM server to VAL server for unicast resources.

Table 14.3.2.9-1: Resource modification response

Information element	Status	Description
Result	M	The result indicates success or failure of the resource modification operation.

14.3.2.10 MBMS bearers request

Table 14.3.2.10-1 describes the information flow for the MBMS bearers request from VAL server to NRM server.

Table 14.3.2.10-1: MBMS bearers request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL group ID	M	The identity of the group that the MBMS bearer is requested for.
Service announcement mode	M	Indicates whether the request is sent by NRM server or by the VAL server
QoS	M	Indicates the requested QoS for the bearer
Broadcast area	O	Indicate the area where the MBMS bearer is requested for
Endpoint information	M	Information of the endpoint of the VAL server to which the user plane notifications have to be sent.
Local MBMS information (see NOTE)	O	
> MB2-U information	O	IP address, UDP port number of the MB2-U interface
> xMB-U information	O	IP address, UDP port number of the xMB-U interface
> M1 interface information	O	M1 interface information for local MBMS
Local MBMS activation indication (see NOTE)	O	Indicates whether to request the NRM server to use Local MBMS information.
NOTE: The VAL server may provide either the Local MBMS information or the Local MBMS activation indication. This IE is present when the local MBMS is required for VAL services like V2X service.		

14.3.2.11 MBMS bearers response

Table 14.3.2.11-1 describes the information flow for the MBMS bearers response from NRM server to VAL server.

Table 14.3.2.11-1: MBMS bearers response

Information element	Status	Description
Result	M	The result indicates success or failure of the MBMS bearers request operation.
TMGI	O (see NOTE 1)	TMGI information.
User plane address	M (see NOTE 2)	BM-SC user plane IP address and port
Service description	O (see NOTE 2)	Indicates MBMS bearer related configuration information as defined in 3GPP TS 26.346 [28] (e.g. radio frequency and MBMS Service Area Identities)
NOTE 1: TMGI may not be required if the service announcement mode indicates that the request is sent by the NRM server.		
NOTE 2: If the Result Information element indicates failure then the values of the other information elements have no meaning.		

14.3.2.12 User plane delivery mode

Table 14.3.2.12-1 describes the information flow for the user plane delivery mode from NRM server to VAL server.

Table 14.3.2.12-1: User plane delivery mode

Information element	Status	Description
Delivery mode	M	Indicates whether to deliver the user data to the UE(s) via unicast mode or multicast mode
MBMS media stream identifier	M	Indicates the MBMS media stream to be used to deliver the media currently over unicast, or the MBMS media stream currently being used.
Unicast media stream identifier(s)	M	Indicates the unicast media stream to be used to deliver the media currently over multicast, or the unicast to be stopped and switched to multicast.

14.3.2.13 end-to-end QoS management request

Table 14.3.2.13-1 describes the information flow end-to-end QoS management request from the NRM client to the NRM server.

Table 14.3.2.13-1: end-to-end QoS management request

Information element	Status	Description
List of VAL UEs	M	List of VAL UEs for whom the end-to-end QoS management occurs
>VAL UE/user ID	M	Identity of the VAL UE
> IP address	M	IP address of the VAL UE
VAL service ID	O	The VAL service identity for whom the end-to-end QoS management occurs.
End-to-end QoS requirements	O	The application QoS requirements / KPIs (latency, error rate, ..) for the end-to-end session. This may optionally include information which will support the NRM server to identify the per session QoS requirements (e.g. a flag indicating the use of HD video for assisting the end-to-end session, a video resolution/encoding required for the HD video).
Service area	O	The area where the QoS management request applies. This can be geographical area, or topological area.
Time validity	O	The time of validity of the requirement.

14.3.2.14   end-to-end QoS management response

Table 14.3.2.14-1 describes the information flow end-to-end QoS management response from the NRM server to the NRM client.

Table 14.3.2.14-1: end-to-end QoS management response

Information element	Status	Description
Result	M	The positive or negative result of the end-to-end QoS management request.
QoS report configuration	O	The configuration of the NRM client's report triggering by NRM server (e.g. setting thresholds for reporting a QoS downgrade / notifications based on channel loss great than threshold value)

14.3.2.15   QoS downgrade indication

Table 14.3.2.15-1 describes the information flow QoS downgrade indication from the NRM client to the NRM server.

Table 14.3.2.15-1: QoS downgrade indication

Information element	Status	Description
VAL UE ID	M	The identifier of the VAL UE which indicates the QoS downgrade.
QoS downgrade report	M	The report including the expected or actual QoS / QoE parameters which were downgraded (i.e. latency, throughput, reliability, jitter). This report may be configured by the end-to-end QoS management response message.

14.3.2.16   Application QoS change notification

Table 14.3.2.16-1 describes the information flow Application QoS change notification from the NRM server to the NRM clients (which are involved at the end-to-end session).

Table 14.3.2.16 -1: Application QoS change notification

Information element	Status	Description
NRM server ID	M	The identifier of the NRM server which provides the notification.
Requested QoS parameters	M	The updated requested QoS parameters for the end-to-end session (NRM server to source VAL UE or NRM server to target VAL UE), based on the QoS change on one or both links involved in the network-assisted end-to-end communication.

14.3.2.17 Monitoring Events Subscription Request

Table 14.3.2.17-1 describes the information flow from the VAL server to the NRM server for monitoring events subscription request.

Table 14.3.2.17-1: Monitoring Events Subscription request

Information element	Status	Description
Identities list	O (see NOTE 1)	List of VAL users or VAL UEs whose events monitoring is requested.
VAL group ID	O (see NOTE 1)	VAL group ID of the VAL UE group of target UEs.
VAL service ID	O	VAL service ID.
Monitoring profile ID	O (see NOTE 2)	The monitoring profile ID, which identifies a list of monitoring and/or analytics events.
Validity conditions	O	The temporal and/or spatial conditions applied for the events to be considered as valid.
Event Details	O (see NOTE 2)	List of monitoring and/or analytics events that the VAL server is interested in.
NOTE 1: For identifying the target UE(s), either a list of VAL users/UEs or a group of VAL UEs shall be provided.		
NOTE 2: Either Event Details or Monitoring profile ID is present.		

14.3.2.18 Monitoring Events Subscription Response

Table 14.3.2.18-1 describes the information flow from the NRM server to the VAL server for Monitoring Events Subscription response.

Table 14.3.2.18-1: Monitoring Events Subscription response

Information element	Status	Description
Subscription status	M	It indicates the subscription result
Monitoring profile ID	O	It indicates the monitoring profile identifier. It is present when Event Details are provided in the Monitoring Events Subscription request.

14.3.2.19 Monitoring Events Notification message

Table 14.3.2.19-1 describes the information flow from the NRM server to the VAL server on notification of monitoring events.

Table 14.3.2.19-1: Monitoring Events Notification

Information element	Status	Description
EventDetails		List of events related to VAL UE(s).
> identity	M	VAL UE for which the events are related to.
> events	M	List of Monitoring and Analytics events related to the VAL UE.
Timestamp	O	The timestamp for the monitoring and analytics events

14.3.2.20 Unicast QoS monitoring subscription request

Table 14.3.2.20-1 describes the information flow from the VAL server to the network resource management server for unicast QoS monitoring subscription request.

Table 14.3.2.20-1: Unicast QoS monitoring subscription request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
List of VAL UE IDs	O (see NOTE 1)	List of VAL UEs whose QoS monitoring data is requested.
VAL group ID	O (see NOTE 1)	The group ID used for the VAL group for which QoS monitoring data is requested.
List of VAL stream IDs	O (see NOTE 1)	List of VAL streams for which QoS monitoring data is requested.
Measurement requirements	O	It describes the requirements on the QoS measurements.
> type of data	M	At least one of the following measurement index shall be provided.
>> packet delay	O	UL/DL/RT packet delay. For VAL stream, the packet delay means measurement from a source UE to a target UE.
>> packet loss rate	O	Average packet loss rate.
>> data rate	O	Average data rate and/or maximum data rate.
>> traffic volume	O	Average traffic volume for UL and/or DL
> measurement time period	O	The measurement time period indicates a current time period. If absent, current time and 5 minutes duration are used as default setting.
> aggregation granularity window	O	Indicates how long the QoS monitoring is performed to compute the average value and gather the maximum value. If absent, 1 minute is used as default setting.
Reporting requirements	O	It describes the requirements for QoS monitoring reporting.
> Frequency of reporting	O	It indicates the requested frequency of reporting. The reporting frequency may be periodic or event triggered (i.e. threshold reached). If absent in the request, default event triggered reporting is used.
> Reporting threshold	O	If the Frequency of reporting is event triggered (threshold reached), the reporting threshold corresponding to the measurement index shall be provided.
> Threshold reaching direction	O	It indicates the reaching direction (i.e. ascending, descending or crossed) for the reporting threshold. It shall be provided if reporting threshold is present.
> Reporting periodicity	O	If the Frequency of reporting is periodic, the reporting periodicity shall be provided.
> Termination of reporting	O	It indicates when the reporting of QoS monitoring shall stop. It can be event triggered (i.e. either number of reports reached or threshold reached) or when reporting duration expires or when explicit termination is requested. If absent in the request, it defaults to explicit termination. Once the termination condition is met, the monitoring subscription ceases to exist.
> Max number of reports	O (see NOTE 3)	It indicates the maximum number of reports, it shall be provided when Termination of reporting is set to event triggered (number of reports reached).
> Termination threshold	O (see NOTE 2, NOTE 3)	It indicates the reporting termination threshold corresponding to the measurement index. Each measurement index has only one termination threshold.
> Termination condition for termination threshold	O (see NOTE 2)	It indicates threshold-based termination condition (e.g. all reached or any of them reached) if multiple measurement indexes are provided.
> Reporting duration	O (see NOTE 3)	It indicates the reporting duration, it shall be provided when Termination of reporting is set to duration expiration.
NOTE 1: Only one of these information elements shall be present. NOTE 2: It shall be provided when Termination of reporting is set to event triggered (threshold reached). NOTE 3: Only one of these information elements may be present.		

14.3.2.21   Unicast QoS monitoring subscription response

Table 14.3.2.21-1 describes the information flow from the network resource management server to the VAL server for unicast QoS montoring subscription response.

Table 14.3.2.21-1: Unicast QoS monitoring subscription response

Information element	Status	Description
Subscription status	M	It indicates the subscription result

14.3.2.22   Unicast QoS monitoring notification

Table 14.3.2.22-1 describes the information flow for unicast QoS monitoring notification from the network resource management server to the VAL server.

Table 14.3.2.22-1: Notify unicast QoS monitoring event

Information element	Status	Description
List of VAL UE IDs	O (see NOTE)	List of VAL UEs whose QoS monitoring data is provided. This list is either the list provided in the subscription request or a subset of that list. It can contain a single UE.
VAL group ID	O (see NOTE)	The group ID used for the VAL group for which QoS monitoring data is provided. This group ID shall be the same VAL group ID as the VAL group ID provided in the subscription request.
List of VAL stream IDs	O (see NOTE)	List of VAL stream IDs whose QoS monitoring data is provided. This list is either the list provided in the subscription request or a subset of that list. It can contain a single stream ID.
QoS monitoring data	M	QoS monitoring data is an aggregate of QoS measurements data obtained from the 5GS.
NOTE: Only one of these information elements shall be present.		

14.3.2.23   TSC stream availability discovery request

Table 14.3.2.23-1 describes the information flow TSC stream availability discovery request from the VAL server to the NRM server.

Table 14.3.2.23-1: TSC stream availability discovery request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
Stream specification	M	Stream specification includes MAC addresses of the source and destination DS-TT ports (e.g. as defined in IEEE 802.1CB [37]).

14.3.2.24   TSC stream availability discovery response

Table 14.3.2.24-1 describes the information flow TSC stream availability discovery response from the NRM server to the VAL server.

Table 14.3.2.24-1: TSC stream availability discovery response

Information element	Status	Description
Result	M	Result includes success or failure of the TSC stream availability discovery with the underlying network.
Stream specification	M	Stream specification includes MAC addresses of the source and destination DS-TT ports (e.g. as defined in IEEE 802.1CB [37]).
List of traffic specifications	M	The traffic classes supported by the DS-TTs and available end-to-end MaxLatency value per traffic class. The VAL server should not request lower latency than the available end-to-end latency.

14.3.2.25 TSC stream creation request

Table 14.3.2.25-1 describes the information flow TSC stream creation request from the VAL server to the NRM server.

Table 14.3.2.25-1: TSC stream creation request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL Stream ID	M	It identifies the VAL stream.
Stream specification	M	Stream specification includes MAC addresses of the source and destination DS-TT ports (e.g. as defined in IEEE 802.1CB [37]).
Traffic specification	M	It includes MaxLatency, MaxFrameInterval, MaxFrameSize, MaxIntervalFrames, etc. (e.g. as described in IEEE 802.1Qcc [IEEE8021Qcc] in clause 46.2).

14.3.2.26 TSC stream creation response

Table 14.3.2.26-1 describes the information flow TSC stream creation response from the NRM server to the VAL server.

Table 14.3.2.26-1: TSC stream creation response

Information element	Status	Description
Result	M	Result includes success or failure of the TSC stream creation.
VAL Stream ID	M	It identifies the VAL stream.

14.3.2.27 TSC stream deletion request

Table 14.3.2.27-1 describes the information flow TSC stream deletion request from the VAL server to the NRM server.

Table 14.3.2.27-1: TSC stream deletion request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL Stream ID	M	It identifies the VAL stream.

14.3.2.28 TSC stream deletion response

Table 14.3.2.28-1 describes the information flow TSC stream deletion response from the NRM server to the VAL server.

Table 14.3.2.28-1: TSC stream deletion response

Information element	Status	Description
Result	M	Result includes success or failure of the network TSC stream deletion. Even in case of failure, the stream is deemed unusable.
VAL Stream ID	M	It identifies the VAL stream.

14.3.2.29 TSN bridge information report

The 5GS bridge management information is defined in TS 23.501 [10], clause 5.28.1 (5GS bridge management).

14.3.2.30 TSN bridge information confirmation

The 5GS bridge management information is defined in TS 23.501 [10], clause 5.28.1 (5GS bridge management).

14.3.2.31 TSN bridge configuration request

The configuration information of 5GS Bridge is defined in TS 23.501 [10], clause 5.28.2 (The configuration information of 5GS Bridge).

14.3.2.32 TSN bridge configuration response

The configuration information of 5GS Bridge is defined in TS 23.501 [10], clause 5.28.2 (The configuration information of 5GS Bridge).

14.3.2.33 Unicast QoS monitoring data request

Table 14.3.2.33-1 describes the information flow from the VAL server to the network resource management server for unicast QoS monitoring data request.

Table 14.3.2.33-1: Unicast QoS monitoring data request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
List of VAL UE IDs	O (see NOTE)	List of VAL UEs whose QoS monitoring data is requested.
VAL group ID	O (see NOTE)	The group ID used for the VAL group for which QoS monitoring data is requested.
List of VAL stream IDs	O (see NOTE)	List of VAL streams for which QoS monitoring data is requested.
Measurement requirements	M	It describes the requirements on the QoS measurement data to be provided.
> type of data	M	At least one of the following measurement index shall be provided.
>> packet delay	O	UL/DL/RT packet delay. For VAL stream, the packet delay means measurement from a source UE to a target UE.
>> packet loss rate	O	Average packet loss rate.
>> data rate	O	Average data rate and/or maximum data rate.
>> traffic volume	O	Average traffic volume for UL and/or DL
> measurement time period	O	The measurement time period indicates either a current or past time period. If absent, current time and 5 minutes duration are used as default setting.
> aggregation granularity window	O	Indicates how long the QoS monitoring is performed to compute the average value and gather the maximum value. If absent, 1 minute is used as default setting.
NOTE: Only one of these information elements shall be present.		

14.3.2.34 Unicast QoS monitoring data response

Table 14.3.2.34-1 describes the information flow from the VAL server to the network resource management server for unicast QoS monitoring data response.

Table 14.3.2.34-1: Unicast QoS monitoring data response

Information element	Status	Description
List of VAL UE IDs	O (see NOTE 1)	List of VAL UEs whose QoS monitoring data is provided. This list is either the list provided in the request or a subset of that list. It can contain a single UE.
VAL group ID	O (see NOTE 1)	The group ID used for the VAL group for which QoS monitoring data is provided. This group ID shall be the same VAL group ID as the VAL group ID provided in the request.
List of VAL stream IDs	O (see NOTE 1)	List of VAL stream IDs whose QoS monitoring data is provided. This list is either the list provided in the request or a subset of that list. It can contain a single stream ID.
Result	M	Indicates the success or failure for the operation
QoS monitoring data	M (see NOTE 2)	QoS monitoring data is an aggregate of QoS measurements data obtained from the 5GS.
Cause	O	Provides reason for the failure (e.g. when data for the requested time period is not available).
NOTE 1: Only one of these information elements shall be present. NOTE 2: If the Result information element indicates failure then the value of the QoS monitoring data information element has no meaning.		

14.3.3 Unicast resource management

14.3.3.1 General

The following subclauses specify the procedures for unicast resource management for vertical application layer. The NRM server sets up bearers and may need to modify the bearers for an already established VAL service communication.

Characteristics that may need to be modified include:

- activation and deactivation of the bearer;

- modification of the QoS characteristics of the bearer (e.g. bearer priority adjustment); and

- modification of GBR due to application requirement

   NOTE: A VAL service communication can consist of both unicast and multicast bearers which can all need modification due to the same event.

Vertical application layer specific pre-requisites and resultant behaviour by functional entities in performing these procedures are specified in the respective vertical application layer TS (e.g. for V2X application layer, see 3GPP TS 23.286 [7]).

Unicast resource management is supported with PCC interactions with SIP core and PCC interactions with NRM server. The PCC procedures for EPS are specified in 3GPP TS 23.203 [18] and the PCC procedures for 5GS are specified in 3GPP TS 23.503 [19].

14.3.3.2 Unicast resource management with SIP core

14.3.3.2.1 Request for unicast resources at VAL service communication establishment

14.3.3.2.1.1 General

The procedure defined in this subclause specifies how network resources are requested at VAL service communication establishment. If concurrent sessions are used the NRM server may utilize the capability of resource sharing specified for underlying network policy and charging functions. The request for resources includes application type, bandwidth, priority, application identifier and resource sharing information.

14.3.3.2.1.2 Procedure

The procedure is generic to any type of session establishment that requires requests for network resources.

Procedures in figure 14.3.3.2.1.2-1 are the signalling procedures for the requesting resource at session establishment.

Pre-condition:

- The VAL client has requested VAL service communication with the VAL server.

Figure 14.3.3.2.1.2-1: Resource request at VAL service communication establishment

1. The VAL server sends request for resources to the NRM server.

2. The NRM server evaluates the need for network resources and use of resource sharing.

3. The NRM server sends a session progress request containing request for resources.

4. PCC procedures are initiated from SIP core local inbound/outbound proxy.

5. The SIP core local inbound / outbound proxy sends a OK message to the NRM server.

6. The NRM server sends a resource response to the VAL server.

7. The VAL service communication is established, and resources have been allocated.

14.3.3.2.2 Request for modification of unicast resources

14.3.3.2.2.1 General

To modify unicast bearers, the NRM server shall send a resource modification request containing the parameters to be modified for the UE.

Possible scenarios when this procedure may be used are:

- Modify the allocation and retention priority for unicast resources;

- Release and resume resources in-between VAL service communications; or

- Release and resume resources when a UE is able to receive the VAL service communications over multicast transmission

14.3.3.2.2.2 Procedure

Procedures in figure 14.3.3.2.2.2-1 are the signalling procedures for the modification of a unicast:

Pre-condition:

- A VAL service communication is already in progress;

Figure 14.3.3.2.2.2-1: Bearer modification request

1. The VAL server sends a resource modification request to the NRM server.

2a. The NRM server decides to modify the parameters of a unicast bearer.

2b. If the media bearer modification is not required, the NRM server sends a resource modification response to the VAL server.

3. The NRM server sends a session update which includes a resource modification request containing the modified parameters of the unicast bearer.

4. PCC procedures are initiated from SIP core local inbound/outbound proxy.

5. The SIP core local inbound / outbound proxy sends a OK message to the NRM server.

6. The NRM server sends a resource modification response to the VAL server.

7. The VAL service communication continues with the modified unicast resources.

NOTE 1: If the VAL service communication is transferred to multicast transmission, the unicast resources could be temporarily be released.

NOTE 2: If multiple VAL service communication streams are sent to the UE, additional bearer resources could be required during an established VAL service communication. Pre-allocation of additional bearer resources already at VAL service communication establishment could be useful.

