ETSI TS 123 434 V18.11.0 (2025-04)

5G;
Service Enabler Architecture Layer for Verticals (SEAL);
Functional architecture and information flows
(3GPP TS 23.434 version 18.11.0 Release 18)

Reference
RTS/TSGS-0623434vib0

Keywords
5G

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

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 EPS or 5GS architecture defined in 3GPP TS 23.401 [9], 3GPP TS 23.246 [17], 3GPP TS 23.468 [16], 3GPP TS 23.501 [10], and 3GPP TS 23.247 [39]. 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, network resource management, notification management, network slice capability enablement, data delivery and application data analytics enablement.

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".

[39] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services; Stage 2".

[40] 3GPP TS 23.435: "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service".

[41] 3GPP TS 28.531: "Management and orchestration; Provisioning".

[42] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[43] 3GPP TS 28.530: "Management and orchestration; Concepts, use cases and requirements".

[44] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[45] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[46] 3GPP TS 28.554: "Management and orchestration; 5G end to end Key Performance Indicators (KPI)".

[47] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics".

[48] 3GPP TS 23.433: "Service Enabler Architecture Layer for Verticals (SEAL); Data Delivery enabler for vertical applications".

[49] 3GPP TS 23.436: "Procedures for Application Data Analytics Enablement Service".

[50] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2"

[51] 3GPP TS 29.572: "5G System; Location Management Services; Stage 3"

[52] 3GPP TS 23.256 "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".

[53] 3GPP TS 37.355: "LTE Positioning Protocol (LPP)".

[54] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[55] Void

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.

MBS session announcement: Mechanism to provide the necessary information to the NRM client to enable the reception of the VAL service data via the MBS session.

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

Vertical domain

For the purpose of the present document, the following terms given in 3GPP TS 23.247 [39] apply:

MBS session
MBS service area
MB-SMF service area

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
SEAL-UU	Service Enabler Architecture Layer for Verticals, Universal UE-network interface
TSC	Time Sensitive Communication
TSN	Time Sensitive Networking
VAL	Vertical Application Layer
NOP	Network Operator
NSaaS	Network Slice as a Service

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 On-network functional model 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.

4.3.3 Off-network functional model requirements

[AR-4.3.3-a] The SEAL shall support on-demand location reporting and event-triggered location reporting within PC5 communication.

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.

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.

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

[AR-4.8.2-g] The SEAL shall enable support for MBS session (multicast or broadcast type) establishment and modification to support service KPIs for VAL communications.

[AR-4.8.2-h] The SEAL shall support announcement of MBS session (multicast or broadcast type) to the UEs.

[AR-4.8.2-i] The SEAL shall support switching of between unicast PDU session and MBS session (multicast or broadcast type).

[AR-4.8.2-j] The SEAL shall support MBS session (multicast or broadcast type) 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.

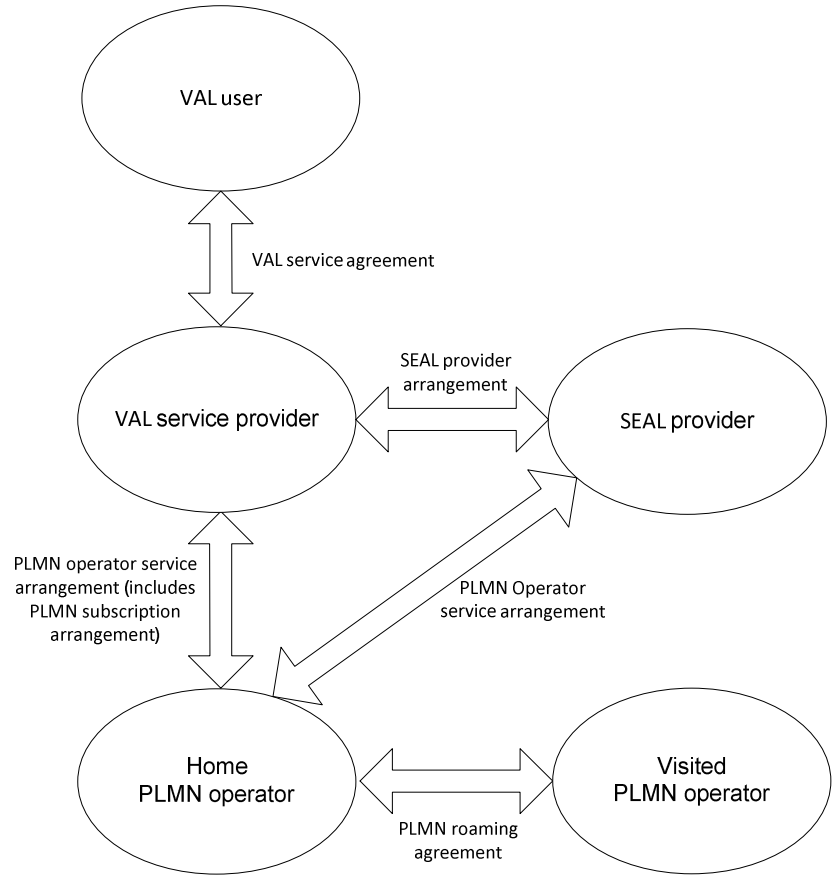

Figure 5-1: Business relationships for VAL services

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;
- Network resource management;
- Data delivery;
- Notification management;
- Network slice capability enablement; and
- Application data analytics enablement.

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.

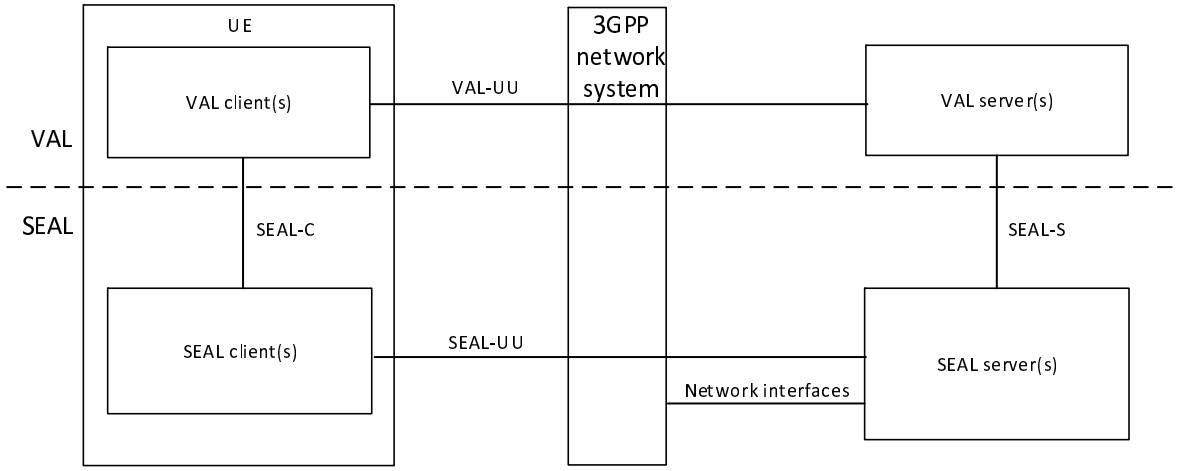

Figure 6.2-1: Generic on-network functional model

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.

NOTE 4: Non-3GPP access used by the UE is out of scope of the present document.

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.

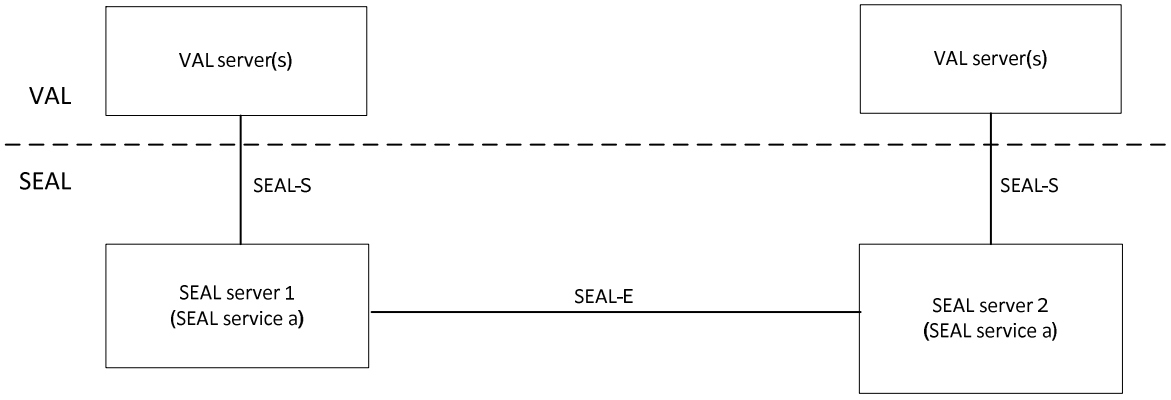

Figure 6.2-2: Interconnection between SEAL servers

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.

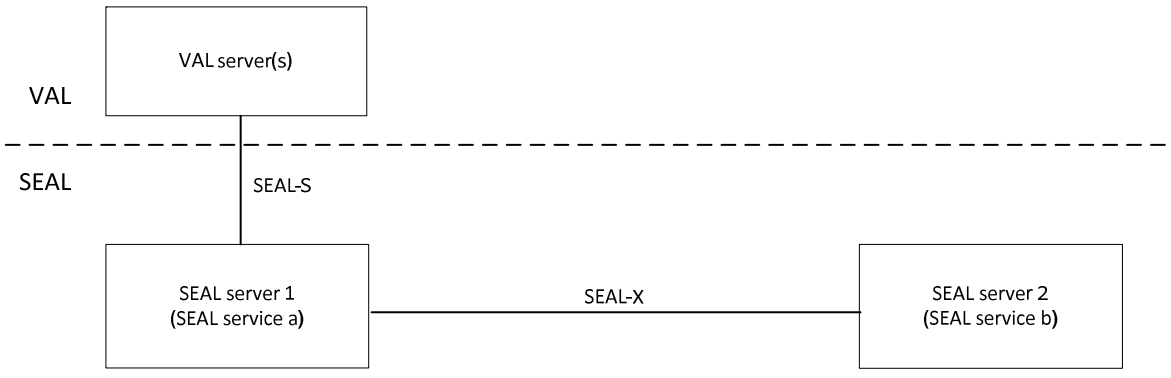

Figure 6.2-3: Inter-service communication between SEAL servers

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.