14.3.3.3 Unicast resource management without SIP core

14.3.3.3.1 Network resource adaptation

14.3.3.3.1.1 General

This subclause describes the procedure for network resource adaptation using PCC procedures. This procedure satisfies the requirements for requesting unicast resources and modification to already allocated unicast resources to VAL communications.

14.3.3.3.1.2 Procedure

Figure 14.3.3.3.1.2-1 illustrates the procedure for the network resource adaptation.
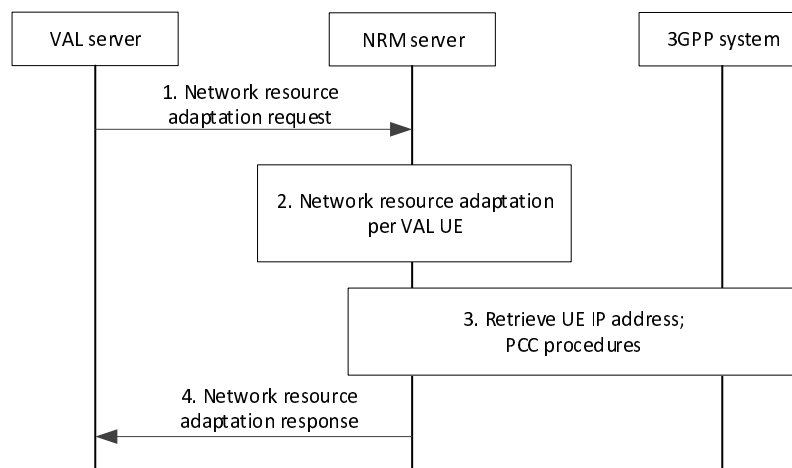
Figure 14.3.3.3.1.2-1: Network resource adaptation

1. The VAL server sends a network resource adaptation request to the NRM server for one or more users belonging to one or more VAL services, and may comprise one or more VAL UEs that will have updated resource requirement. This requirement may be in the form of exact resources /resource pools to be used or indication of bandwidth increase/decrease for the corresponding VAL UEs or set of VAL UEs.

2. The NRM server processes the request and applies / enforces the resource adaptation per VAL UE.

3. The NRM server retrieves UE IP address by using event monitoring capability for PDU session status (or PDN connectivity status) and initiates the PCC procedures for each VAL UE.

4. The NRM server provides a network resource adaptation response to the VAL server, providing information on the fulfilment of the network resource adaptation request. This will include information either per VAL UE or per set of VAL UEs, as indicated by the request of the VAL server in step 1.

14.3.3.3.2 Request for unicast resources at VAL service communication establishment

14.3.3.3.2.1 General

The procedure defined in this subclause specifies how network resources are requested at VAL service communication establishment. If concurrent sessions are used the NRM server may utilize the capability of resource sharing specified for underlying network policy and charging functions. The request for resources includes application type, bandwidth, priority, application identifier and resource sharing information.

14.3.3.3.2.2 Procedure

The procedure is generic to any type of session establishment that requires requests for network resources.

Procedures in figure 14.3.3.3.2.2-1 are the signalling procedures for the requesting resource at session establishment.

Pre-condition:

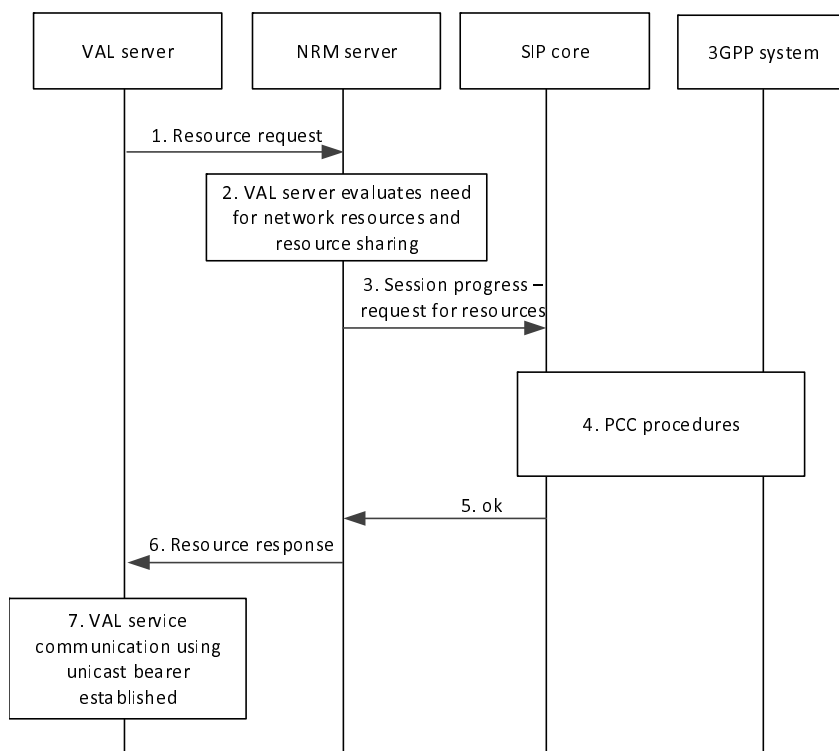- The VAL client has requested VAL service communication with the VAL server.
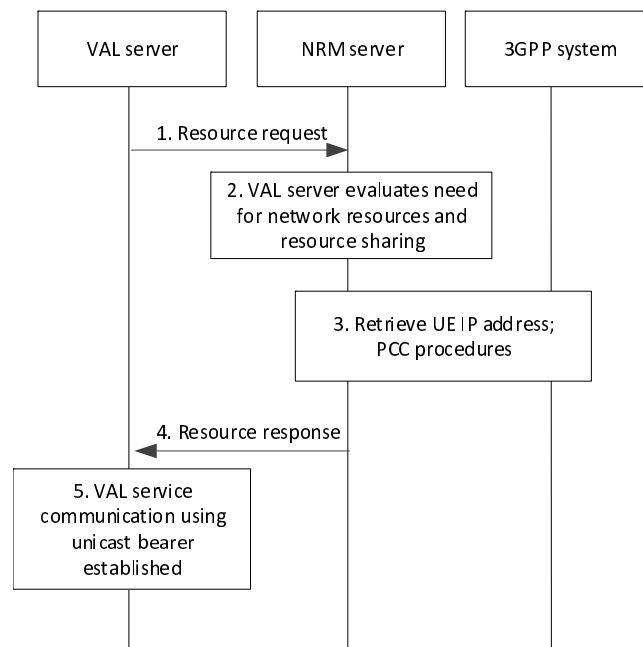
Figure 14.3.3.3.2.2-1: Resource request at VAL service communication establishment

1. The VAL server sends request for resources to the NRM server.

2. The NRM server evaluates the need for network resources and use of resource sharing.

3. The NRM server retrieves UE IP address by using event monitoring capability for PDU session status (or PDN connectivity status), and then PCC procedures are initiated from NRM server.

4. The NRM server sends a resource response to the VAL server.

5. The VAL service communication is established, and resources have been allocated.

14.3.3.3.3 Request for modification of unicast resources

14.3.3.3.3.1 General

To modify unicast resources, the NRM server shall send a resource modification request containing the parameters to be modified for the UE.

Possible scenarios when this procedure may be used are:

- Modify the allocation and retention priority for unicast resources;

- Release and resume resources in-between VAL service communications; or

- Release and resume resources when a UE is able to receive the VAL service communications over multicast transmission

14.3.3.3.3.2 Procedure

Procedures in figure 14.3.3.3.3.2-1 are the signalling procedures for the modification of a unicast:

Pre-condition:
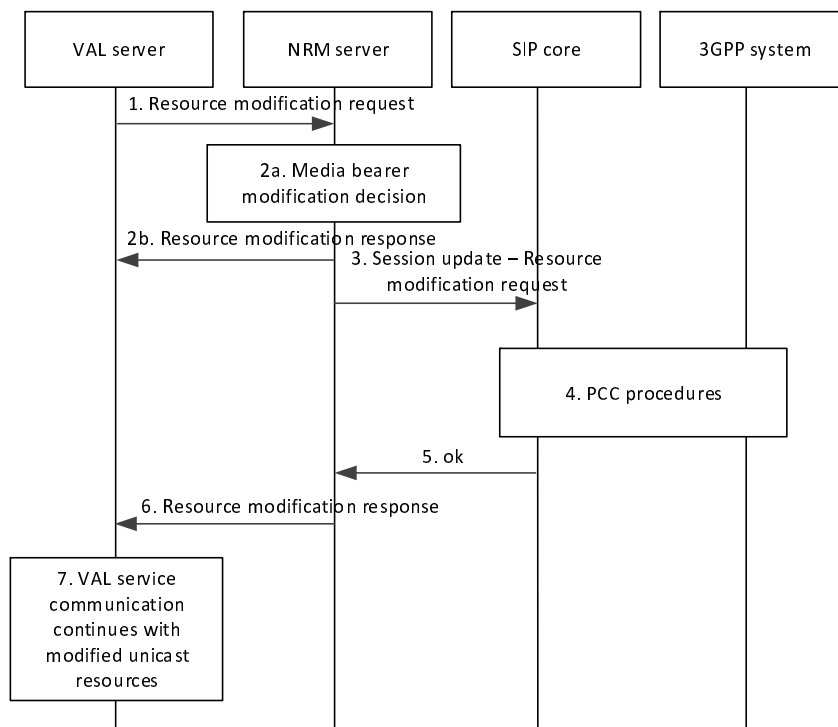
- A VAL service communication is already in progress;
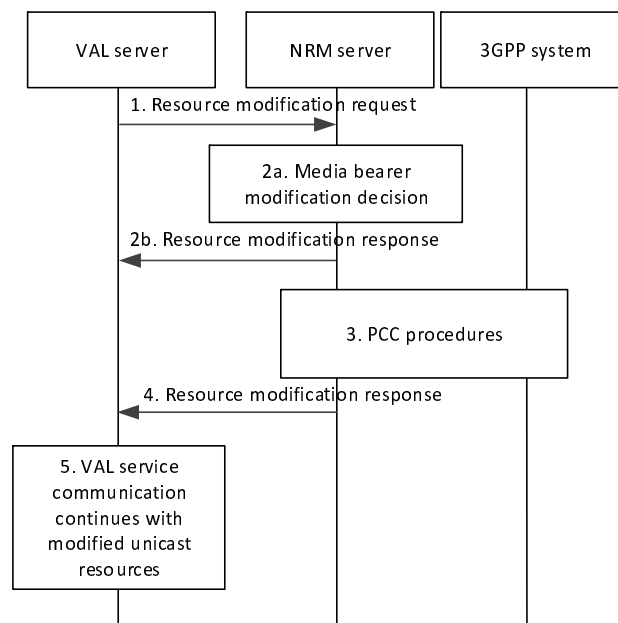
Figure 14.3.3.3.3.2-1: Bearer modification request

1. The VAL server sends a resource modification request to the NRM server.

2a. The NRM server decides to modify the parameters of a unicast bearer.

2b. If the media bearer modification is not required, the NRM server sends a resource modification response to the VAL server.

3. PCC procedures are initiated from NRM server.

4. The NRM server sends a resource modification response to the VAL server.

5. The VAL service communication continues with the modified unicast resources.

NOTE 1: If the VAL service communication is transferred to multicast transmission, the unicast resources could be temporarily be released.

NOTE 2: If multiple VAL service communication streams are sent to the UE, additional bearer resources could be required during an established VAL service communication. Pre-allocation of additional bearer resources already at VAL service communication establishment could be useful.

14.3.3.4   Unicast QoS monitoring

14.3.3.4.1   Unicast QoS monitoring subscription procedure

14.3.3.4.1.1   General

This subclause describes the high level procedure for unicast QoS monitoring subscription. This procedure satisfies the requirements for monitoring of unicast QoS for already allocated unicast resources to VAL communications.

14.3.3.4.1.2   Procedure

Figure 14.3.3.4.1.2-1 illustrates the high level procedure for unicast QoS monitoring subscription.

Pre-conditions:

-    The VAL UE has an established connection in the 5GS
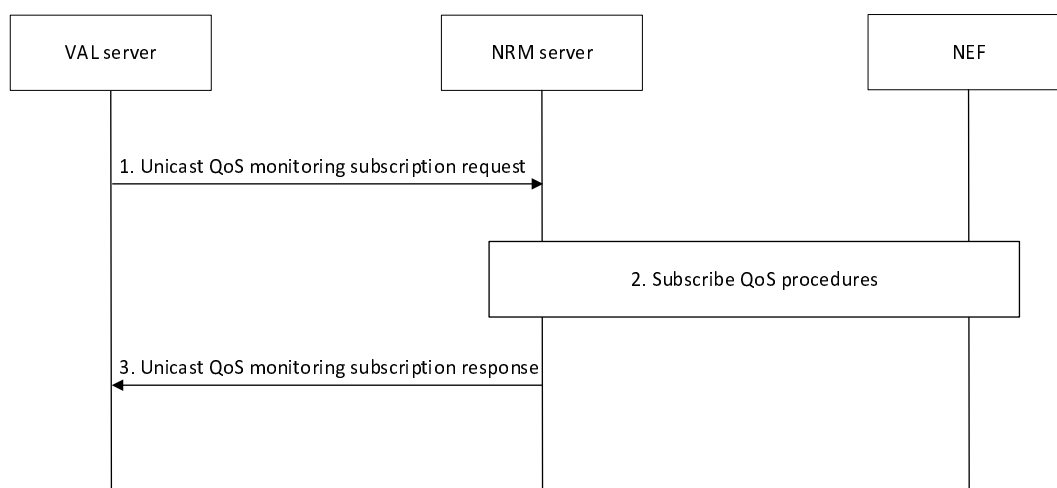
Figure 14.3.3.4.1.2-1: Unicast QoS monitoring subscription

1. The VAL server sends a unicast QoS monitoring subscription request to the NRM server either in conjunction with a request for unicast network resources requiring QoS or when the unicast QoS connection is already established. The NRM server checks if the VAL server is authorized to initiate the unicast QoS monitoring request for the requested target VAL UEs, VAL group ID, or VAL stream IDs.

NOTE: It is left for stage 3 to decide whether to combine the QoS monitoring subscription request with the request for unicast resources.

2. The NRM server interacts with the NEF to establish relevant QoS monitoring subscriptions. The NRM server uses the NEF procedures for the AFsessionWithQoS described in clause 5.2.6.9 of 3GPP TS 23.502 [11] and the NEF procedures for the AnalyticsExposure described in clause 5.2.6.16 of 3GPP TS 23.502 [11] and in particular the UE Communication Analytics described in clause 6.7.3 of 3GPP TS 23.288 [34] and DN Performance Analytics described in clause 6.14 of 3GPP TS 23.288 [34]. Based on the input received from the VAL server in step 1, the NRM server determines the relevant NEF subscription procedures and the parameters for these subscriptions, such as the QoS parameters to be measured (e.g. packet delay, data rate, traffic volume), the frequency of reporting etc. For the frequency of reporting which can be event triggered, periodic, or when the PDU Session is released, the NRM server determines the following:

    a) if the reporting frequency is event triggered:

        i)   the corresponding reporting threshold to each QoS parameter;

        ii) minimum waiting time between subsequent reports;

    b) if the reporting frequency is periodic, the reporting period.

3. The NRM server responds with a unicast QoS monitoring subscription response indicating the subscription status.

14.3.3.4.2 Unicast QoS monitoring notification procedure

14.3.3.4.2.1 General

This subclause describes the high level procedure for unicast QoS monitoring notification.

14.3.3.4.2.2 Procedure

Figure 14.3.3.4.2.2-1 illustrates the high level procedure of unicast QoS monitoring notification event.

Pre-conditions:

- The VAL server has an active unicast QoS monitoring subscription with the NRM server
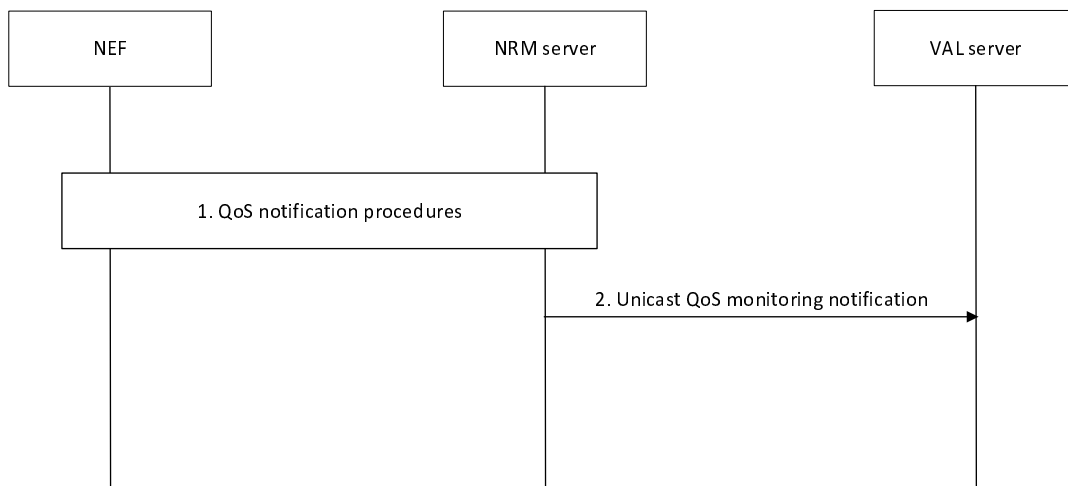
Figure 14.3.3.4.2.2-1: Unicast QoS monitoring notification procedure

1. The NRM server receives QoS monitoring data by means of notifications provided by the NEF. The NRM server coordinates and combines the information from the NEF notifications and determines whether to send a notification to the VAL server based on the VAL server subscription's frequency of reporting. For a VAL group or a list of VAL UEs, the NRM server aggregates QoS monitoring data for each UE belonging to the group or the list; for a VAL stream, the NRM server aggregates the QoS monitoring data for the stream. The NRM server stores the QoS monitoring data as needed for later retrieval.

2. The NRM server sends a unicast QoS monitoring notification including the measured QoS data to the VAL server. If the reporting termination criteria is met (e.g. number of reports reached, threshold reached), NRM server shall also terminate the subscription.

14.3.3.4.3 Unicast QoS monitoring subscription termination procedure

14.3.3.4.3.1 General

This subclause describes the high level procedure for unicast QoS monitoring subscription termination.

14.3.3.4.3.2 Procedure

Figure 14.3.3.4.3.2-1 illustrates the high level procedure of unicast QoS monitoring subscription termination.

Pre-conditions:

- The VAL server has an active unicast QoS monitoring subscription with the NRM server
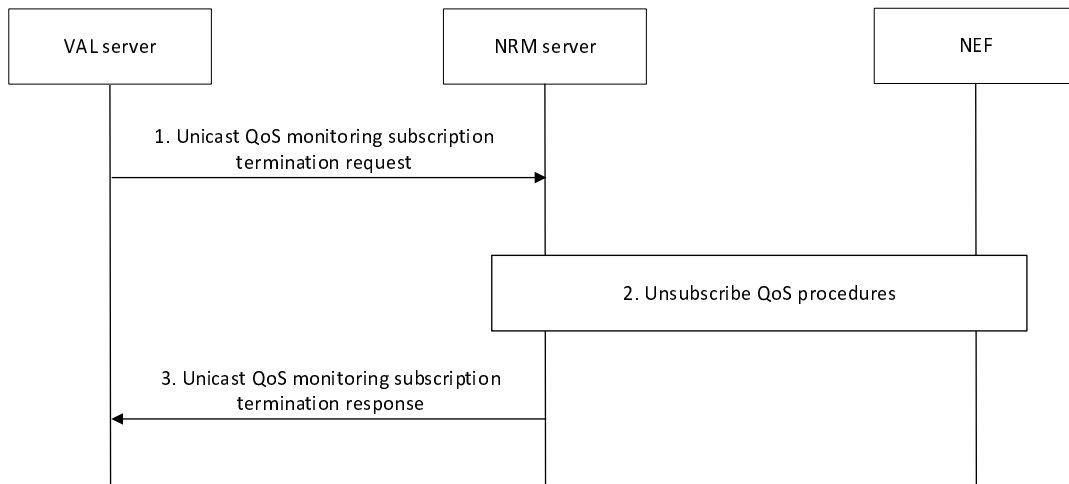
Figure 14.3.3.4.3.2-1: Unicast QoS monitoring subscription termination procedure

1. When the VAL server decides to terminate a unicast QoS monitoring subscription, it sends a QoS monitoring unsubscribe request to the NRM server.