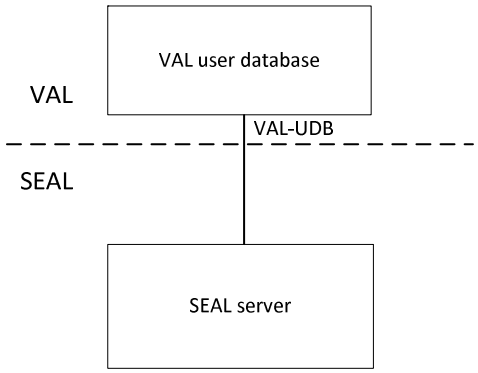

Figure 6.2-4: Communication between SEAL server and VAL user database

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.

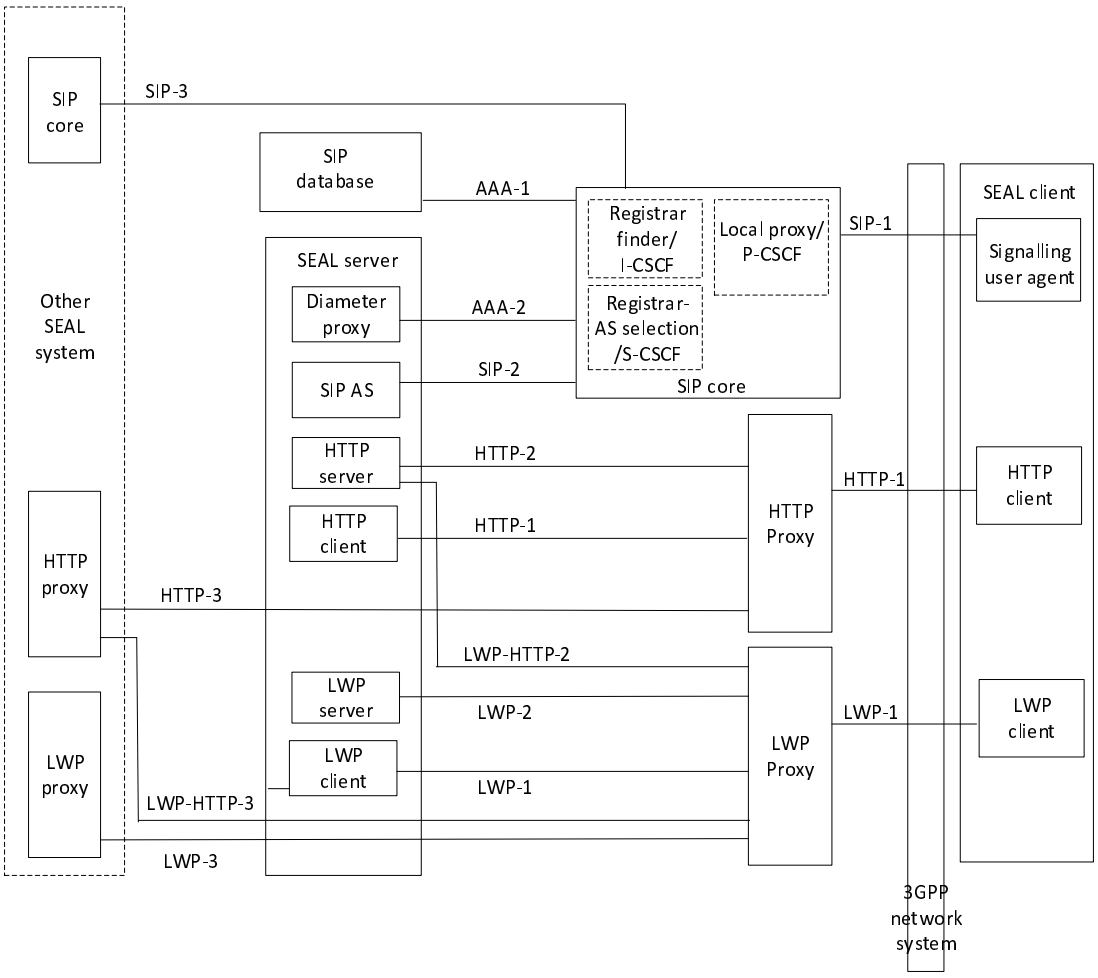

Figure 6.2-5: Functional model for signalling control plane

NOTE 5: 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.

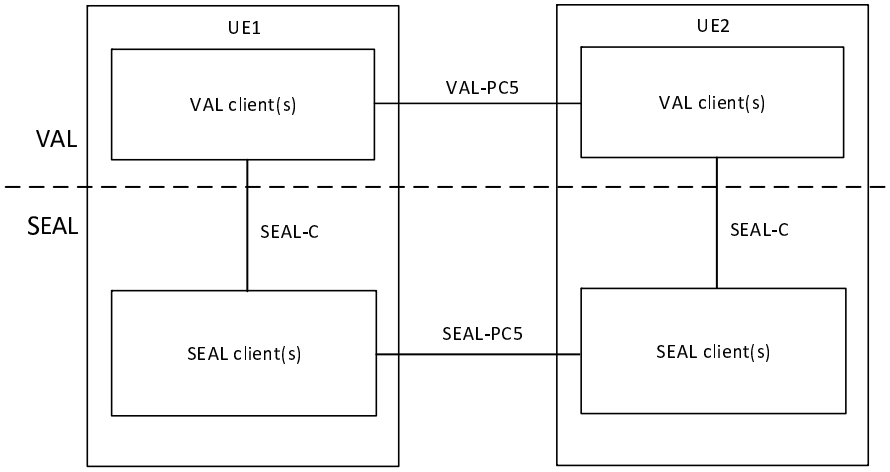

Figure 6.3-1: Generic off-network functional model

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.

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.

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.

NOTE: The functions enabled over SEAL-E reference point are specified in each SEAL service.

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.

6.5.2.9.4 Reference point SEAL-X3 (between the group management server and the configuration management server)

The SEAL-X3 reference point enables the group management server to interact with the configuration management server.

The SEAL-X3 reference point supports:

- the group management server to retrieve VAL service data from the configuration 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;
- obtaining the user profile from the specific VAL user database for further configuration in the UE;
- updating the user profile data in the specific VAL user database; and
- deleting the user profile data from the specific VAL user database.

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.

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).

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].

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.

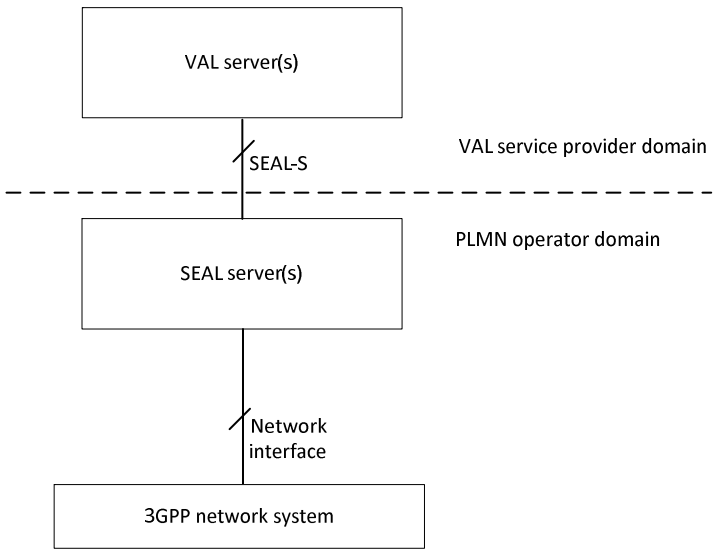

Figure 8.2.1-1: SEAL server(s) deployed in a single PLMN operator domain

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.

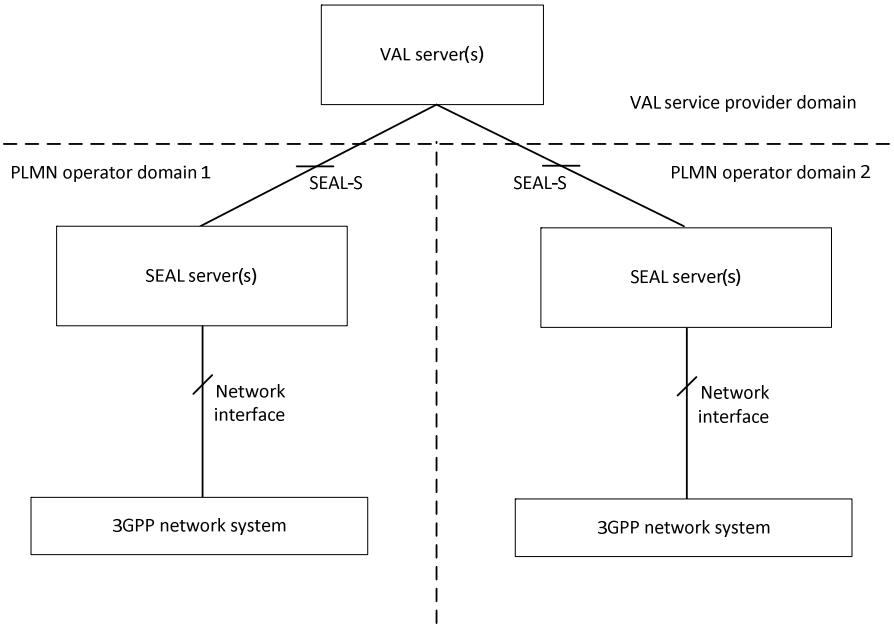

Figure 8.2.1-2: SEAL server(s) deployed in multiple PLMN operator domain without interconnection between SEAL servers

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.