2. The NRM server interacts with the NEF to terminate the related QoS monitoring subscriptions.

3. The NRM server sends a QoS monitoring unsubscribe response to the VAL server.

14.3.3.4.4 Unicast QoS monitoring data retrieval procedure

14.3.3.4.4.1 General

This subclause describes the high level procedure for unicast QoS monitoring data retrieval.

14.3.3.4.4.2 Procedure

Figure 14.3.3.4.4.2-1 illustrates the high level procedure of unicast QoS monitoring data retrieval.
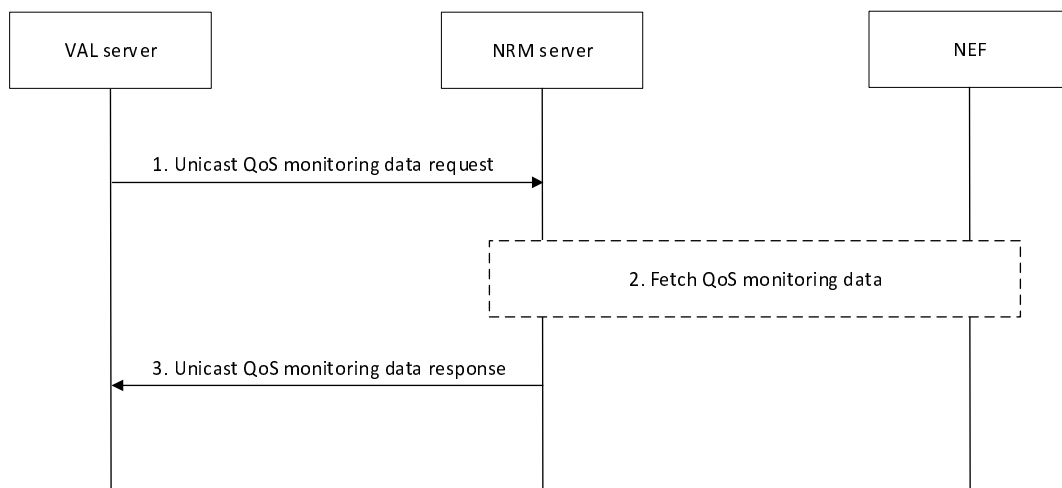
Figure 14.3.3.4.4.2-1: Retrieval of unicast QoS monitoring data

1. The VAL server sends a unicast QoS monitoring data request to the NRM server specifying the details of the requested data and the time period of interest. The NRM server checks if the VAL server is authorized to initiate the unicast QoS monitoring data request for the requested target VAL UEs, VAL group ID, or VAL stream IDs.

2. The NRM server determines if it has the requested data stored internally or whether it needs to interact with the NEF to fetch the data using the AnalyticsExposure described in clause 5.2.6.16 of 3GPP TS 23.502 [11] and in particular the UE Communication Analytics described in clause 6.7.3 of 3GPP TS 23.288 [34] and DN Performance Analytics described in clause 6.14 of 3GPP TS 23.288 [34]. The NRM server collects and processes the collected data to match the measurement data requirement provided in the VAL server request.

3. The NRM server responds with a unicast QoS monitoring data response with the requested data or with a failure indication, and optionally the cause of the failure, in case the requested data is not available.

14.3.4 Multicast resource management for EPS

14.3.4.1 General

The VAL server utilizes the NRM server for multicast resource management.

To activate the multicast bearers in the EPS, the NRM server shall use the Activate MBMS Bearer procedure specified in 3GPP TS 23.468 [16] with the NRM server performing the GCS AS function.

To deactivate the multicast bearers in the EPS, the NRM server shall use the Deactivate MBMS Bearer procedure specified in 3GPP TS 23.468 [16] with the NRM server performing the GCS AS function.

To modify multicast bearers in the EPS, the NRM server shall use the Modify MBMS Bearer procedure specified in 3GPP TS 23.468 [16] with the NRM server performing the GCS AS function.

Editor's note: To support other modes of MBMS is FFS.

14.3.4.2 Use of pre-established MBMS bearers

14.3.4.2.1 General

In this scenario, upon triggered by VAL server, the NRM server pre-establishes MBMS bearer(s) in certain pre-configured areas before the initiation of the VAL service group communication session. When a user originates a request for a VAL service group communication session for one of these areas, the pre-established MBMS bearer(s) is used for the DL VAL service communication.

The following steps need to be performed prior to the start of the VAL service group communication session over pre-established MBMS bearer:

-   Pre-establish MBMS bearer(s)

-   Announce the pre-established MBMS bearer to the NRM clients

When these preparation steps have been done the VAL service group communication session using MBMS bearer can start.

The vertical application level communications are sent on the MBMS bearer. Optionally a separate MBMS bearer could be used for the application level control messages, due to different bearer characteristic requirements.

14.3.4.2.2 Procedure

The procedure figure 14.3.4.2.2-1 shows only one of the receiving VAL clients using an MBMS bearer. There might also be VAL clients in the same VAL service group communication session that receive the communication on unicast bearers.
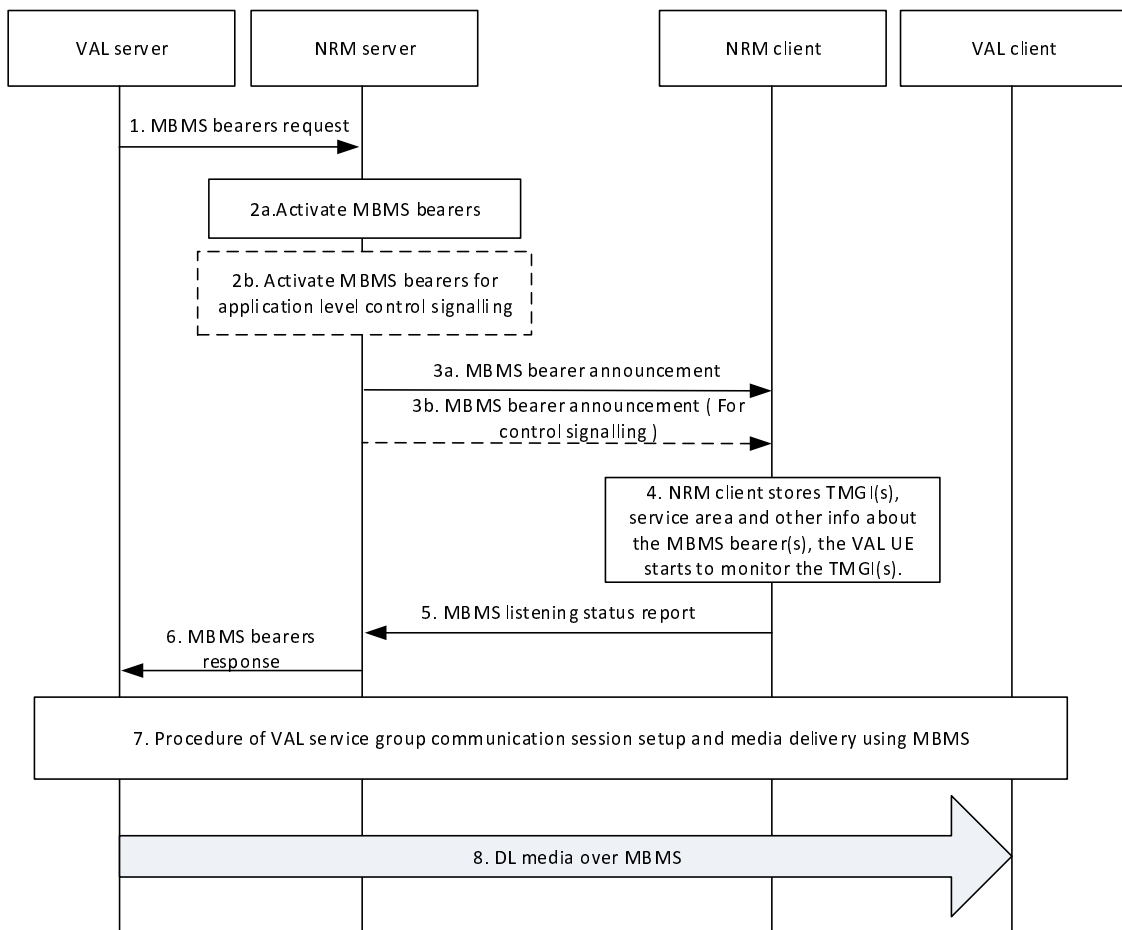
Figure 14.3.4.2.2-1: Use of pre-established MBMS bearers

1. The VAL server sends a MBMS bearers request to the NRM server including service description(s) for which the MBMS bearers are requested.

2a. The NRM server determines to activate MBMS bearer. The activation of the MBMS bearer in EPS is done on the MB2-C reference point and according to 3GPP TS 23.468 [16]. This bearer will be used for the VAL service communication. If local MBMS is requested in step 1, the NRM server uses the local MBMS information provided by VAL server in step 1 or the local MBMS information configured locally in the NRM server to activate the MBMS bearers. The NRM server performs local MBMS procedures in line with the procedure of L.MBMS based MBMS data delivery defined in 3GPP TS 23.285 [31].

2b. Optionally, the NRM server may also activate an MBMS bearer dedicated for application level control signalling. The activation of the MBMS bearer is done on MB2-C reference point and according to 3GPP TS 23.468 [16]. If local MBMS is requested in step 1, the NRM server uses the local MBMS information provided by VAL server in step 1 or the local MBMS information configured locally in the NRM server to activate the MBMS bearers. The NRM server performs local MBMS procedures in line with the procedure of L.MBMS based MBMS data delivery defined in 3GPP TS 23.285 [31].

NOTE 1:   The procedure to determine the activation of MBMS bearers is implementation specific.

3a. The NRM server passes the MBMS bearer info for the service description associated with the pre-established MBMS bearer to the NRM client. The NRM client obtains the TMGI, identifying the MBMS bearer, from the service description.

3b. The NRM server may pass the MBMS bearer info for the service description associated with the application control MBMS bearer to the NRM client. The NRM client obtains the TMGI, identifying the MBMS bearer, from the service description.

NOTE 2:   Step 3a and step 3b can be done in one MBMS bearer announcement message.

4. The NRM client stores the information associated with the TMGI(s). The NRM service client uses the TMGI and other MBMS bearer related information to activate the monitoring of the MBMS bearer by the VAL UE. The NRM client shares the MBMS bearer related information with the VAL client.

5. The NRM client that enters or is in the service area of at least one announced TMGI indicates to the NRM server that the VAL UE is able to receive VAL service communication over MBMS, whereby the NRM server may decide to use the MBMS bearer instead of unicast bearer for VAL service communication sessions based on available information at the NRM server including the MBMS listening status report as described in clause 14.3.4.5.

NOTE 3: Step 5 is optional for the VAL UE on subsequent MBMS bearer announcements.

6. The NRM server provides a MBMS bearers response to the VAL server.

7. A VAL service group communication session is established.

8. As the VAL server transmits the VAL service communication over the MBMS bearer, the VAL service communication packets are detected and delivered to the VAL client.

14.3.4.3 Use of dynamic MBMS bearer establishment

14.3.4.3.1 General

In this scenario, the VAL server uses a unicast bearer for communication with the UE on the DL at the start of the group communication session. When the VAL server triggers to use an MBMS bearer in EPS for the DL VAL service communication, the NRM server decides to establish an MBMS bearer in EPS using the procedures defined in 3GPP TS 23.468 [16]. The NRM server provides MBMS service description information associated with MBMS bearer(s), obtained from the BM-SC, to the UE. The UE starts using the MBMS bearer(s) to receive DL VAL service and stops using the unicast bearer for the DL VAL service communication.

14.3.4.3.2 Procedure

Figure 14.3.4.3.2-1 illustrates the use of dynamic MBMS bearer establishment.
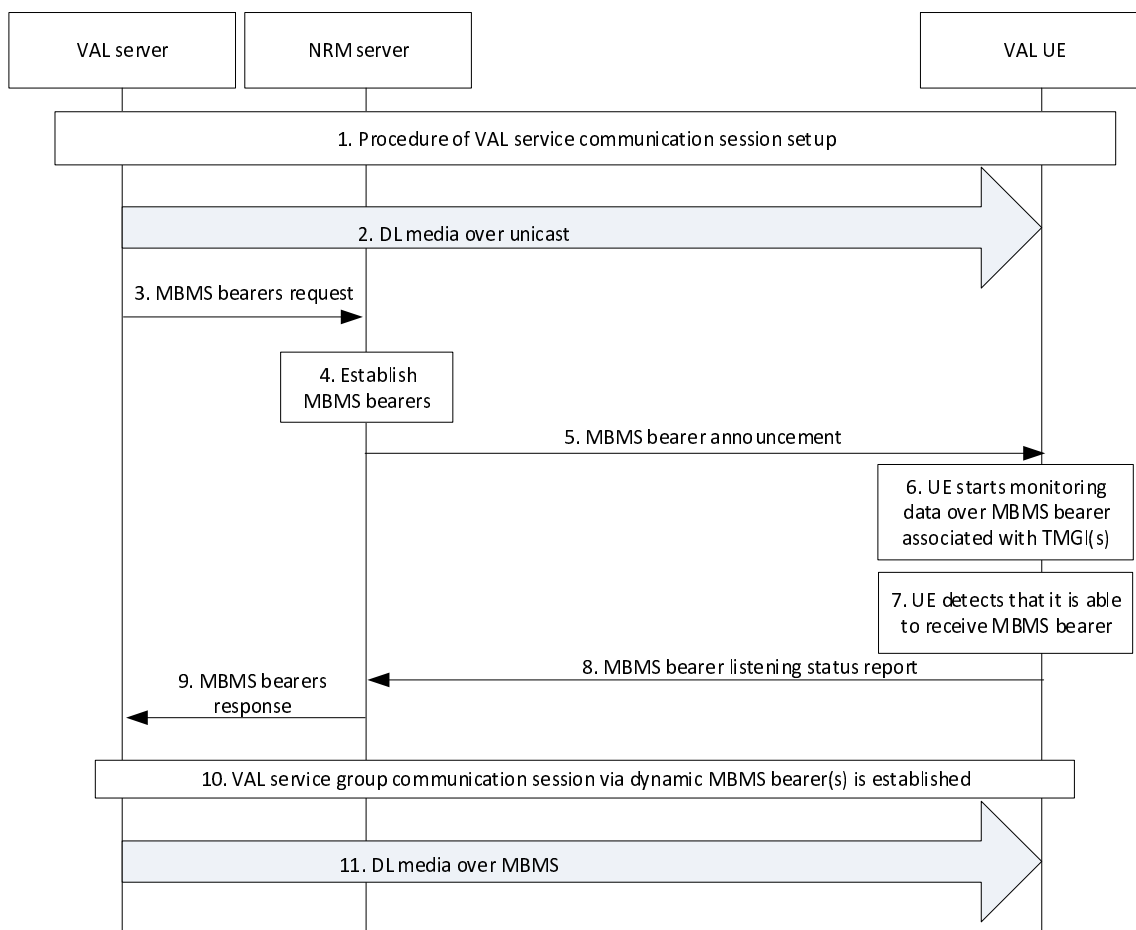
Figure 14.3.4.3.2-1: Use of dynamic MBMS bearer establishment

1. A VAL service group communication session is established.

2. The downlink data is sent by unicast delivery.

3. The VAL server sends MBMS bearers request to the NRM server.

4. The NRM server establishes the MBMS bearer(s) for the VAL service group communication session according to the procedures defined in 3GPP TS 23.468 [16]. Service description associated with the MBMS bearer(s) is returned from the BM-SC. If local MBMS is requested in step 3, the NRM server uses the local MBMS information provided by VAL server in step 3 or the local MBMS information configured locally in the NRM server to activate the MBMS bearers. The NRM server performs local MBMS procedures in line with the procedure of L.MBMS based MBMS data delivery defined in 3GPP TS 23.285 [31].

5. The NRM server provides service description information associated with the MBMS bearer to the UE. The VAL UE obtains the TMGI from the announcement message. This message may be sent on an application level control signalling bearer.

6. The VAL UE starts monitoring data over MBMS associated with the TMGI, while in the service area associated with the TMGI.

7. The VAL UE detects that it is able to receive data over MBMS associated with the TMGI.

8. The NRM client notifies the NRM server the MBMS listening status associated to the monitored TMGI, (e.g. that it is successfully receiving the TMGI). The NRM client may also notify the MBMS reception quality level of the TMGI. The NRM server may decide to use the MBMS bearer instead of unicast bearer for VAL service communication sessions based on available information at the NRM server including the MBMS listening status report as described in clause 14.3.4.5.

9.   The NRM server provides an MBMS bearer response to the VAL server with the dynamic MBMS bearer(s) information. The VAL server stops sending VAL service communication data over unicast way to the VAL client.

NOTE: The MBMS reception quality level may be used by the NRM server to make an efficient decision to switch again to a unicast transmission or to take measures to prepare such a switch (e.g. when the quality level indicates that the reception quality of the MBMS bearer is decreasing or reaching an insufficient quality level for the reception of VAL services).

10. A VAL service group communication session via dynamic MBMS bearer(s) is established.

11. The VAL server sends the downlink VAL service communication for the VAL service group communication session over the MBMS.

14.3.4.4   MBMS bearer announcement over MBMS bearer

14.3.4.4.1   General

The MBMS announcement may be done on either a unicast bearer or a MBMS bearer. Using a unicast bearer for MBMS bearer announcement provides an interactive way of doing announcement. The NRM server will send the MBMS bearer announcement message to the NRM client regardless if there is an MBMS bearer active or the VAL client can receive the data on the MBMS bearer with sufficient quality. The benefit of the existing procedure is that it gives a secure way to inform the NRM client about the MBMS bearer and how to retrieve the data on the MBMS bearer.

When there is more than one MBMS bearer active in the same service area for VAL service, there are not the same reasons to use unicast bearer for additional MBMS bearer announcement. Instead a MBMS bearer for application level control signalling can be used to announce additional MBMS bearers.

The MBMS bearer announcement messages are sent on an MBMS bearer used for application control messages. This bearer will have a different QoS setting compared to an MBMS bearer used for VAL service communication, since application signalling messages are more sensitive to packet loss.

14.3.4.4.2   Procedure

Figure 14.3.4.4.2-1 illustrates a procedure that enables the NRM server to announce a new MBMS bearer.

Pre-conditions:

1.   An MBMS bearer used for VAL service application control messages must have been pre-established and announced to the NRM client.

2.   Additional MBMS bearer information may have already been announced to the NRM client.
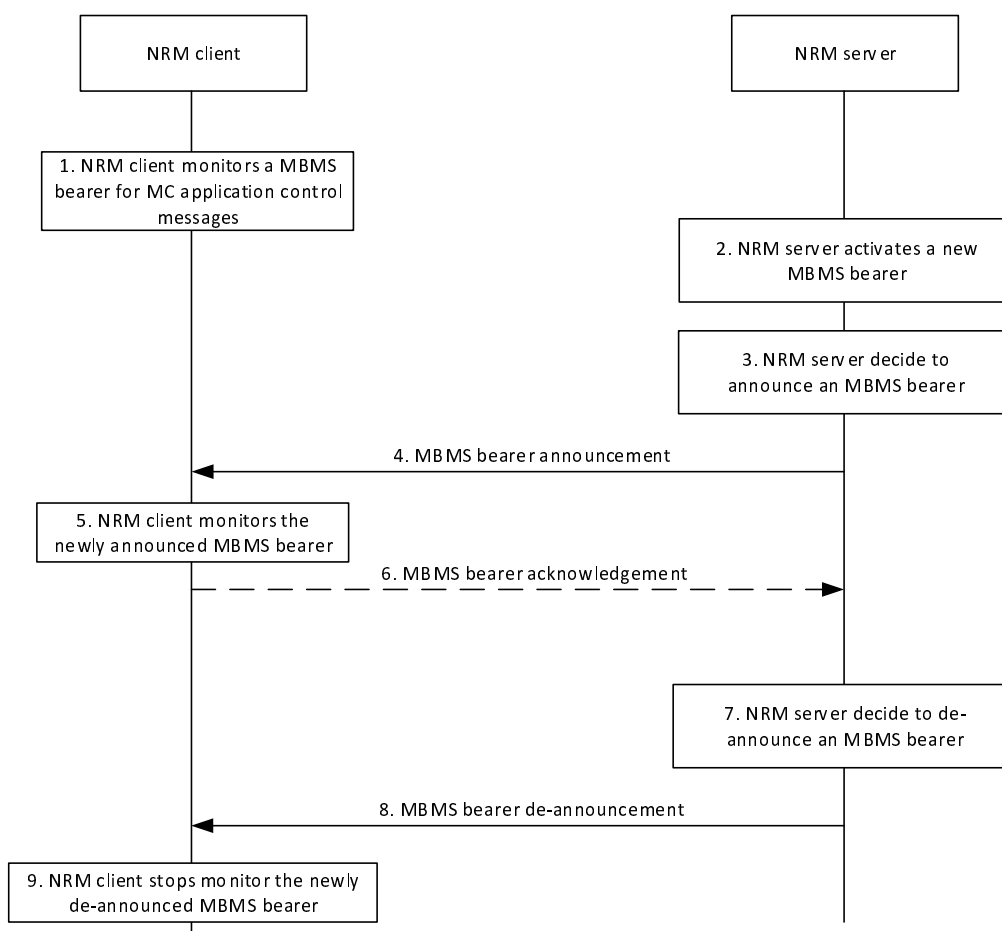
Figure 14.3.4.4.2-1: MBMS bearer announcement over an MBMS bearer used for application control messages

1. The NRM client monitors an MBMS bearer that is used for VAL service application signalling messages, such as bearer announcement messages.