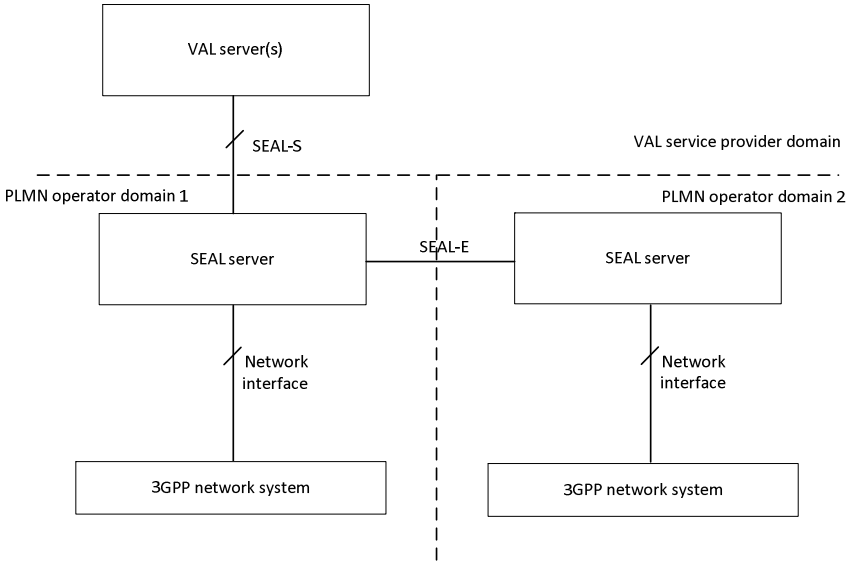

Figure 8.2.1-3: SEAL server(s) deployed in multiple PLMN operator domain with interconnection between SEAL servers

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.

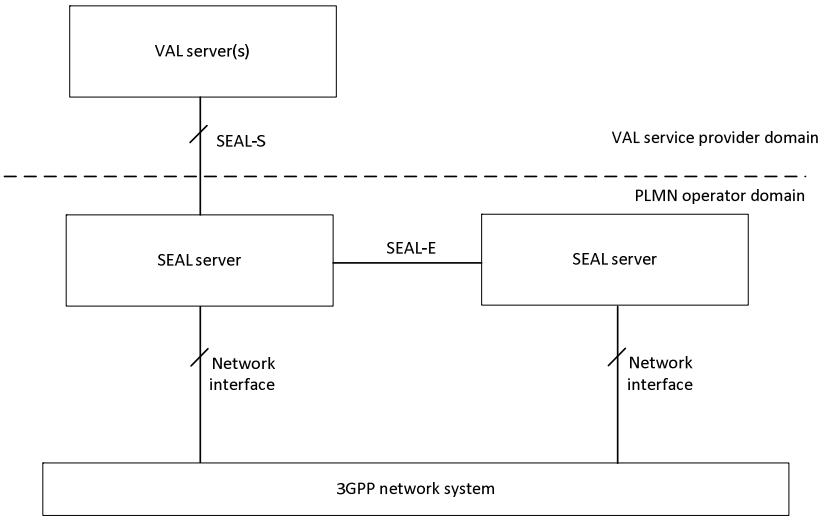

Figure 8.2.1-4: SEAL server(s) deployed in a single PLMN operator domain with interconnection between SEAL servers

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.

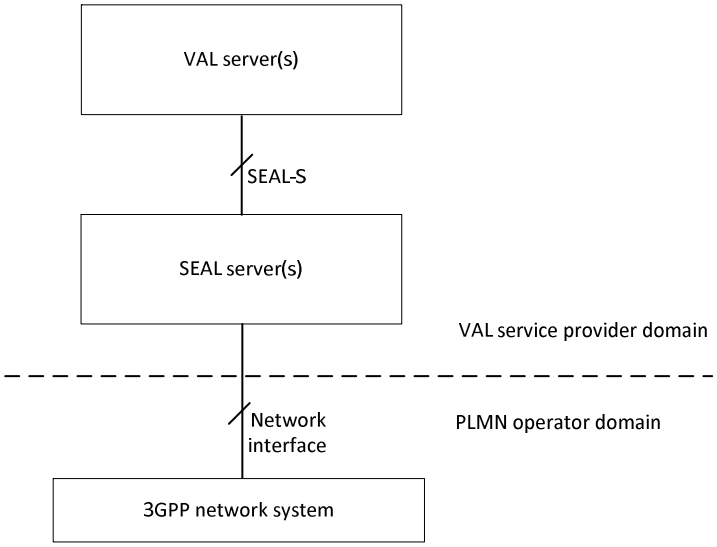

Figure 8.2.2-1: Deployment of SEAL server(s) with connections to 3GPP network system in a single PLMN operator domain

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

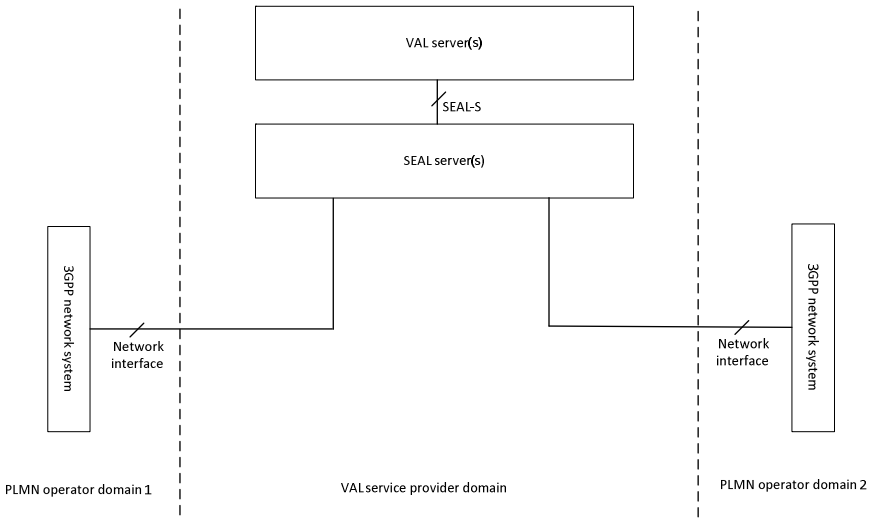

Figure 8.2.2-2: Deployment of SEAL server(s) with connections to 3GPP network system in multiple PLMN operator domains

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.

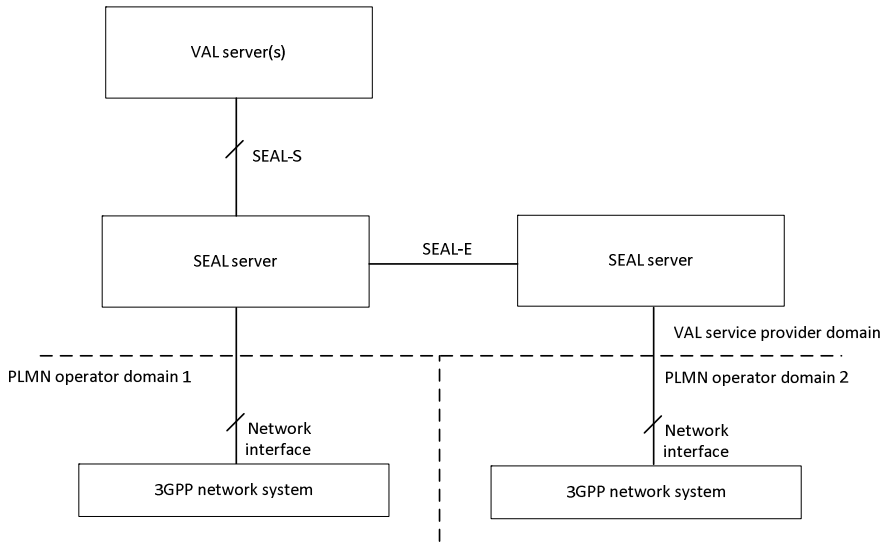

Figure 8.2.2-3: Distributed deployment of SEAL servers in VAL service provider domain

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.

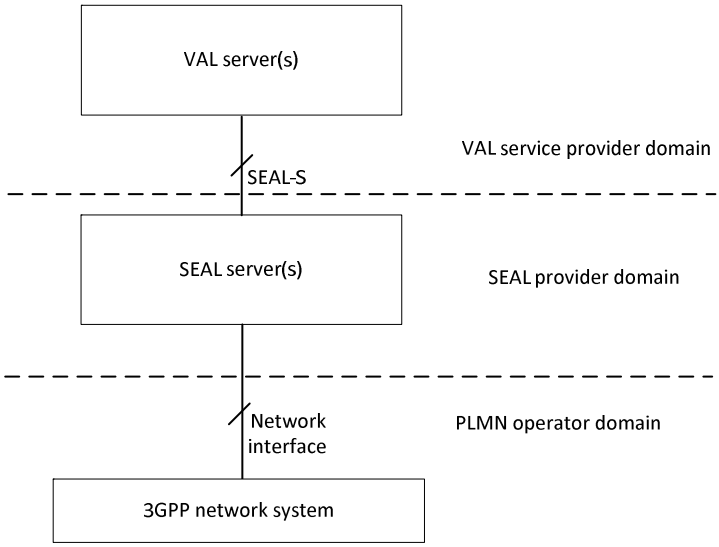

Figure 8.2.3-1: Deployment of SEAL server(s) outside of VAL service domain and PLMN operator domain

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.