2. The NRM server activates a new MBMS bearer.

3. The NRM server announces the MBMS bearer to the NRM client. The bearer may have just been activated or may have already been running for some time. The step may be repeated as needed.

4. The NRM server sends a MBMS bearer announcement on the MBMS bearer used for VAL application control messages. The MBMS bearer announcement contains the identity of the MBMS bearer (i.e. the TMGI) and may optionally include additional information about the newly announced bearer. Required and optional MBMS bearer announcement details may have already been provided. In this case the MBMS bearer identity could be used as a key for such MBMS bearer details.

5. The NRM client start to monitor the newly announced MBMS bearer.

6. If requested by the NRM server, the NRM client sends an acknowledgement of the MBMS bearer to the NRM server.

7. The NRM server de-announce the MBMS bearer.

8. The NRM server sends a MBMS bearer de-announcement message that contains the identity of the MBMS bearer.

9. The NRM client stops monitoring the de-announced MBMS bearer.

The same procedure can also be used to modify existing MBMS bearer announcement information. Example of such modification could be addition of UDP ports or modification of codec in the SDP.

14.3.4.5 MBMS bearer quality detection

14.3.4.5.1 General

The NRM client and NRM server use this procedure to report and take action on the MBMS bearer quality towards VAL service communications. A NRM client monitors an MBMS bearer to enable receiving VAL service communication. Based on the received quality (e.g. radio level quality, transport level quality), the NRM client needs to inform the NRM server that the VAL UE is able to receive the VAL service communication on the MBMS bearer with sufficient quality or not able to receive the VAL service communication on the MBMS bearer with sufficient quality. Furthermore, based on the received quality, the NRM client may notify the NRM server at which MBMS reception quality level it has received the VAL service communication on the MBMS bearer.

The issue can be more complex since the NRM client needs to estimate the quality of the bearer even in the scenario when there are no data currently transmitted on the MBMS bearer. The reason for this is that an NRM client that has entered an area with significantly degraded MBMS quality, might not even notice that a VAL service communication is ongoing, meanwhile the NRM server still assumes that the VAL UE can receive the VAL service communication being broadcasted.

To estimate the MBMS bearer quality, for example as an equivalent BLER (Block Error Rate), when no data is sent is implementation specific. This estimation can be dependent on for example the modulation and coding scheme (MCS) and measurements from the reference signals from the eNB(s). Other metrics (e.g. RTP packet loss) may be used to estimate the MBMS bearer quality.

Based on the MBMS bearer quality reported from the NRM clients, the NRM server may decide to use the MBMS bearer for a group communication if a certain number of NRM clients located in the MBMS service area are able to receive the VAL service communication. And if a NRM client is not able to receive the VAL service communication on the MBMS bearer, the NRM server may decide to switch the user plane deliver mode for the NRM client from MBMS bearer to unicast bearer.

14.3.4.5.2 Procedure

The NRM client shall indicate the ability of the NRM client to receive the MBMS bearer.

Pre-conditions:

1. There is an MBMS bearer activated and the MBMS bearer information is announced to the NRM client

2. The NRM client is located in the MBMS broadcasting area

3. The VAL UE monitors SIB-13 (or SIB-20) and (SC-)MCCH to receive the modulation and coding scheme

4. The VAL UE monitors the cell specific reference signal and when MBSFN transmission is used, the MBSFN specific reference signals
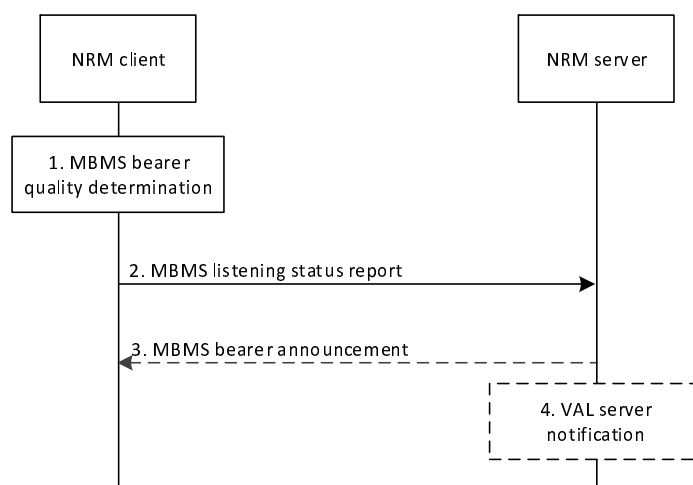
Figure 14.3.4.5.2-1: MBMS bearer quality detection

1. The NRM client determines that the MBMS bearer quality shall be reported to the NRM server. The NRM client may determine the MBMS bearer quality by using the BLER of the received data. When no data is received, the quality estimation can consider the reference signals and the modulation and coding scheme (MCS). The UE may also use predictive methods to estimate the expected MBMS bearer quality (e.g. speed and direction) to proactively inform the NRM server of an expected loss of the MBMS bearer quality. The NRM client may also map the determined MBMS bearer quality to a MBMS reception quality level. The MBMS reception quality level indicates at which specific MBMS bearer quality level the VAL service communication has been received.

Editor's note: The set of MBMS reception quality levels and the mapping of the determined MBMS bearer quality to those levels are FFS.

NOTE 1: When MBSFN transmission is used, the MBSFN reference signal needs to be used and when SC-PTM is used the cell specific reference signal needs to be used. With the measured reference signal, the reference signal received quality (RSRQ) can be calculated.

2. If the MBMS bearer quality reaches a certain threshold, the NRM client sends an MBMS listening status report. The threshold is used to define the MBMS listening status, which indicates if the MBMS bearer quality has been acceptable or not to receive a specific VAL service communication. If the MBMS bearer quality is mapped to a different MBMS reception quality level, the NRM client may send an MBMS listening status report including the MBMS reception quality level. Based on the MBMS listening status, if MBMS reception quality level is received, then the NRM server may efficiently decide to switch to another bearer (e.g., MBMS bearer or unicast bearer) or to take measures to prepare such a switch and further notify the VAL server.

NOTE 2: Prior sending the MBMS listening status report, it could be beneficial to also include information for different alternatives e.g. another MBMS bearer might have better quality and could be a better option than a transfer of the communication to unicast.

NOTE 3: The threshold used to indicate MBMS bearer quality depends on VAL service type (i.e. V2X, MCPTT, MCVideo or MCData) and the metrics used. The metrics used and the associated thresholds are out of scope of this specification.

3. The NRM server may send additional proposal for measurements e.g. information about neighbouring MBMS bearers. This message may be an MBMS bearer announcement message.

4. The NRM server may send user plane delivery mode to VAL server based on the MBMS listening status to preserve the service continuity as described in clause 14.3.4.6 and clause 14.3.4.9.

14.3.4.6 Service continuity in MBMS scenarios

14.3.4.6.1 General

This subclause specifies service continuity scenarios when MBMS bearers are used. There are different solutions for different scenarios.

14.3.4.6.2 Service continuity when moving from one MBSFN to another

The service continuity solution described in this subclause is suitable in the scenario when multiple MBMS bearers are used with the purpose to cover a larger area. In VAL communications several VAL service communication streams may be multiplexed in one MBMS bearer. Furthermore, one VAL service communication stream may be sent on more than one MBMS bearer if the receiving users are distributed over more than one MBMS service area. A VAL UE that is interested in receiving a VAL service communication stream that is broadcasted in both MBMS bearers is a candidate for this service continuity procedure.

Figure 14.3.4.6.2-1 illustrates a deployment scenario that provides service continuity between two MBSFN areas. Two different MBMS bearers are activated (TMGI 1 and TMGI 2), the activation of the bearers is done in the two MBSFN areas (MBSFN 1 and MBSFN 2). The MBSFN areas 1 and 2 are partially overlapping, meaning that some transmitting cells belong to both MBSFN area 1 and MBSFN area 2.
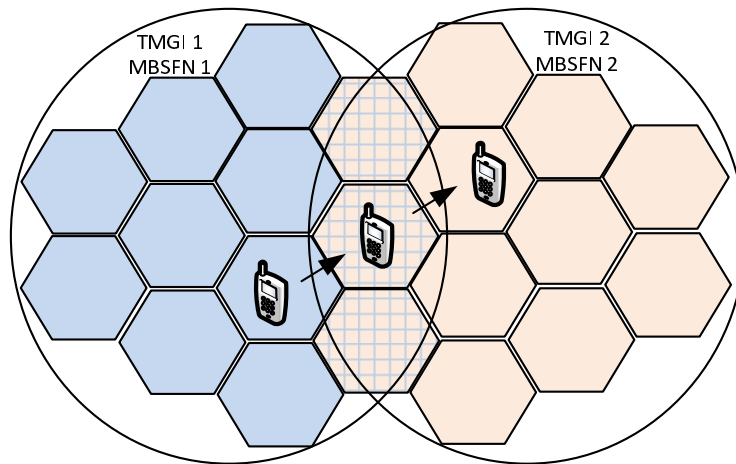
Figure 14.3.4.6.2-1: Two MBMS bearer using overlapping MBSFN areas

Figure 14.3.4.6.2-2 illustrates the procedure:
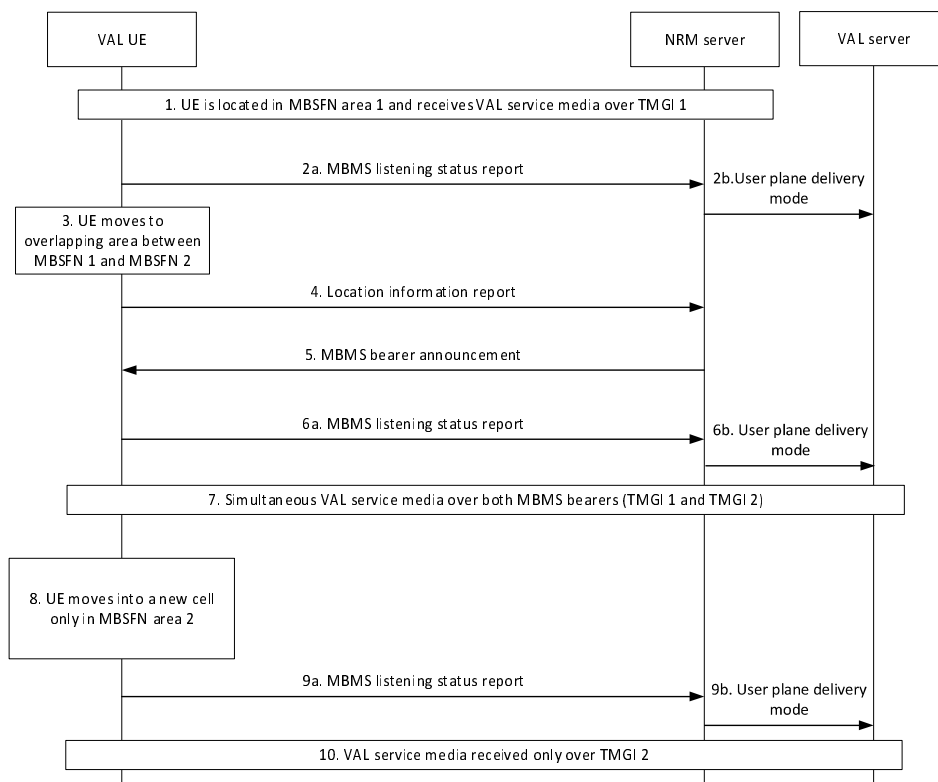
Figure 14.3.4.6.2-2: Service continuity when moving from one MBSFN to another

1. The VAL UE is located in MBSFN 1 and can listen to TMGI 1. No additional MBMS bearers that the NRM client is interested in are active in the current cell.

2a. The NRM client notifies the NRM server that the VAL UE is successfully receiving the VAL service communication over TMGI 1. The NRM client may also notify the MBMS reception quality level of TMGI 1.

2b. The NRM server notifies a user plane delivery mode to the VAL server.

NOTE: The MBMS reception quality level may be used by the NRM server to make an efficient decision to switch to another MBMS bearer or to a unicast bearer, or to take measures to prepare such a switch (e.g. when the quality level indicates that the reception quality of the MBMS bearer is decreasing or reaching an insufficient quality level for the reception of VAL services).

3. The VAL UE moves into a new cell in which both TMGI 1 and TMGI 2 are active. This cell is part of both MBSFN area 1 and MBSFN area 2, and broadcast the same service on both TMGIs.

4. The NRM client sends a location information report to the NRM server. For that, the UE uses the SAI information found in the system information block (SIB) transmitted by the radio cells.

5. The NRM server sends to the NRM client a MBMS bearer announcement with information related to TMGI 2 (if the NRM server had not done it before). Hence, the NRM client knows that TMGI 2 transmits the same VAL service communication.

6a. The NRM client notifies the NRM server that it is successfully receiving TMGI 1 and TMGI 2. The NRM client may also notify the MBMS reception quality level per TMGI.

6b. The NRM server notifies a user plane delivery mode to the VAL server.

7. The VAL UE may receive the VAL service communication over both MBMS bearers, i.e. TMGI 1 and TMGI 2. The VAL UE may also verify that it is the same content sent on both bearers. The duplicated packets may also be used to perform error corrections.

8. The VAL UE moves into a new cell in MBSFN area 2, where only TMGI 2 is active.

9a. The NRM client notifies the NRM server that the VAL UE is successfully receiving the VAL service communication over TMGI 2. The NRM client may also notify the MBMS reception quality level of TMGI 2.

9b. The NRM server notifies a user plane delivery mode to the VAL server.

10. The VAL UE receives the VAL service communication only over TMGI 2.

This service continuity procedure mitigates the risk of packet loss that may occur if the VAL UE would request to transfer the VAL service communication stream to a unicast bearer when moving into the new area and then back to a multicast bearer when the UE can listen to TMGI 2. However, it is still required that the NRM client sends a location report (and MBMS listening report), as described in steps 4-6 above. To send the location report and the MBMS listening report by the NRM client to the NRM server a unicast bearer is needed. The location report from the NRM client is required, since the NRM server must know that the VAL UE has entered a new area and can only listen to MBMS bearer active in that area. If this is not done the VAL server might send a VAL service communication stream that the VAL UE is required to listen to on the MBMS bearer 1, since the NRM server still assumes that the VAL:UE is located in the MBSFN area 1.

The solution can be improved as illustrated in figure 14.3.4.6.2-3. In this case two different MBMS bearers are activated (TMGI 1 and TMGI 2), these MBMS bearers are used only for VAL service communication. An application level signalling bearer is activated (TMGI 9), in both MBSFN areas. This bearer is used for application level signalling messages that are sent on the MBMS bearer TMGI 9. By using an application level signalling bearer (e.g. TMGI 9) the VAL UEs can receive application control messages for all VAL service communication going on in the areas of both TMGI 1 and TMGI 2. A VAL UE that is located in the area of TMGI 2 and is interested in a VAL service group transmission (e.g. V2X) only going on in TMGI 1, can with the information received in TMGI 9 initiate a unicast bearer and request to receive that specific VAL service communication over a unicast instead. Without the information received over TMGI 9 the NRM client must immediately report that the VAL UE has left the broadcast area that the NRM server assumes that the VAL UE is located in. With the use of TMGI 9 there is no immediate need for the NRM client to inform the NRM server of a location change.
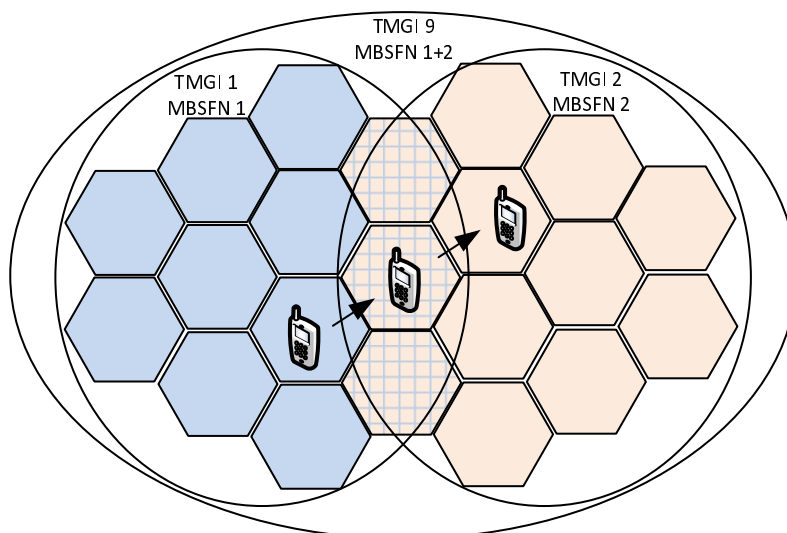
Figure 14.3.4.6.2-3: Two MBMS bearer using overlapping MBSFN areas with a separate application signalling bearer

The procedural steps in this scenario will be the same as described above in this subclause. However, in this scenario the NRM client is not required to initiate a unicast bearer to send location report (or MBMS listening report). The VAL UE may move between the two MBMS bearers (TMGI 1 and TMGI 2) without the need to report an area change. A condition for this to work is that there is an application level signalling bearer (TMGI 9) activated in the full area (i.e. the area of both TMGI 1 and TMGI 2). The TMGI 9 will broadcast all application control messages for all VAL service communications ongoing in both areas. If the VAL UE is in coverage of one of the two MBMS bearers that does not transmit the VAL service communication of interest the VAL UE can report to the NRM server that it is not able to listen to the VAL service communication over the MBMS bearer, which triggers the NRM server to switch to a unicast bearer instead.

14.3.4.7 MBMS suspension notification

14.3.4.7.1 General

In this procedure the NRM client is requested by the NRM server to send a MBMS suspension report. This request for MBMS suspension report can be included in the MBMS bearer announcement and the NRM server may choose to only send this request for MBMS suspension report to a subset of all NRM clients.

14.3.4.7.2 Procedure

Figure 14.3.4.7.2.-1 illustrates a procedure in which the NRM client notifies the NRM server about an MBMS suspension decision in RAN.

The NRM server can decide on a subset of all VAL UEs in the MBMS broadcast area that shall report on MBMS bearer suspension. When the NRM server makes the decision of the VAL UE subset, consideration shall be taken to the location of the VAL UEs, since VAL UEs' location is dynamically changed. This means that the MBMS suspension reporting instruction may need to be updated regularly based on the VAL UEs mobility.

Pre-condition:

- It is assumed that there is at least one active MBMS bearer
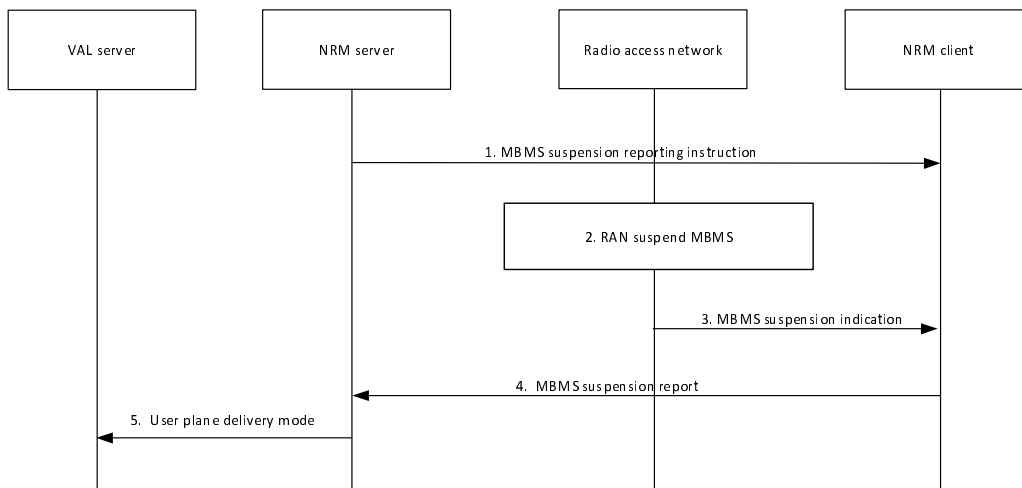
Figure 14.3.4.7.2-1: MBMS suspension notification

1. The NRM server sends an MBMS suspension reporting instruction to the NRM client.

NOTE: This message may be included in the MBMS bearer announcement message and may be sent both on a unicast bearer and a multicast bearer.