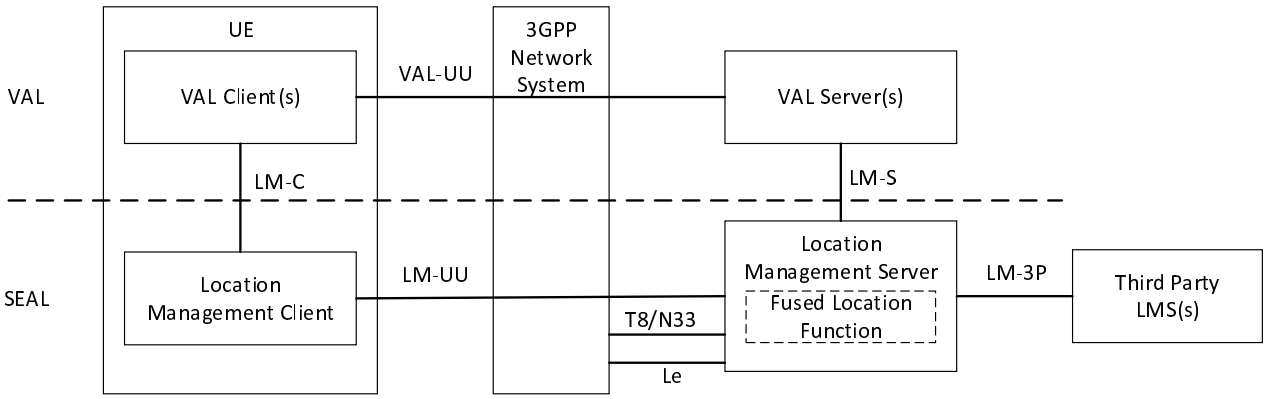

Figure 9.2.2-1: On-network functional model for location management

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 VAL client communicates with the VAL server over the VAL-UU reference point which is outside the scope of this document.

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]. The location management server may obtain location information from the GMLC via Le reference point defined in clause 4.4.1 of 3GPP TS 23.273 [50]. The location management server may optionally obtains location information from the 3rd party location server via LM-3P reference point.

When the fused location function is present, the location management server, may use the location information from multiple sources to determine a more accurate UE location. The fused location function may select one or more location sources and location methods based on the requested location QoS which obtained from the location management server.

NOTE 1: Location information from LCS of 4G system is not exposed by SCEF.

NOTE 2: Non-3GPP access used by the UE is out of scope of the present document.

Figure 9.2.2-2 exhibits the service-based interfaces for providing and consuming location management services. The location management server could provide service to VAL server and location management client through interface Slm.

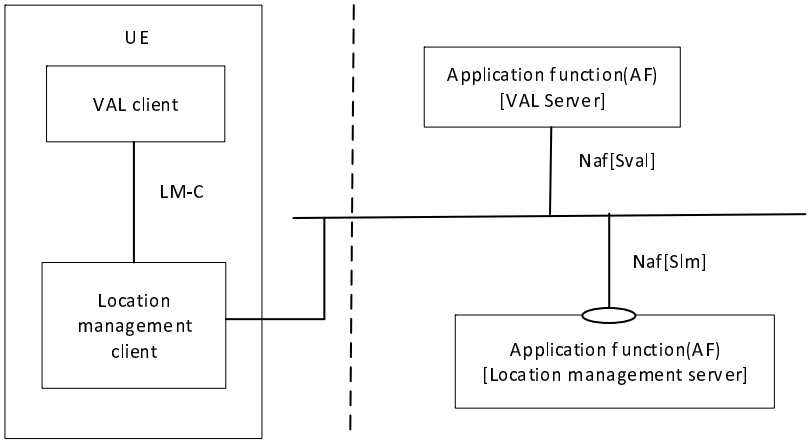

Figure 9.2.2-2: Architecture for location management – Service based representation

Figure 9.2.2-3 illustrates the service-based representation for utilization of the 5GS network services based on the 5GS SBA specified in 3GPP TS 23.501 [10].

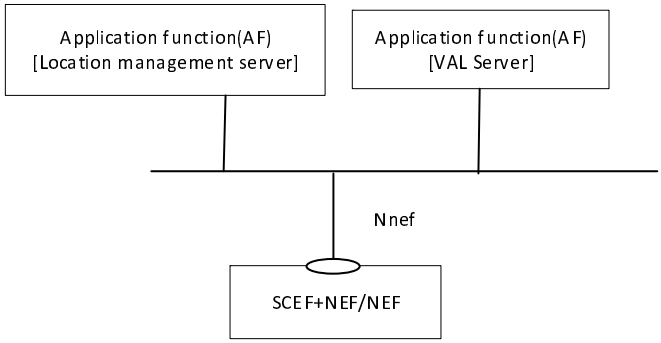

Figure 9.2.2-3: Architecture for location management utilizing the 5GS network services based on the 5GS SBA – Service based representation

Figure 9.2.2-4 illustrates the service-based representation for utilization of the Core Network (5GC, EPC) northbound APIs via CAPIF.

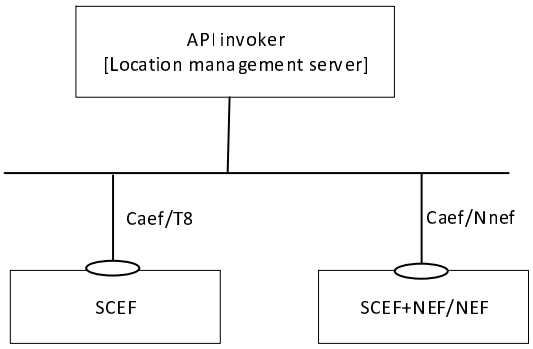

Figure 9.2.2-4: Utilization of Core Network Northbound APIs via CAPIF – service based representation