2. RAN decides to suspend the MBMS bearer, according to existing procedures in 3GPP TS 36.300 [23].

3. An MBMS suspension indication is sent in the MSI (MCH Scheduling Information), according to existing procedures in 3GPP TS 36.300 [23].

4. The NRM client detect the MBMS suspension and sends an MBMS suspension report.

5. Based on the MBMS suspsension report received, the NRM server determines whether to switch to a new bearer (unicast or MBMS). If NRM server determines to switch to unicast bearer, then the NRM server sends the user plane delivery mode message to VAL server , and the VAL server sends the downlink data over the new bearer.

The NRM client that is not instructed to send an MBMS suspension report shall still detect the MBMS suspension indication from RAN (step 3). A NRM client shall in this case not send other types of report (e.g. MBMS listening reports).

The same procedure can be applied at MBMS resumption or other MBMS events that may be detected by the NRM client.

14.3.4.8 MBMS bearer event notification

14.3.4.8.1 General

The NRM server is an instantiation of a GCS AS. For the NRM server to know the status of the MBMS bearer, and thus know the network's ability to deliver the VAL service, it is required that the network provides MBMS bearer event notifications to the NRM server. The different events notified to the NRM server include the MBMS bearer start result (e.g. when the first cell successfully allocated MBMS resources), including information if any cells fail to allocate MBMS resources to a specific MBMS bearer, the current status of the MBMS bearer, MBMS bearer suspension/resume or overload scenarios.

Editor's note: The procedure defined in this sub clause requires an enhancement to GCSE and RAN and is therefore subject to implementation in EPC and RAN.

14.3.4.8.2 Procedure

The procedure in figure 14.3.4.8.2-1 shows notification information flows from NRM server to BM-SC.
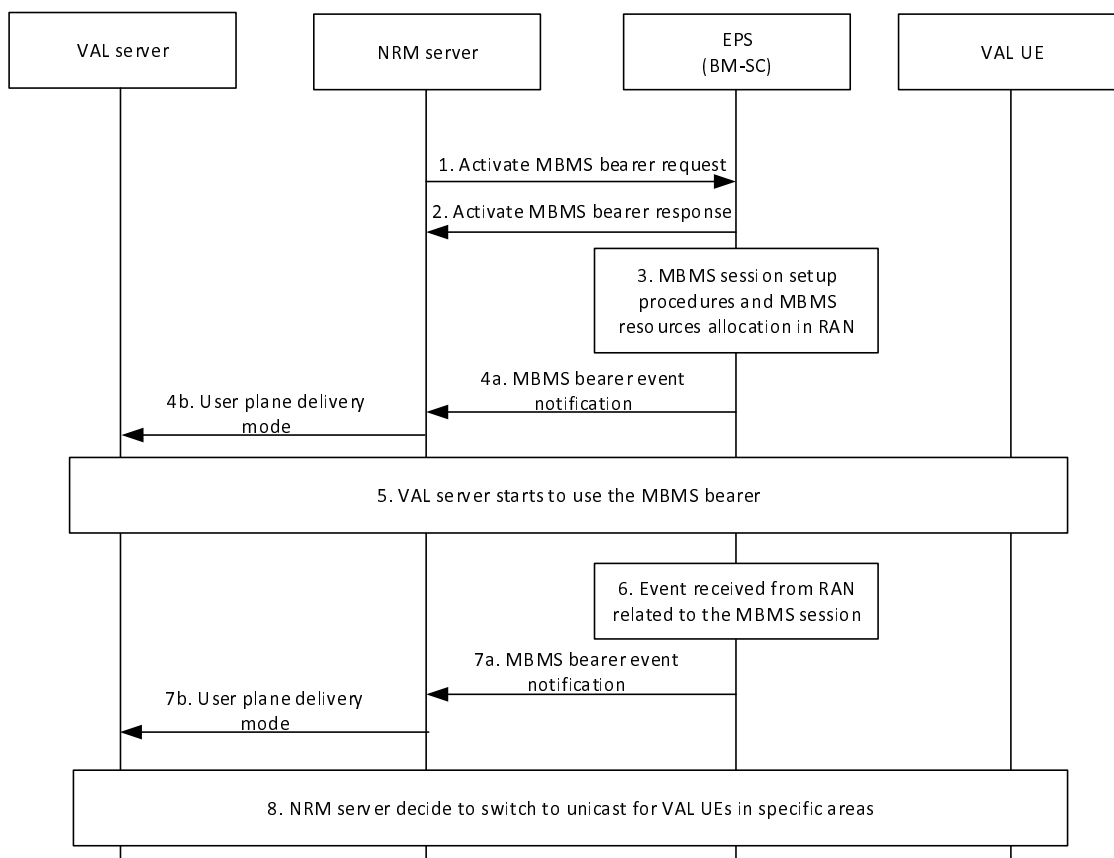
Figure 14.3.4.8.2-1: MBMS bearer event notification

1. The NRM server activates an MBMS bearer. The activation of the MBMS bearer is done on the MB2-C reference point and according to 3GPP TS 23.468 [16].

2. The BMSC will respond to the activation with an Activate MBMS bearer response message, according to 3GPP TS 23.468 [16].

3. The EPC and RAN will initiate the MBMS session start procedure according to 3GPP TS 23.246 [17]. This procedure is outside the scope of this specification.

4a. At the first indication of a successful MBMS session start procedure, the BM-SC sends a MBMS bearer event notification, indicating that the MBMS bearer is ready to use.

4b. The NRM server notifies user plane delivery mode to the VAL server.

5. The VAL server starts to use the MBMS bearer according to the MBMS procedures in this specification.

6. An event from RAN related to the MBMS session is received by the BM-SC.

7a. The BM-SC notifies the NRM server of certain MBMS related events including references to affected MBMS services areas or list of cells. Example of such events may be radio resources not available, overload, MBMS suspension.

7b. The NRM server notifies user plane delivery mode to the VAL server.

8. The NRM server may decide, based on the received events, to switch to unicast transmission for relevant VAL UEs.

NOTE: Steps 6-8 should be seen as example events from the network that may occur and possible actions taken by the NRM server. These steps may be done at any time and repeatedly during the life time of an MBMS bearer.

14.3.4.9 Switching between MBMS bearer and unicast bearer

14.3.4.9.1 General

The NRM server monitors the bearers used for VAL service communications and decides to switch between MBMS and unicast bearers.

14.3.4.9.2 Procedure

Figure 14.3.4.9.2-1 shows the procedure for service continuity when a UE is about to move out of MBMS coverage or getting into good MBMS coverage by switching between MBMS bearer and unicast bearer.

Pre-condition:

- It is assumed that a bearer (unicast or MBMS) has been activated by the VAL server for downlink delivery.
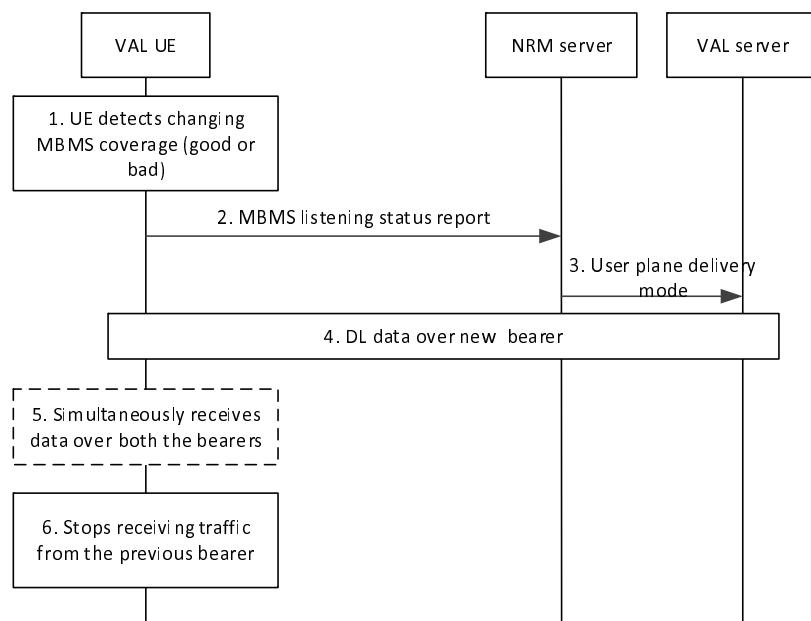
Figure 14.3.4.9.2-1: Switching between MBMS delivery and unicast delivery

1. The VAL UE detects changing MBMS bearer condition (good or bad MBMS coverage) for the corresponding MBMS service. The method to detect is implementation specific.

2. The NRM client notifies the NRM server about the MBMS bearer condition for the corresponding MBMS service by sending the MBMS listening status report.

NOTE 1: To efficiently notify the NRM server, e.g., when the NRM client detects that the reception quality of the MBMS bearer is decreasing or reaching an insufficient quality level for the reception of VAL services, the NRM client proactively may send to the NRM server a MBMS listening status report including the MBMS reception quality level.

3. The NRM server makes the decision to switch between MBMS delivery and unicast delivery based on available information at the NRM server including the MBMS listening status report as described in clause 14.3.4.5. The NRM server notifies a user plane delivery mode to the VAL server.

4. The VAL server sends the downlink data over the new bearer (unicast or MBMS) to the VAL client as per step 3.

NOTE 2: The new bearer (unicast or MBMS) may be set up on demand after step 3 or before.

5. During the switching, the VAL client simultaneously receives downlink data through both bearers (unicast bearer and MBMS bearer). If there is no downlink data to the VAL client, this step can be skipped.

6. The VAL client ceases to receive the downlink data through previous bearer but continues receiving data through new bearer.

14.3.5 QoS/resource management for network-assisted UE-to-UE communications

14.3.5.1 General

This feature provides the SEAL NRM support for coordinated QoS/resource management for network assisted UE-to-UE communications. Such capability may be required for guaranteeing end-to-end QoS fulfilment (primarily for meeting end-to-end latency requirements) in network assisted UE to UE communications and may accommodate various vertical-specific application services, e.g.:

- Network-assisted Command and Control (C2) communications in UASAPP [TS 23.255], where the UAV controller navigates its UAV over the 5GS;

- Teleoperated Driving (ToD) in eV2XAPP [TS 23.286], where the a V2X UE acting as server may remotely control a further V2X UE over the 5GS;

- Network-assisted Device-to-Device communications in Factory of the Future (FF) use cases, such as control-to-control communications.

14.3.5.2 QoS/resource management capability initiation in network assisted UE-to-UE communications

This procedure provides a mechanism for initiating the capability at the NRM server for managing the end-to-end application QoS requirement fulfilment for a network-assisted VAL UE to VAL UE session (comprising a PDU session for each of the constituent links, e.g. VAL UE 1 to PLMN, and PLMN to VAL UE 2). The request may come from NRM client of either of the VAL UEs within the service and will trigger the end-to-end QoS/resource management by the NRM server. The triggering the end-to-end QoS management request can be initiated by the VAL application at the VAL UE, and the conditions may depend on the requirements of the VAL service, e.g. for UAS such triggering may be needed when a UAV is in-flight, or for V2X such trigger may be initiated when a controlled VAL UE enters an urban area.

14.3.5.2.1 Procedure

Figure 14.3.5.2.1-1 illustrates the procedure where the NRM server is initiating the end-to-end QoS/resource management capability for network-assisted UE-to-UE communications.

Pre-conditions:

1. The NRM client is connected to the NRM server.

2. The VAL UEs involved in the end-to-end session (VAL UE 1 and VAL UE 2) are connected to one or more PLMNs and have ongoing PDU sessions.

3. NRM server has used the "Setting up an AF session with required QoS procedure" (clause 4.15.6.6 of TS 23.502).
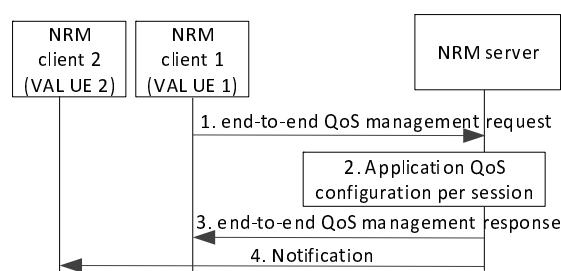
Figure 14.3.5.2.1-1 end-to-end QoS management request / response

1. The NRM client 1 (of VAL UE 1) sends to the NRM server an end-to-end QoS management request for managing the QoS for the end-to-end application session.

2. The NRM server configures the application QoS parameters by decomposing the end-to-end QoS requirements (VAL UE 1 to VAL UE 2) to application QoS parameters for each individual session (e.g. network session for VAL UE 1 -and network session for VAL UE 2) which are part of the end-to-end application session.

3. The NRM server sends to the NRM client 1 an end-to-end QoS management response with a positive or negative acknowledgement of the request.

4. The NRM server may also send a notification to NRM client 2 (of VAL UE 2) to inform about the end-to-end QoS management initiation by the NRM server.

14.3.5.3 Procedure for coordinated QoS provisioning operation in network assisted UE-to-UE communications

This procedure provides a mechanism for ensuring the end-to-end application QoS requirement fulfilment for the application service (which is between two or more VAL UEs), considering that the QoS of one of the links may downgrade. It is assumed that the application session is ongoing, and both the source and target VAL UEs are connected to 3GPP network (the same or different). The communication between the VAL UEs is assumed to be in-direct / network-assisted; hence two PDU sessions are established respectively (one per VAL UE).

14.3.5.3.1 Procedure

Figure 14.3.5.3.1-1 illustrates the procedure where the NRM server supports the coordinated QoS provisioning for network-assisted UE-to-UE communications.

Pre-conditions:

1. NRM server has activated the end-to-end QoS/resource management capability, as described in 14.3.5.2.1

2. NRM server, acting as AF, has registered to receive QoS monitoring event notifications from 5GC and notifications from VAL UEs (from both UEs), as specified in TS 23.501.
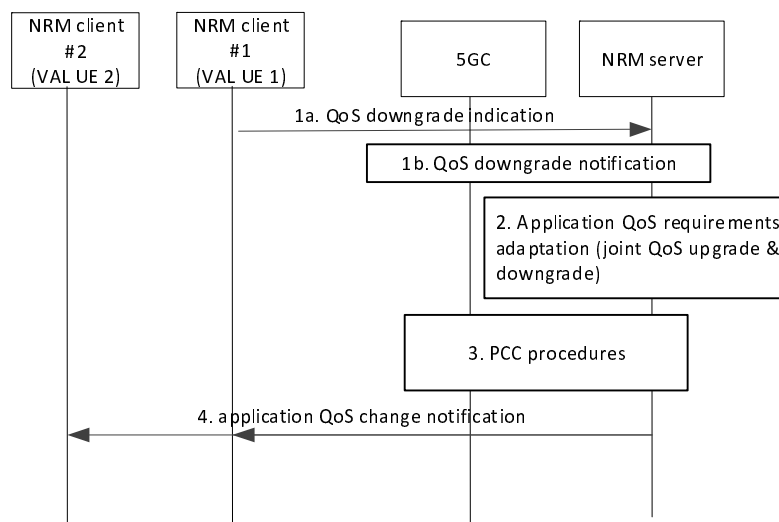
Figure 14.3.5.3.1-1: NRM-assisted coordinated QoS provisioning for C2 communication

1a. A QoS downgrade trigger event is sent from the NRM client of the VAL UE 1 to the NRM server, denoting an application QoS degradation (experienced or expected) e.g. based on the experienced packet delay or packet loss for the Uu link (e.g. packet loss great than threshold value). The conditions for triggering the QoS downgrade indication from the NRM client is based on the threshold that may be provided in advance by the NRM server (at the end-to-end QoS management response by the NRM server in 14.3.5.2.1).

1b. Alternatively, the NRM server receives a trigger event from the 5GC (SMF/NEF), denoting a QoS downgrade notification for the VAL UE 1 session. (described in clause 5.7.2.4.1b of 3GPP TS 23.501).

2. The NRM server evaluates the fulfilment/non-fulfilment of the end-to-end QoS based on the trigger event. NRM server may retrieve additional information based on subscription to support its evaluation. This could be from the 5GC (NEF Monitoring Events as in 23.502, QoS sustainability analytics as in TS 23.288 [34]) or SEAL LMS (on demand location reporting for one or both VAL UEs 1 and 2).

Then, the NRM server, determines an action, which is the QoS parameter adaptation of one or both links (QoS profile downgrade for the link receive QoS notification control, and QoS upgrade for the link which can be upgraded).

3. The NRM/SEAL server, acting as AF, sends to the 5GC (to SMF via NEF or to PCF via N5) a request for a change of the QoS profile mapped to the one or both network sessions (for VAL UE 1 and UE 2) or the update of the PCC rules to apply the new traffic policy (as specified in 3GPP TS 23.502 in clause 4.15.6.6a: AF session with required QoS update procedure).

4. The NRM server sends an application QoS change notification to the affected NRM clients, to inform on the adaptation of the QoS requirements for the individual session.

14.3.6 Event Monitoring

14.3.6.1 General

The VAL server utilizes the NRM server for monitoring the events related to its VAL UEs and receive the event reports. The NRM server shall subscribe to multiple core network services to fetch all the required events related to the multiple VAL UEs served by the VAL server and report the same to the VAL server with the event details.

To monitor and report the events related to the VAL UE from the 3GPP core network, the NRM server shall use the Monitoring Events procedures as specified in 3GPP TS 23.502 [11].

To monitor and report the analytics events related to the VAL UE, the NRM server shall use the procedures specified in 3GPP TS 23.288 [34].

14.3.6.2 Monitoring Events Subscription Procedure

14.3.6.2.1 General

The VAL server subscribes to the NRM server to monitor the events related to VAL UE(s). Based on the VAL server request, the NRM server consumes the relevant core network services to receive the events related to the VAL UE(s). The related procedure is illustrated in the next clause.

14.3.6.2.2 Procedure

The procedure for VAL server subscribing to the NRM server, to monitor the VAL UE(s) related events is described in figure 14.3.6.2.2-1.

Pre-conditions:

- The NRM server is authorized to consume the core network services (Monitoring events as specified in 3GPP TS 23.502 [11] and Analytics services as specified in 3GPP TS 23.288 [34]);
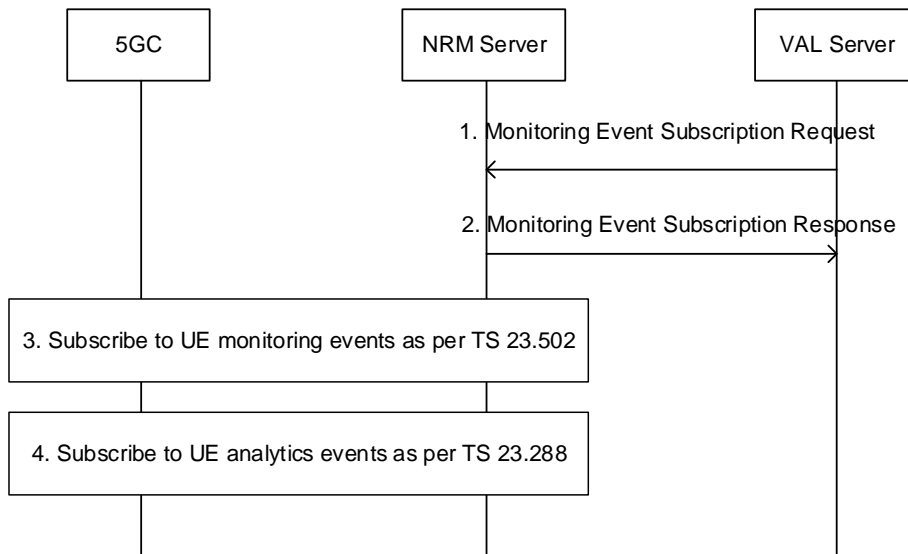
Figure 14.3.6.2.2-1: Monitoring Events Subscription Procedure

1. The VAL server sends Monitoring Events Subscription request to the NRM server, requesting the NRM server to monitor the events related to the VAL UE(s) as per the subscription request, and shall include the information related to the events that the VAL server is interested in.

2. The NRM server shall check if the VAL server is authorized to initiate the Monitoring Events Subscription request and if authorized, shall respond with Monitoring Events Subscription Response message, indicating the successful subscription status along with subscription information to the VAL server. The VAL service ID may be used by the NRM server to derive event specific information in 3GPP core network services (e.g. QoS requirement in analytics event subscription), based on e.g. local configuration. The NRM server maps the VAL group ID (if received) to the External Group ID known to the 3GPP core network.

NOTE: The mapping between Monitoring profile ID and event details in the NRM server can be pre-configured and/or dynamically built based on VAL server request with explicitly sent event details, which is implementation specific.

3. Based on the events of interest information in the subscription request message, if applicable, the NRM server shall subscribe to the UE monitoring events (like, LOSS_OF_CONNECTIVITY, COMMUNICATION_FAILURE etc.) for the set of UEs (VAL UEs) in the subscription request, as specified in 3GPP TS 23.502 [11].

4. Based on the events of interest information in the subscription request message, if applicable, the NRM server shall subscribe to the UE analytics events (like ABNORMAL_BEHAVIOUR etc.) for the set of UEs (VAL UEs) in the subscription request, as specified in 3GPP TS 23.288 [34].

14.3.6.3 Monitoring Events Notification Procedure

14.3.6.3.1 General

The NRM server receives the events related to VAL UE(s) from the 3GPP core network. The NRM server reports the monitoring events information to the VAL server.

14.3.6.3.2 Procedure

The procedure for NRM server notifying the VAL server with VAL UE(s) related events is described in figure 14.3.6.3.2-1.

Pre-conditions:

- The VAL server has subscribed with NRM server using Monitoring Events Subscription Procedure as specified in clause 14.3.6.2;
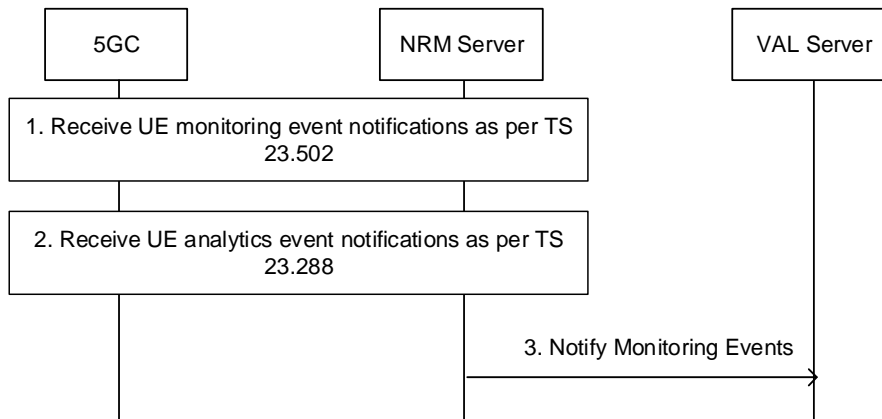
Figure 14.3.6.3.2-1: Monitoring Events Notification Procedure

1. If applicable, the NRM server receives the VAL UE related monitoring event notifications from the 3GPP core network as specified in 3GPP TS 23.502 [11].

2. If applicable, the NRM server receives the VAL UE related Analytics event notifications from the 3GPP core network as specified in 3GPP TS 23.288 [34].

3. The NRM server notifies the VAL server about the events related to the VAL UE in Notify Monitorng Events message. If multiple events are to be notified, then the NRM server may aggregate the notifications and send to the VAL server.

14.3.7 5G TSC resource management procedures

14.3.7.1   General

The procedures related to the 5G TSC network resource management are described in the following subclauses.

14.3.7.2   TSC stream availability discovery procedure

The TSC stream availability discovery procedure is used by the VAL server to discover the availability of resources for TSC communication for the given stream specification (i.e., between the target UEs) prior to creating the stream.

Pre-conditions:

1. Each UE has an established Ethernet PDU session and DS-TTs are connected to the 5GS TSC bridge. The traffic classes are configured on each DS-TT.

2. The NRM server has collected the 5GS TSC bridge management and port management information. The latter is related to the Ethernet ports located in the DS-TTs including bridge delay per DS-TT Ethernet port pair per traffic class.

3. NRM server has calculated the bridge delay for each port pair, i.e. composed of (ingress DS-TT Ethernet port, egress DS-TT Ethernet port) including the UE-DS-TT residence time, packet delay budget (PDB) and propagation delay for both UL from sender UE and DL to receiver UE.
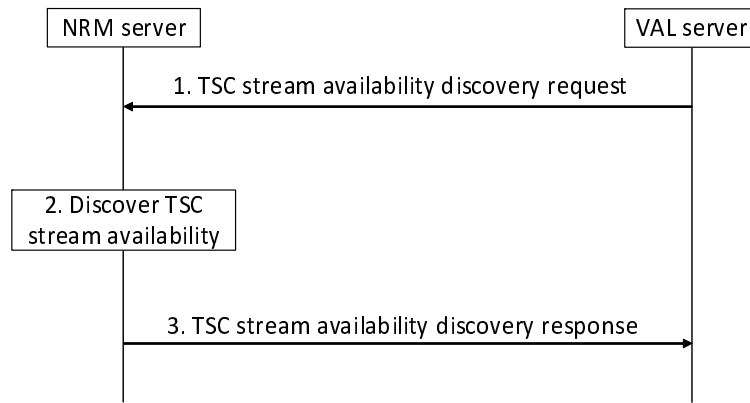
Figure 14.3.7.2-1: TSC stream availability discovery procedure

1. The NRM server receives a request from a VAL server on NRM-S reference point to discover the connectivity and available QoS characteristics between DS-TTs identified by the stream specification.

2. The NRM server validates the connectivity between the DS-TTs connected in the same 5GS TSC bridge based on the collected 5GS TSC bridge management and port management information, identifies the traffic classes supported by the DS-TTs and determines the end-to-end latency (including the UE-DS-TT residence times, PDBs and propagation delay).

3. NRM server responds to the VAL server with the stream specification and a list of traffic specifications with the available end-to-end latency and the traffic classes supported by the DS-TTs.

14.3.7.3 TSC stream creation procedure

This procedure allows the VAL server to create a TSC stream. The TSC stream creation procedure enables the VAL server to establish TSC connectivity with the required QoS between the UEs connected to the 5GS after the stream discovery procedure.

Pre-conditions:

1. Each UE has an established Ethernet PDU session for its DS-TT port MAC address.

2. Connectivity between the DS-TTs has been validated by the TSC stream availability discovery procedure.

3. NRM server maintains mapping from the traffic class to TSC QoS.
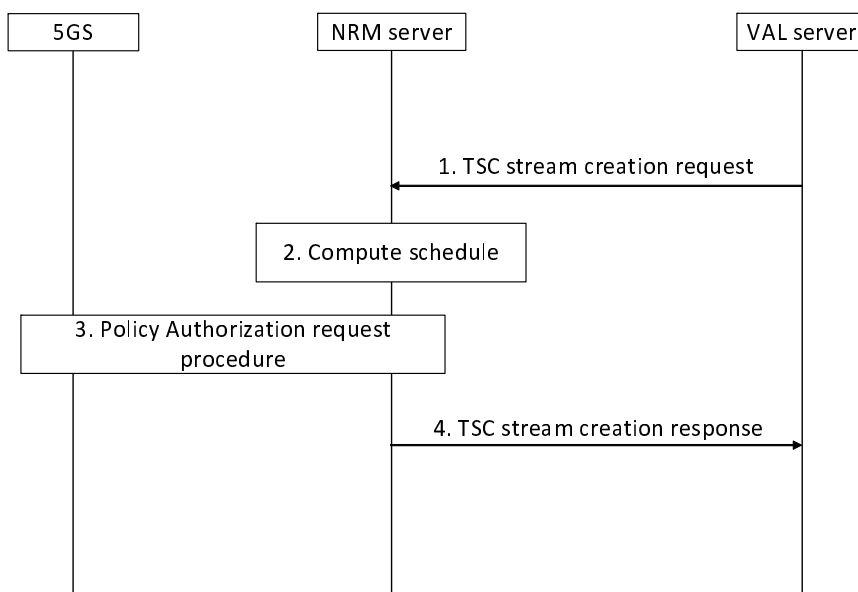
Figure 14.3.7.3-1: TSC stream creation procedure

1. NRM server receives a TSC stream creation request from a VAL server to create a TSC stream identified by a VAL Stream ID, between DS-TT ports in the stream specification and for the traffic class in the traffic specification.

2. NRM server calculates the schedule for the VAL Stream ID based on the information collected earlier from the 5GS via N5. It provides per-stream filtering and policing parameters (e.g. as defined in IEEE 802.1Q [IEEE8021Q]) used to derive the TSC QoS information and related flow information. NRM server also provides the forwarding rule (e.g. as defined in IEEE 802.1Q [IEEE8021Q]) used to identify the DS-TT MAC address of the corresponding PDU session. Based on the 5GS bridge delay information it determines the TSC QoS information and TSC Assistance information for the stream.

3. As a TSCTSF, the NRM server triggers via N5 the Npcf_policy_Authorization_Create service operation as described in 3GPP TS 23.502 [11] for the TSC stream for both UL QoS flow (sender UE to UPF/bridge) and DL QoS flow (UPF/bridge to receiver UE). The Policy Authorization request includes the DS-TT port MAC address, TSC QoS information, TSC Assistance Information (3GPP TS 23.501 [1], cl.5.27.2.3), flow bit rate, priority, Service Data Flow Filter containing flow description including Ethernet Packet Filters. The QoS flow will be assigned for the PDU session for the source MAC address for the UL direction and for the PDU session for the destination MAC address for the DL direction. This information is delivered to the DS-TT by the 5GS.

Editor's note: Using gate control parameters for hold and forward buffering is FFS.

4. NRM server sends TSC stream creation response to the VAL server with the result of TSC stream creation for the VAL Stream ID.

14.3.7.4 TSC stream deletion procedure

This procedure allows the VAL server to delete a TSC stream.

Pre-conditions:

1. The TSC stream is configured in the 5GS and the DS-TTs.
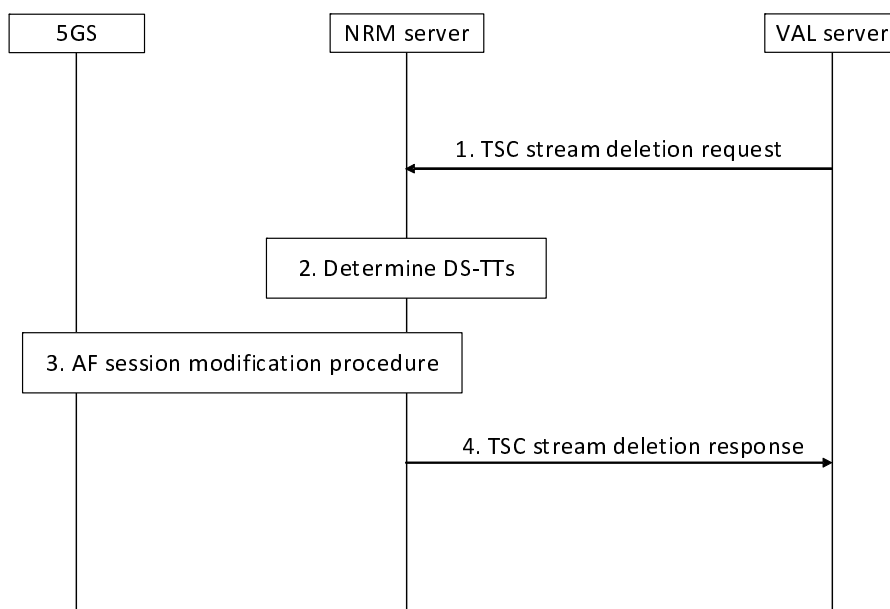
Figure 14.3.7.4-1: TSC stream deletion procedure

1. NRM server receives a request from VAL server to delete a TSC stream for with a VAL Stream ID.

2. NRM server identifies the MAC addresses of the DS-TTs involved in the stream based on the stored information for the VAL Stream ID.

3. As a TSCTSF, the NRM server triggers via Nxx the Npcf_PolicyAuthorization_Delete service operation defined in 3GPP TS 23.502 [11] for MAC addresses referred to by the VAL Stream ID. NRM server uses the procedure to delete both UL QoS flow (sender UE to UPF/bridge) and DL QoS flows (UPF/bridge to receiver UE) from the PDU sessions of the UEs referred to by the VAL Stream ID.

4. NRM server sends TSC stream deletion response to the VAL server with the result of TSC stream deletion for the VAL Stream ID.

14.3.8 TSN resource management procedures

14.3.8.1   General

The procedures related to the TSN network resource management are described in the following subclauses.

14.3.8.2   5GS TSN Bridge information reporting

Pre-conditions:

1. There is already an established session between the TSN CNC and the NRM-S acting as TSN-AF.
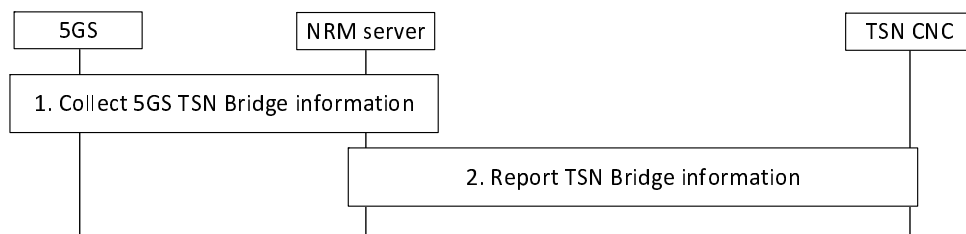
Figure 14.3.8.2-1: TSN Bridge information reporting procedure

1. Acting as the TSN AF the NRM server collects 5GS TSN Bridge information by interaction with the 5GS via the N5 reference point, as described in in TS 23.502 [11] Annex F.1. The NRM server stores the binding relationship between 5GS Bridge ID, MAC address of the DS-TT Ethernet port and also updates 5GS bridge delay as defined in clause 5.27.5 of TS 23.501 [10]. The NRM server retrieves txPropagationDelay and Traffic Class table from DS-TT and it also retrieves txPropagationDelay and Traffic Class table from NW-TT.

2. Whenever there is a new or updated bridge information the NRM server interacts with the TSN CNC and reports the TSN Bridge information to register a new TSN Bridge or update an existing TSN Bridge. The TSN CNC stores the TSN Bridge information and confirms to the NRM server.

14.3.8.3   5GS TSN Bridge configuration procedure

Pre-conditions:

1. The TSN CNC has stored the 5GS TSN Bridge information received from the NRM server acting as TSN AF.

2. The NRM server acting as TSN AF has stored the 5GS TSN Bridge information collected from the 5GS, as described in clause 14.3.8.2.
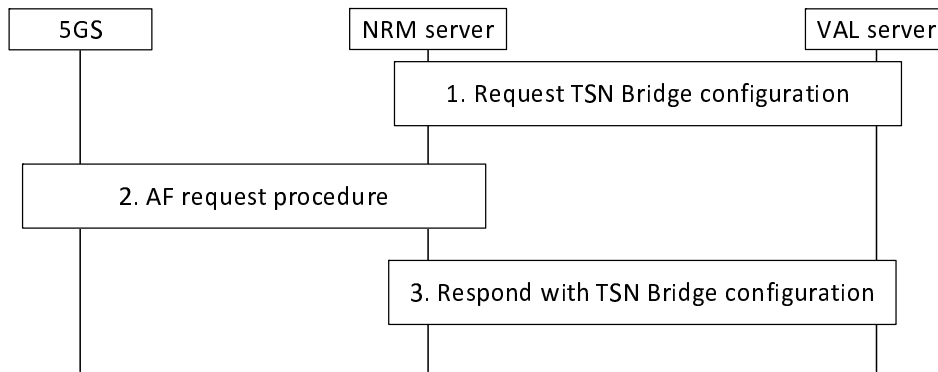
Figure 14.3.8.3-1: TSN Bridge configuration procedure

1. The NRM server receives from the TSN CNC per-stream filtering, policing parameters and related flow information according to IEEE 802.1Q [36] and it uses them to derive TSN QoS information and related flow information. The TSN AF uses this information to identify the DS-TT MAC address of the corresponding PDU session.

2. NRM server triggers via N5 the AF request procedure as described in 3GPP TS 23.502 [11] Annex F.2. The AF request includes the DS-TT port MAC address, TSC QoS information, TSC Assistance Information, flow bit rate, priority, Service Data Flow Filter containing flow description including Ethernet Packet Filters.

3. NRM server responds with a TSN Bridge configuration.

14.4 SEAL APIs for network resource management

14.4.1 General

Table 14.4.1-1 illustrates the SEAL APIs for configuration management.

Table 14.4.1-1: List of SEAL APIs for network resource management

API Name	API Operations	Known Consumer(s)	Communication Type
SS_NetworkResourceAdaptation	Reserve_Network_Resource	VAL server	Request /Response
	Request_Unicast_Resource	VAL server	Request /Response
	Update_Unicast_Resource	VAL server	Request /Response
	Request_Multicast_Resource	VAL server	Request /Response
	Notify_UP_Delivery_Mode	VAL server	Subscribe/Notify
	TSC_Stream_Availability_Discovery	VAL server	Request /Response
	TSC_Stream_Creation	VAL server	Request /Response
	TSC_Stream_Deletion	VAL server	Request /Response
SS_EventsMonitoring	Subscribe_Monitoring_Events	VAL server	Subscribe/Notify
	Notify_Monitoring_Events	VAL server	
SS_NetworkResourceMonitoring	Subscribe_Unicast_QoS_Monitoring	VAL server	Subscribe/Notify
	Notify_Unicast_QoS_Monitoring	VAL server	
	Unsubscribe_Unicast_QoS_Monitoring	VAL server	
	Obtain_Unicast_QoS_Monitoring_Data	VAL server	Request /Response

14.4.2 SS_NetworkResourceAdaptation API

14.4.2.1 General

API description: This API enables the VAL server to communicate with the network resource management server for network resource adaptation and VAL UE monitoring over NRM-S.

14.4.2.2 Reserve_Network_Resource operation

API operation name: Reserve_Network_Resource

Description: Requesting for network resource adaptation.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.1

Outputs: See subclause 14.3.2.2

See subclause 14.3.3 for the details of usage of this API operation.

14.4.2.3 Request_Unicast_Resource

API operation name: Request_Unicast_Resource

Description: Requesting unicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.6

Outputs: See subclause 14.3.2.7

See subclause 14.3.3 for the details of usage of this API operation.

14.4.2.4 Update_Unicast_Resource

API operation name: Update_Unicast_Resource

Description: Updating unicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.8

Outputs: See subclause 14.3.2.9

See subclause 14.3.3 for the details of usage of this API operation.

14.4.2.5 Request_Multicast_Resource

API operation name: Request_Multicast_Resource

Description: Requesting multicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.10

Outputs: See subclause 14.3.2.11

See subclause 14.3.4 for the details of usage of this API operation.

14.4.2.6 Notify_UP_Delivery_Mode

API operation name: Notify_UP_Delivery_Mode

Description: Notifying the user plane delivery mode.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.12

Outputs: None.

See subclause 14.3.4 for the details of usage of this API operation.

14.4.2.7 TSC_Stream_ Availability_Discovery

API operation name: TSC_Stream_ Availability_Discovery

Description: Requesting to discover the connectivity and available QoS characteristics between DS-TTs.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.23

Outputs: See subclause 14.3.2.24

See subclause 14.3.7.2 for the details of usage of this API operation.

14.4.2.8 TSC_Stream_Creation

API operation name: TSC_Stream_Creation

Description: Requesting the NRM to create a TSC stream.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.25

Outputs: See subclause 14.3.2.26

See subclause 14.3.7.3 for the details of usage of this API operation.

14.4.2.9 TSC_Stream_Deletion

API operation name: TSC_Stream_Deletion

Description: Requesting the NRM to delete the TSC stream.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.27

Outputs: See subclause 14.3.2.28

See subclause 14.3.7.4 for the details of usage of this API operation.

14.4.3 SS_EventsMonitoring API

14.4.3.1 Subscribe_Monitoring_Events

API operation name: Subscribe_Monitoring_Events

Description: Subscription to monitoring events.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.17

Outputs: 14.3.2.18.

See subclause 14.3.6.2 for the details of usage of this API operation.

14.4.3.2 Notify_Monitoring_Events

API operation name: Notify_Monitoring_Events

Description: Notifying the VAL server with monitoring events related to VAL UE(s).

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.19

Outputs: None.

See subclause 14.3.6.3 for the details of usage of this API operation.

14.4.4 SS_NetworkResourceMonitoring API

14.4.4.1 General

API description: This API enables the VAL server to monitor a network resource and to retrieve monitoring data.

14.4.4.2 Subscribe_Unicast_QoS_Monitoring operation

API operation name: Subscribe_Unicast_QoS_Monitoring

Description: Subscribing to QoS monitoring of a unicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.20

Outputs: See subclause 14.3.2.21

See subclause 14.3.3.4.1 for the details of usage of this API operation.

14.4.4.3 Notify_Unicast_QoS_Monitoring operation

API operation name: Notify_Unicast_QoS_Monitoring

Description: Notification of latest QoS data of a monitored unicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.22

Outputs: See subclause 14.3.2.22

See subclause 14.3.3.4.2 for the details of usage of this API operation.

14.4.4.4 Unsubscribe_Unicast_QoS_Monitoring operation

API operation name: Unsubscribe_Unicast_QoS_Monitoring

Description: Unsubscribing from QoS monitoring of a unicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.20

Outputs: See subclause 14.3.2.21

See subclause 14.3.3.4.3 for the details of usage of this API operation.

14.4.4.5 Obtain_Unicast_QoS_Monitoring_Data operation

API operation name: Obtain_Unicast_QoS_Monitoring_Data

Description: Request QoS monitoring data of a unicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.33

Outputs: See subclause 14.3.2.34

See subclause 14.3.3.4.4 for the details of usage of this API operation.

15 Service-based interface representation of the functional model for SEAL services

15.1 General

The functional models for SEAL services is represented using functional entities and reference points between the functional entities as specified in subclause 6. The vertical applications consume the SEAL services in the form of APIs. Each SEAL service offers these APIs on a service-based interface to all its consumer entities.

15.2 Functional model representation

Figure 15.2-1 illustrates the service-based interface representation of the functional model for SEAL services.
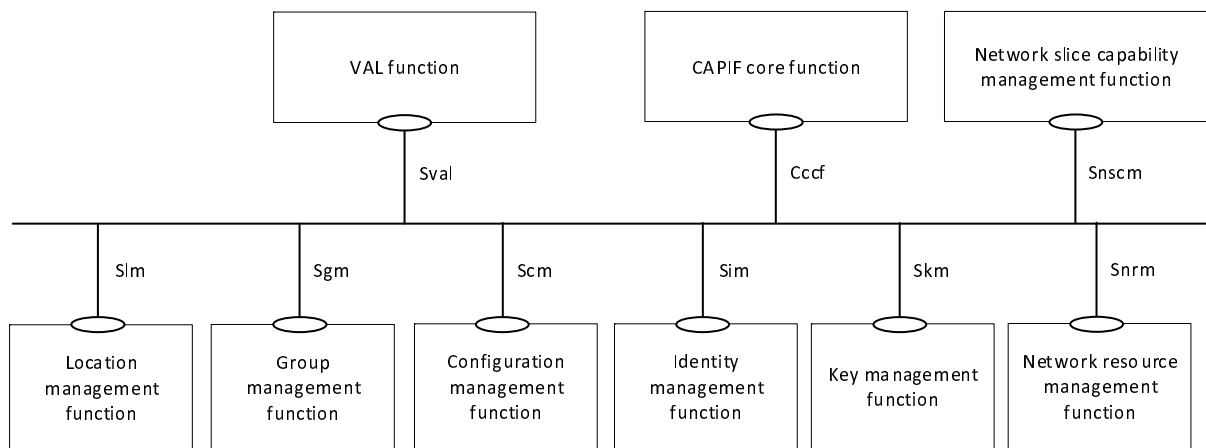
Figure 15.2-1: SEAL generic functional model representation using service-based interfaces

The SEAL function(s) exhibit the service-based interfaces which are used for providing and consuming SEAL services. The service APIs are specified for each SEAL function enabled over the service-based interface. The service-based interfaces of specific SEAL services are specified in this document. All the interactions with SEAL are governed based on the reference point interactions of the functional models specified in subclause 6. VAL function represents the functionalities of the VAL server.

NOTE: The service-based interface Sval for the VAL function is out of scope of the present document.

The service APIs offered by the SEAL function(s) are published and discovered on the CAPIF core function as specified in 3GPP TS 23.222 [8].

Editor's note: Refinement of the SEAL services in service-based interface representation is FFS.

15.3 Service-based interfaces

Table 15.3-1 specifies the service-based interfaces supported by SEAL.

Table 15.3-1: Service-based interfaces supported by SEAL

Service-based interface	Application functionEntity	Mapping server entity	APIs offered
Slm	Location management function	Location Management Server	Specified in subclause 9.4
Sgm	Group management function	Group management server	Specified in subclause 10.4
Scm	Configuration management function	Configuration management server	Specified in subclause 11.4
Sim	Identity management function	Identity management server	Specified in subclause 12.4
Skm	Key management function	Key management server	Specified in subclause 13.4
Snrm	Network resource management function	Network resource management server	Specified in subclause 14.4
Snsce	Network slice capability enablement function	Network slice capability enablement server	Specified in subclause 16.4
Cccf	CAPIF core function	Not applicable	Specified in subclause 10 of 3GPP TS 23.222 [8]

16 Network slice capability enablement

16.1 General

The network slice capability enablement is a SEAL service that offers network slice capability enablement capabilities, such as support for vertical application to slice re-mapping (which can be defined as the mapping of the UEs running a vertical application to different slice), to one or more vertical applications. In particular, network slice capability enablement uses a network-based mechanism to apply the slice re-mapping based on the network slice capability enablement server configuration, where the network slice capability enablement server acting as AF influences the URSP rules for the application traffic per UE by providing a guidance on the route selection parameters (including the S-NSSAI and DNN mapping).

NOTE: The network slice capability enablement server, acts as an AF within the trusted domain (MNO-owned, or trusted third party).

16.2 Functional model

16.2.1 General

The functional model for the network slice capability enablement is based on the generic functional model specified in clause 6.2. It is organized into functional entities to describe a functional architecture which addresses the support for network slice capability enablement aspects for vertical applications. Since the slicing is a feature which considers the Uu interfaces, only the on-network functional model is specified in this clause.

16.2.2 Functional model description

Figure 16.2.2-1 illustrates the generic functional model for network slice capability enablement.
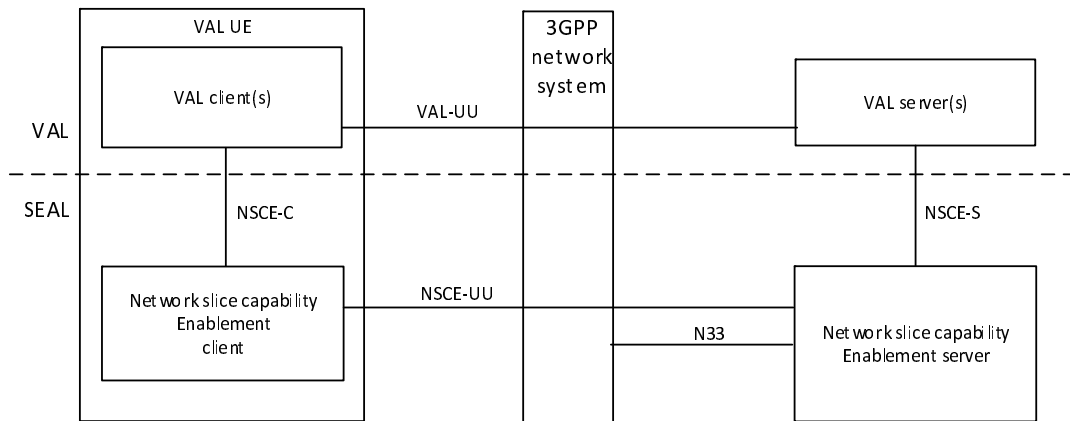
Figure 16.2.2-1: Functional model for network slice capability enablement

The network slice capability enablement client communicates with the network slice capability enablement server over the NSCE-UU reference point. The network slice capability enablement client provides the support for network slice capability enablement functions to the VAL client(s) over NSCE-C reference point. The VAL server(s) communicates with the network slice capability enablement server over the NSCE-S reference point. It is assumed that the network slice capability enablement server is deployed at the 5G system domain. The network slice capability enablement server, acting as AF, may communicate with the 5G Core Network functions via NEF (N33) reference point (for interactions with PCF).

16.2.3   Functional entities description

16.2.3.1 General

The functional entities for network slice capability enablement SEAL service are described in the following subclauses.

16.2.3.2 Network slice capability enablement server

The network slice capability enablement server functional entity provides the enablement of the network slicing aspects to support the VAL applications. Such enablement supports the mapping or migration of one or more vertical applications to one or more network slices (from a set of network slices, as provided by the 3GPP network system) as described in procedure in clauses 16.3.2.3 and 16.3.2.4. Such adaptation assumes that the UE is subscribed to more than one slice and is done via providing a guidance to update the URSP rules at the 5GS (denoted in clause 16.3.3 as network-based mechanism).

16.2.3.3 Network slice capability enablement client

The network slice capability enablement client functional entity acts as the application client for the slice enablement. The network slice capability enablement client interacts with the network slice capability enablement server to trigger a network slice adaptation due to an application requirement change. This trigger may be due to an application QoS requirement change, a service operation change. The NSCE client may receive a network slice / DNN re-mapping notification from the NSCE server. The NSCE client may optionally notify the VAL client on the network slice / DNN re-mapping.

16.2.4   Reference points description

16.2.4.1   General

The reference points for the functional model for network slice capability enablement are described in the following subclauses.

16.2.4.2 NSCE-UU

The interactions related to network slice capability enablement functions between the network slice capability enablement server and the network slice capability enablement client are supported by NSCE-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.501 [10].

16.2.4.3 NSCE-C

The interactions related to network slice capability enablement functions between the VAL client(s) and the network slice capability enablement client within a VAL UE are supported by the NSCE-C reference point. The NSCE client may receive an application requirement change over NSCE-C. Further, the NSCE client may provide a notification on the network slice adaptation upon successful adaptation of the slice to application mapping.

16.2.4.4 NSCE-S

The interactions related to network slice capability enablement functions between the VAL server(s) and the network slice capability enablement server are supported by the NSCE-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

16.2.4.5 N33

The reference point N33 supports the interactions between the network slice capability enablement server and the NEF and is specified in 3GPP TS 23.501 [10]. N33 is used for the network-based mechanism for slice re-mapping, where NSCE server acting as AF influences the URSP rules for the application traffic per UE by providing a guidance on the route selection parameters (including the S-NSSAI and DNN mapping), as specified in TS23.502 clause 4.15.6.10, TS 23.503 clause 6.6.2.2, TS 23.548 clause 6.2.4.

16.3 Procedures and information flows for network slice capability enablement

16.3.1 General

16.3.2 Network slice adaptation for VAL application

16.3.2.1 General

This subclause describes the procedure for network slice adaptation at the Network Slice Capability Enablement (NSCE) server, based on a request from a VAL server to adapt the network slice for the VAL application. This request is handled between the NSCE server and the NSCE client per each VAL UE of the VAL application.

16.3.2.2 Information flows

16.3.2.2.1 Network slice adaptation request

Table 16.3.2.2.1-1 describes the information flow network slice adaptation request from the VAL server to the NSCE server.

Table 16.3.2.2.1-1: Network slice adaptation request

Information element	Status	Description
VAL service ID	M	The VAL service ID of the VAL application for which the network slice adaptation may corresponds to.
List of VAL UE IDs	M	List of the VAL UE IDs within the VAL service for which the slice adaptation request corresponds
Network slice adaptation cause	O	The cause which necessitates the network slice change (e.g. VAL service profile change, VAL service operation change).
Requested S-NSSAI	O	Indication of the new S-NSSAI which is requested.
Requested DNN	O	Indication of the new DNN which is requested.

Editor's note: The details of Network slice adaptation request is FFS

16.3.2.2.2 Network slice adaptation response

Table 16.3.2.2.2-1 describes the information flow network slice adaptation response from the NSCE server to the VAL server.

Table 16.3.2.2.2-1: Network slice adaptation response

Information element	Status	Description
Result	M	Result includes success or failure of the network slice adaptation with the underlying network.

16.3.2.2.3 Network slice adaptation trigger

Table 16.3.2.2.3-1 describes the information flow Network slice adaptation trigger from the NSCE client to the NSCE server.

Table 16.3.2.2.3-1: Network slice adaptation trigger

Information element	Status	Description
VAL UE ID(s)	M	The VAL UE ID(s) within the VAL service, for which the network slice adaptation trigger applies
VAL service ID	M	The VAL service ID of the VAL application for which the network slice configuration may corresponds to.
Requested S-NSSAI	M	Indication of the new S-NSSAI which is requested.
Requested DNN	O	Indication of the new DNN which is requested.

16.3.2.2.4 Network slice adaptation notification

Table 16.3.2.2.4-1 describes the information flow network slice adaptation notification from the NSCE server to the NSCE client and optionally to the VAL client.

Table 16.3.2.2.4-1: Network slice adaptation notification

Information element	Status	Description
Result	M	Result includes success or failure of the network slice adaptation.

16.3.2.3 Procedure for VAL server-triggered and network-based network slice adaptation for VAL application

Figure 16.3.2.3-1 illustrates the VAL server-triggered and network-based procedure where the NSCE server supports the network slice adaptation with the underlying 3GPP system for the VAL UEs of the VAL application.
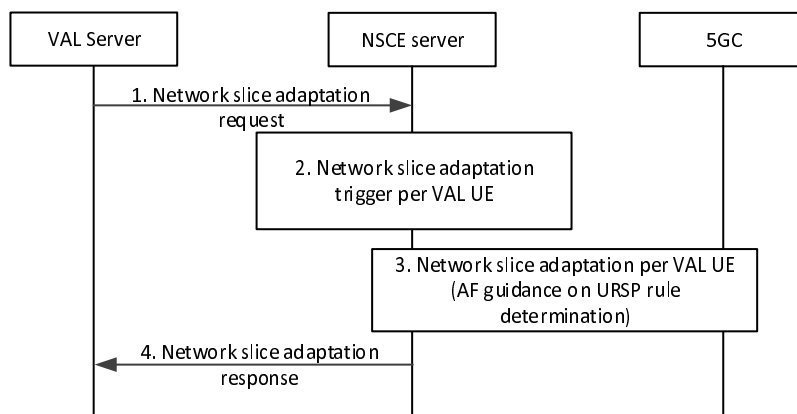
Figure 16.3.2.3-1: Network slice adaptation for VAL application

1. The VAL server sends a network slice adaptation request to the NSCE server for the VAL application (and the VAL UEs within the VAL application). This request may be in the form of exact requested network slice (and optionally DNN) for all the VAL UEs of the VAL application; or indication that the VAL application needs to be remapped to a different network slice (and optionally DNN).

2. The NSCE server processes the request and triggers the network slice configuration per VAL UE within the VAL Application.

3. The NSCE server acting as AF provides the updated S-NSSAI and DNN per VAL UE. In particular, NSCE server sends this information to the PCF via NEF as part of the AF-driven guidance for URSP determination to 5G system (as specified in TS23.502 clause 4.15.6.10, TS 23.503 clause 6.6.2.2, TS 23.548 clause 6.2.4). This guidance may update the route selection parameters to indicate different sets of PDU Session information (DNN, S-NSSAI) that can be associated with applications matching the application traffic.

NOTE: NSCE server provides the updated S-NSSAI/DNN as a suggestion/guidance to PCF; however it is up to PCF to decide whether to perform the slice/DNN re-mapping

4. Upon successful adaptation of the route selection parameters, the NSCE server provides a network slice adaptation response to the VAL server, providing information on the fulfilment of the network slice adaptation request per VAL application.

16.3.2.4 Procedure for VAL UE-triggered and network-based network slice adaptation for VAL application

Figure 16.3.2.4-1 illustrates the VAL UE-triggered and network-based procedure where the NSCE server supports the network slice adaptation with the underlying 3GPP system for the VAL UEs of the VAL application.

Pre-condition:

- The NSCE client has connected to the NSCE server;
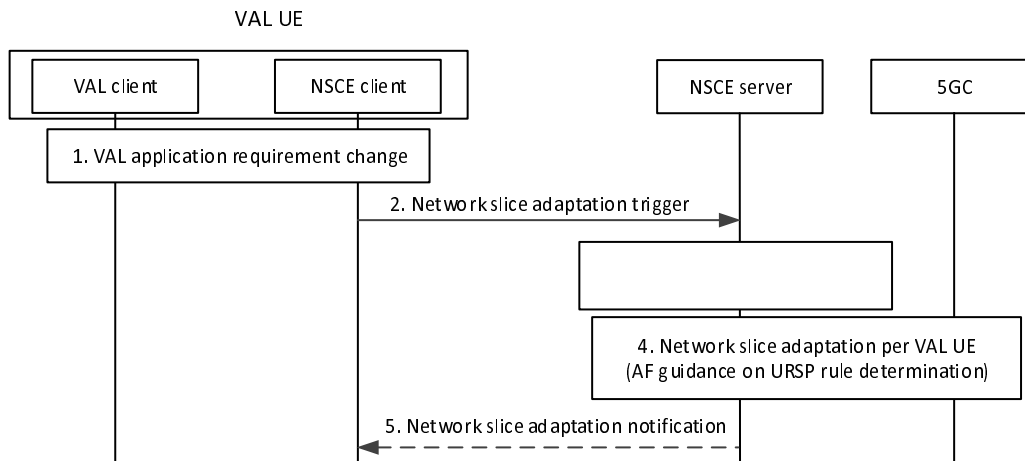
Figure 16.3.2.4-1: Network slice adaptation for VAL application

1. The VAL client provides a new application requirement to the NSCE client, indicating a new service profile for the VAL application. This may be in the form of a change at the application QoS requirements, service operation change, or other application-related parameters.

2. The NSCE client sends a network slice adaptation trigger to the NSCE server for the VAL application. This trigger may be in the form of exact requested network slice (and optionally DNN) for the VAL UE of the VAL application; or indication that the VAL application needs to be remapped to a different network slice (and optionally DNN).

NOTE 1：How the requested network slice is known by the NSCE client is out of scope of this release.

3. The NSCE server processes the request and triggers the network slice configuration per VAL UE within the VAL Application.

NOTE 2：Whether and how the NSCE server triggers the network slice adaptation for all the VAL UEs within the VAL Application is out of scope of this release.

4. The NSCE server acting as AF provides the updated S-NSSAI and DNN per VAL UE. In particular, NSCE server sends this information to the PCF via NEF as part of the AF-driven guidance for URSP determination to 5G system (as specified in TS23.502 clause 4.15.6.10, TS 23.503 clause 6.6.2.2, TS 23.548 clause 6.2.4). This guidance may update the route selection parameters to indicate different sets of PDU Session information (DNN, S-NSSAI) that can be associated with applications matching the application traffic.

NOTE 3: NSCE server provides the updated S-NSSAI/DNN as a suggestion/guidance to PCF; however it is up to PCF to decide whether to perform the slice/DNN re-mapping

5. The NSCE server may send a notification to the NSCE client indicating success or failure.

16.4   SEAL APIs for network slice capability enablement

16.4.1   General

Editor's note: The definition of SEAL APIs for NSCE-UU is FFS

Table 16.4.1-1 illustrates the SEAL APIs for network slice capability enablement.

Table 16.4.1-1: List of SEAL APIs for network slice capability enablement

API Name	API Operations	Known Consumer(s)	Communication Type
SS_NetworkSliceAdaptation	Network_slice_adaptation	VAL server	Request /Response

16.4.2　SS_NetworkSliceAdaptation API

16.4.2.1　General

API description: This API enables the VAL server to communicate with the network slice capability enablement server for network slice adaptation over NSCE-S.

16.4.2.2　Network_Slice_Adaptation

API operation name: Network_Slice_Adaptation

Description: Requesting for network slice adaptation.

Known Consumers: VAL server.

Inputs: See subclause 16.3.2.2.1

Outputs: See subclause 16.3.2.2.2

See subclause 16.3.2.3 for the details of usage of this API operation.

Annex A (informative):
SEAL integration with 3GPP network exposure systems

NOTE: Not all possible SEAL integration with 3GPP network exposure systems are illustrated in this subclause.

Figure A-1 illustrates the service-based interface representation of the functional model for SEAL services integration with 5GC network exposure system.

Figure A-1: SEAL integration with 5GC network exposure system

The details of NEF and its role in exposing network capabilities of 5GS to 3rd party applications are specified in 3GPP TS 23.501 [10] and the details of NEF service operations are specified in 3GPP TS 23.502 [11].

Figure A-2 illustrates the service-based interface representation of the functional model for SEAL services integration with EPC network exposure system.
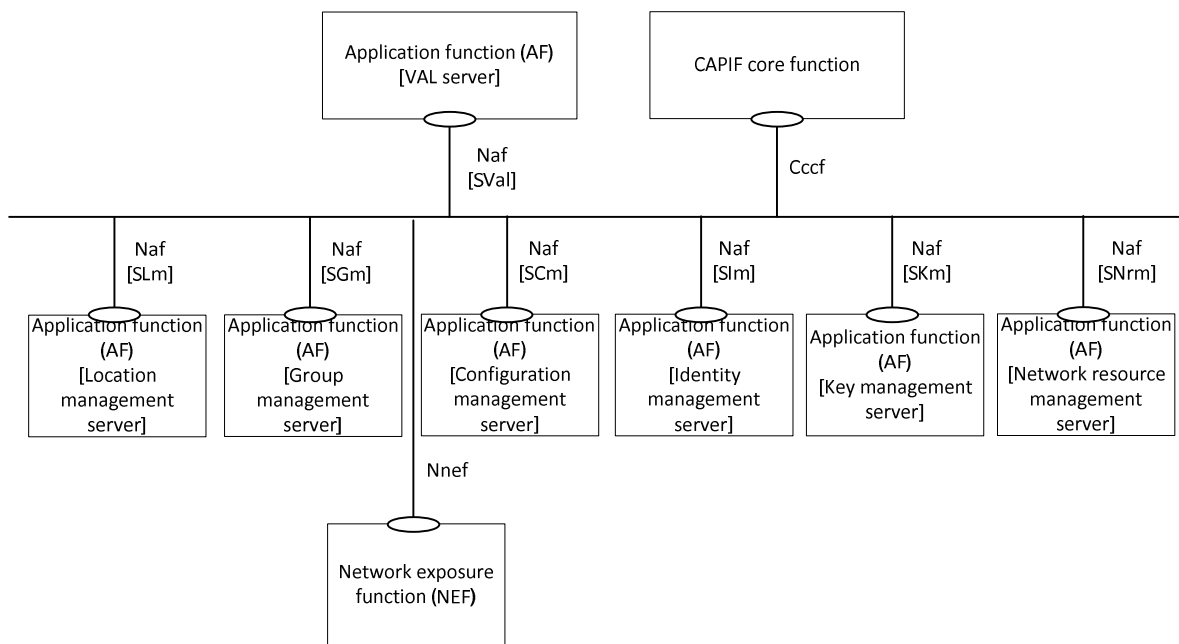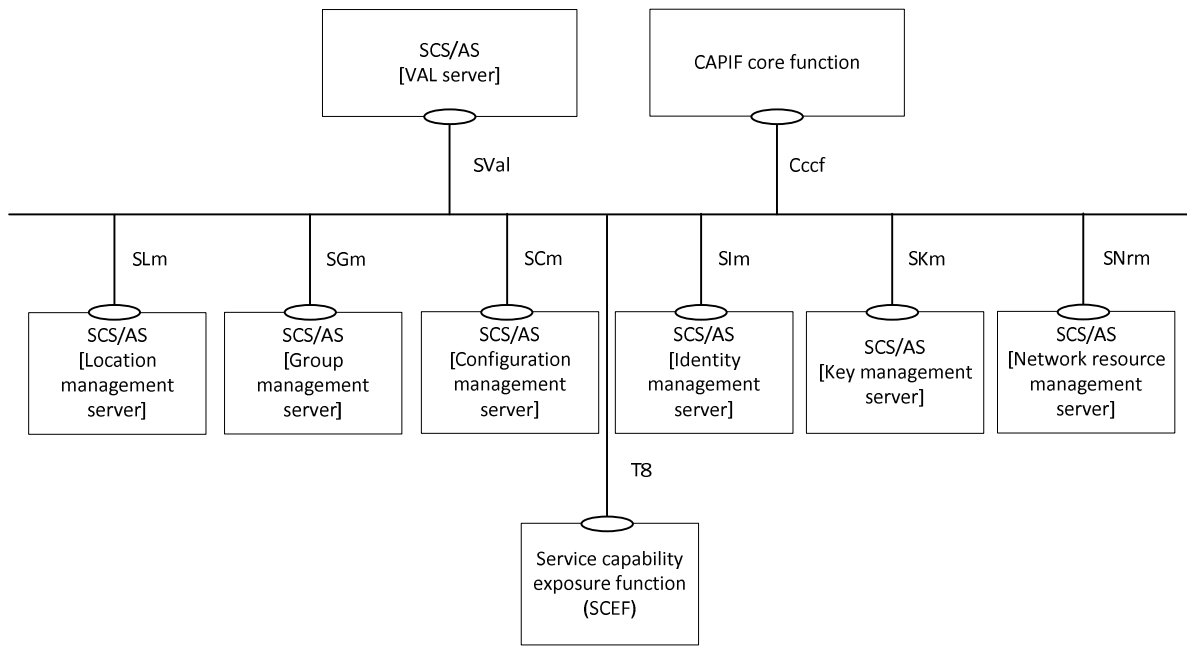
Figure A-2: SEAL integration with EPC network exposure system

The details of SCEF and its role in exposing network capabilities of EPS to 3rd party applications are specified in 3GPP TS 23.682 [13].

Annex B (informative):
SEAL functional model mapping with Common functional architecture (CFA)

The table B-1 shows the mapping between the SEAL functional model and the Common functional architecture (CFA). The details of CFA functional entities and reference points are specified in 3GPP TS 23.280 [4].

Table B-1: SEAL functional model mapping with CFA

SEAL service	Aspects	SEAL	CFA
Location management	Functional entity	Location management client	Location management client
		Location management server	Location management server
	Reference points	LM-UU	CSC-14
		LM-S	CSC-15
		LM-C	Not defined
		LM-E	Not defined
		LM-PC5	Not defined
Group management	Functional entity	Group management client	Group management client
		Group management server	Group management server
	Reference points	GM-UU	CSC-2
		GM-S	CSC-3
		GM-C	Not defined
		GM-E	CSC-16
		GM-PC5	CSC-12
Configuration management	Functional entity	Configuration management client	Configuration management client
		Configuration management server	Configuration management server
	Reference points	CM-UU	CSC-4
		CM-S	CSC-5
		CM-C	Not defined
		CM-E	CSC-17
		CM-PC5	CSC-11
Identity management	Functional entity	Identity management client	Identity management client
		Identity management server	Identity management server
	Reference points	IM-UU	CSC-1
		IM-S	Not defined
		IM-C	Not defined
		IM-E	Not defined
		IM-PC5	Not defined
Key management	Functional entity	Key management client	Key management client
		Key management server	Key management server
	Reference points	KM-UU	CSC-8
		KM-S	CSC-9
		KM-PC5	Not defined
Network resource management	Functional entity	Network resource management client	Not defined (see NOTE)
		Network resource management server	Not defined (see NOTE)
	Reference points	NRM-UU	Not defined (see NOTE)
		NRM-S	Not defined
		NRM-C	Not defined
		NRM-E	Not defined
		NRM-PC5	Not defined
NOTE: Defined in the application layer for Mission Critical service (e.g. MCPTT).			

Annex C (normative):
Protocol realizations of LWP in the signalling control plane

C.1 General

This annex specifies protocol realizations of the light-weight protocol in the signalling control plane.

C.2 Usage of CoAP as LWP

This clause specifies how the CoAP protocol shall be used to realize the generic light-weight protocol in the signalling control plane.

The Constrained Application Protocol (CoAP) is a light-weight protocol defined by IETF in RFC 7252 [32] and designed specifically for application layer communication for constrained devices. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments. RFC 7252 [32] specifies bindings to UDP and DTLS. IETF RFC 8323 [33] specifies bindings to TCP, WebSocket and TLS.

Figure C.2-1 illustrates the functional model for the LWP signalling control plane when CoAP is used as the LWP.
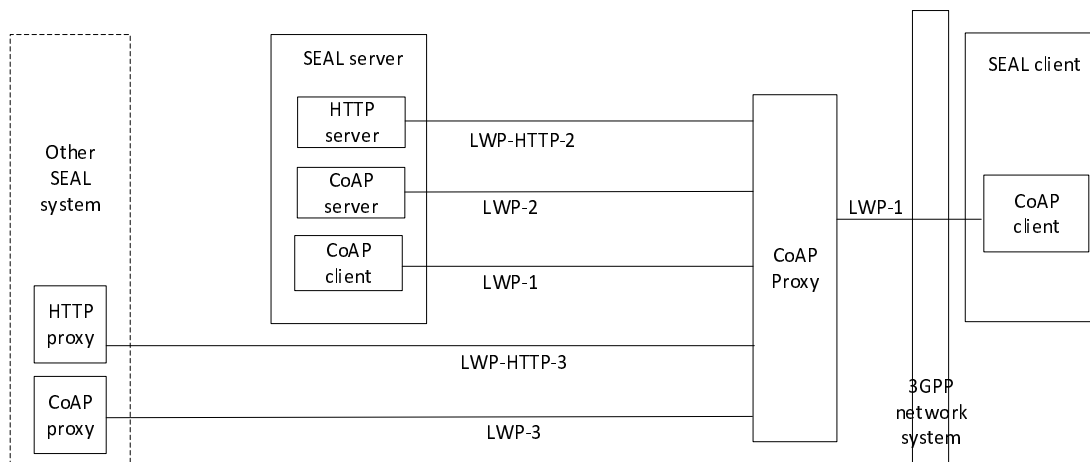
Figure C.2-1: Functional model for LWP signalling control plane when CoAP is used as LWP

When CoAP is used to realize the generic light-weight protocol defined in clause 6.2, then,

1. CoAP client is a realization of the LWP client

2. CoAP proxy is a realization of the LWP proxy, with the following clarifications:

    a. CoAP proxy shall be able to terminate a DTLS, TLS or secure WebSocket session on LWP-1 reference point;

    b. CoAP proxy shall be able to act as a cross-protocol CoAP-HTTP proxy to support LWP-HTTP-2 and LWP-HTTP-3 reference points;

3. CoAP server is a realization of the LWP server

4. CoAP supports the interactions over LWP-1, LWP-2 and LWP-3 reference points

5. The usage of CoAP by the SEAL service enablers shall follow the rules set out in clause 6.4.3.5.

Annex D (informative):
Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2019-01	SA6#28					TS skeleton	0.0.0
2019-01	SA6#28					Implementation of the following pCRs approved by SA6: S6-190283, S6-190284, S6-190285, S6-190301, S6-190210, S6-190286, S6-190272, S6-190287, S6-190295, S6-190215, S6-190296, S6-190297	0.1.0
2019-03	SA6#29					Implementation of the following pCRs approved by SA6: S6-190446, S6-190447, S6-190448, S6-190509, S6-190526, S6-190515, S6-190452, S6-190453, S6-190510, S6-190511, S6-190456, S6-190457, S6-190458	0.2.0
2019-03	SA#83	SP-190063				Presentation for information at SA#83	1.0.0
2019-04	SA6#30					Implementation of the following pCRs approved by SA6: S6-190661, S6-190663, S6-190848, S6-190746, S6-190747, S6-190748, S6-190749, S6-190750, S6-190872	1.1.0
2019-05	SA6#31					Implementation of the following pCRs approved by SA6: S6-191003, S6-191115, S6-191005, S6-191116, S6-191117, S6-191007, S6-191189, S6-191212, S6-191121, S6-191012, S6-191229, S6-191191, S6-191124, S6-191013, S6-191192, S6-191193	1.2.0
2019-05	SA#84	SP-190473				Presentation for Approval at SA#84	2.0.0
2019-06	SA#84	SP-190473				MCC Editorial update for publication after TSG SA approval (SA#84)	16.0.0
2019-09	SA#85	SP-190733	0001	2	F	Architecture requirements group management	16.1.0
2019-09	SA#85	SP-190733	0002	3	F	Group announcement and join	16.1.0
2019-09	SA#85	SP-190733	0003	6	F	Corrections to network resource management procedures	16.1.0
2019-09	SA#85	SP-190733	0004		F	N5 reference point description	16.1.0
2019-09	SA#85	SP-190733	0006	1	F	Change of service-based interface representation of the functional model for SEAL	16.1.0
2019-09	SA#85	SP-190733	0007		F	Remove EN on bearer type identification	16.1.0
2019-09	SA#85	SP-190733	0008		F	Remove EN on granularity of decision of NRM server	16.1.0
2019-12	SA#86	SP-191111	0009	1	F	Corrections to naming and other fixes	16.2.0
2019-12	SA#86	SP-191111	0010	2	F	Result element missing	16.2.0
2019-12	SA#86	SP-191111	0011	1	F	Anonymous requests	16.2.0
2019-12	SA#86	SP-191111	0012	1	F	No multicast resource management in 5GS	16.2.0
2019-12	SA#86	SP-191111	0013	2	F	Mention of SA3 responsibility in a published TS is not relevant.	16.2.0
2019-12	SA#86	SP-191111	0014	2	F	SEAL APIs corrections	16.2.0
2019-12	SA#86	SP-191111	0015	1	F	Update to location configuration procedure	16.2.0
2020-03	SA#87-E	SP-200114	0016		F	Complete SS_NetworkResourceAdaptation API	16.3.0
2020-03	SA#87-E	SP-200114	0017		F	Correct dynamic MBMS bearer establishment	16.3.0
2020-03	SA#87-E	SP-200114	0019		F	MBMS procedures alignment	16.3.0
2020-07	SA#88-E	SP-200338	0021	1	F	Align the Group Management API operation name with CT3	16.4.0
2020-07	SA#88-E	SP-200338	0022	2	F	Clarification and correction on media direction mode	16.4.0
2020-09	SA#89-E	SP-200841	0023	2	F	Correct location trigger configuration	16.5.0
2020-09	SA#89-E	SP-200841	0024	1	F	Clarifications on MBMS listening status uage	16.5.0
2020-09	SA#89-E	SP-200841	0025	2	F	Correct SEAL location API operations	16.5.0
2020-09	SA#89-E	SP-200841	0026	1	F	Correction to NRM unicast procedures	16.5.0
2020-12	SA#90-E	SP-200991	0029	1	F	Clarification on group join notification	16.6.0
2020-12	SA#90-E	SP-200991	0030	1	F	Resolution of ENs on security aspects	16.6.0
2020-12	SA#90-E	SP-200991	0033	1	F	Clarifications for T8 interface	16.6.0
2020-12	SA#90-E	SP-200991	0036	1	F	Correction to location notification to VAL server	16.6.0
2020-12	SA#90-E	SP-200998	0027	3	B	Tracking UE and obtaining dynamic UE information	17.0.0
2020-12	SA#90-E	SP-200998	0031	2	B	Support local MBMS	17.0.0
2020-12	SA#90-E	SP-200999	0032	2	B	Network slice adaptation for VAL applications	17.0.0
2020-12	SA#90-E	SP-200999	0034	1	F	Clarifications for T8 interface	17.0.0
2020-12	SA#90-E	SP-200999	0035	1	B	Temporary Groups formation	17.0.0
2021-04	SA#91-E	SP-210181	0038	3	B	Service identification in location management procedures	17.1.0
2021-04	SA#91-E	SP-210181	0039	2	B	Group management support for 5G-VN groups	17.1.0
2021-04	SA#91-E	SP-210181	0040	2	B	Add location criteria to group creation request	17.1.0
2021-04	SA#91-E	SP-210181	0042	1	B	Update to LMS server APIs	17.1.0
2021-04	SA#91-E	SP-210181	0044		B	Enhancement of information flows to add VAL service specific information	17.1.0
2021-04	SA#91-E	SP-210181	0045	1	B	Service identification in location management procedures	17.1.0
2021-06	SA#92-E	SP-210484	0037	3	B	Network Slice Capability Management functional model	17.2.0
2021-06	SA#92-E	SP-210484	0043	3	B	Off-network location management	17.2.0
2021-06	SA#92-E	SP-210485	0047	1	B	Location report timestamp support	17.2.0
2021-06	SA#92-E	SP-210484	0049	2	F	Update to GMS APIs	17.2.0
2021-06	SA#92-E	SP-210484	0051	2	B	SEAL support for CoAP	17.2.0
2021-06	SA#92-E	SP-210484	0052	1	B	Resolve EN for group management	17.2.0
2021-06	SA#92-E	SP-210484	0053	1	B	Coordinated QoS/resource management for network-assisted UE-to-UE communications	17.2.0
2021-06	SA#92-E	SP-210484	0054	1	B	Group list fetch procedure	17.2.0

2021-06	SA#92-E	SP-210484	0055	1	B	Group management enhancements	17.2.0
2021-06	SA#92-E	SP-210485	0056	4	B	SEAL Location Deviation Service	17.2.0
2021-06	SA#92-E	SP-210485	0057	1	B	SEAL Event Monitoring Service	17.2.0
2021-06	SA#92-E	SP-210484	0058	1	B	Requirements for Location management service	17.2.0
2021-06	SA#92-E	SP-210485	0059		B	Supplementary location information to verticals	17.2.0
2021-06	SA#92-E	SP-210485	0060	2	B	add VAL UE Information to configuration management procedure	17.2.0
2021-06	SA#92-E	SP-210483	0062	1	A	Complete resource reservation with PCC procedure	17.2.0
2021-06	SA#92-E	SP-210484	0063	1	F	QoS Monitoring support	17.2.0
2021-06	SA#92-E	SP-210484	0064	2	B	Unified support for TSC/TSN services	17.2.0
2021-06	SA#92-E	SP-210484	0065	2	B	SEAL enable 5G CN capabilities for SEAL groups	17.2.0
2021-06	SA#92-E	SP-210485	0066	2	B	SEAL Location Deviation Service Information flows and APIs	17.2.0
2021-06	SA#92-E	SP-210484	0067	1	B	API and information flow description for Temporary groups	17.2.0
2021-06	SA#92-E	SP-210483	0069	1	A	Fixing the descriptions of IEs in Information flows for location information	17.2.0
2021-09	na	na	0043	3	B	Editorial re-application of CR0043r3 "Off-network location management"	17.3.0
2021-09	SA#93-E	SP-210964	0075	2	C	Improved Event Monitoring Service	17.3.0
2021-09	SA#93-E	SP-210964	0076	2	B	Utilize NEF location service for SEAL LM	17.3.0
2021-09	SA#93-E	SP-210964	0078	5	B	Updates to Location based Group	17.3.0
2021-09	SA#93-E	SP-210964	0079	2	F	Support for TSC services procedures	17.3.0
2021-09	SA#93-E	SP-210964	0080	1	F	Support for TSN services procedures	17.3.0
2021-09	SA#93-E	SP-210964	0081	1	B	Unicast QoS monitoring data retrieval	17.3.0
2021-12	SA#94-E	SP-211525	0082	1	F	Corrections to network slice adaptation	17.4.0
2021-12	SA#94-E	SP-211521	0083	1	F	Group Deletion procedure	17.4.0
2021-12	SA#94-E	SP-211525	0084	1	F	Replace the NSCM with NSCE to align the terminologies	17.4.0
2021-12	SA#94-E	SP-211525	0086	1	F	Removal of PCP from TSC stream discovery	17.4.0
2021-12	SA#94-E	SP-211525	0087		F	Add missing location area monitoring API	17.4.0
2022-03	SA#95-E	SP-220101	0087		F	Clarify the VAL UE ID	17.5.0
2022-03	SA#95-E	SP-220101	0092	1	F	Correct QoS monitoring service	17.5.0
2022-03	SA#95-E	SP-220101	0093		F	Correct TSC stream availability discovery	17.5.0
2022-06	SA#96-E	SP-220473	0095	2	F	Minor corrections on network resource management for 5G TSC	17.6.0
2022-06	SA#96-E	SP-220473	0099	1	F	Minor essential corrections to TS 23.434	17.6.0
2022-06	SA#96-E	SP-220473	0102	1	F	QoS monitoring clarification	17.6.0

History

Document history		
V17.5.0	May 2022	Publication
V17.6.0	July 2022	Publication