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

9.2.3 Off-network functional model description

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

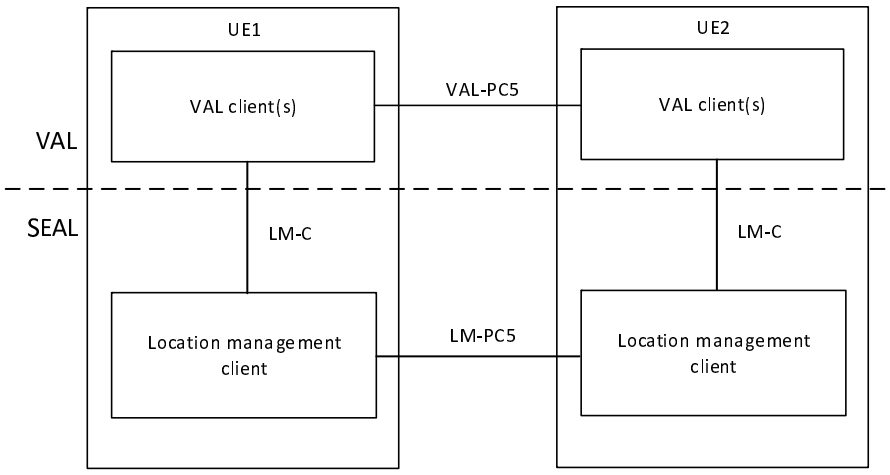

Figure 9.2.3-1: Off-network functional model for location management

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 and may provide UE-based positioning and location-related information. 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, N33, or Le reference points. The location management service may optionally obtain location information from 3rd party location servers via LM-3P reference point. The LM-3P reference point is out of scope of this specification.

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. The location management server, with the fused location function, may combine/aggregate location information from multiple sources to provide a more accurate UE location.

NOTE: The accuracy of location information acquired from 4G system via T8 reference point is not higher than 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.

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.

9.2.5.8 Le

The reference point Le supports the interactions between the location management server and the GMLC and is specified in 3GPP TS 23.273 [50].

9.2.5.9 LM-3P

The reference point LM-3P is used for location retrieval of the target UE from a third-party location server.

NOTE: Further definition of LM-3P is out of scope of this specification.

9.2.5.10 N33

The reference point N33 supports the interactions between the location management server and the NEF and is specified in 3GPP TS 23.501 [10] and 3GPP TS 23.502 [11]. The functions related to location management of N33 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.

NOTE: The security and privacy aspects related to location management (e.g. VAL server obtains UE’s location information or LM-Uu and LM-S in relation to the VAL service ID) are out of scope of this specifiction.

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 1)	Identifies what location information is requested
Requested location access type (see NOTE 2)	O (see NOTE 1)	Identifies the location access type for which the location information is requested, e.g. as described in TS 23.273 [50] and TS 29.572 [51].
Requested positioning method	O (see NOTE 1)	Identifies the positioning method for which the location information is requested, e.g. as described in TS 23.273 [50] and TS 29.572 [51].
Triggering criteria	O (see NOTE 1)	Identifies when the location management client will send the location report as specified in table 9.3.2.4-2. The triggering may be e.g., SAI changes, ECGI changes, RAT changes.
Minimum time between consecutive reports	O (see NOTE 1)	Defaults to 0 if absent otherwise indicates the time interval between consecutive reports
NOTE 1: If none of the information element is present, this represents a cancellation for location reporting. NOTE 2: The non-3GPP access as defined in 23.273[50] and TS 29.572 [51] is out of scope of the present specification.		

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. The triggering event may be e.g., SAI changes, ECGI changes, RAT changes.
Location Information	M	Location information. For LM-UU reference point, it may include UE location information via non-3GPP positioning technologies (e.g. GNSS, Sensor, TBS, WLAN, Bluetooth) as described in 3GPP TS 37.355 [53].
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/or 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.
Requested location information	O	Identifies what location information is requested
Requested location access type (NOTE 4)	O (NOTE 1)	Identifies the location access type for which the location information is requested, e.g. as described in TS 23.273[50] and TS 29.572[51].
Requested positioning method	O (NOTE 1)	Identifies the positioning method for which the location information is requested, e.g. as described in TS 23.273[50] and TS 29.572[51].
Location QoS	O (NOTE 3)	Definition of the location Quality of Service for which the location information is requested (see NOTE 2).
NOTE 1: This e element is only applicable for request sent from the LM server to the LM client. NOTE 2: The definition of location QoS has been defined in clause 4.1b of TS 23.273 [50] and the clause 6.1.6.2.13 of TS 29.572 [51]. NOTE 3: The element is only applicable for the information flow from the VAL server to the location management server. NOTE 4: The non-3GPP access as defined in TS 23.273[50] and TS 29.572[51] is out of scope of the present specification.		

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
Requestor Identity	M (see NOTE 1)	Identity of the requesting authorized VAL user or VAL UE or VAL server
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. This information element may be represented as VAL service area ID(s) when this information flow from VAL server to the location management server.
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 as specified in table 9.3.2.4-2.
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/VAL server and the requested VAL user/UE should belong to the same VAL service. NOTE 2: At least one of these rows shall be present.		

Table 9.3.2.4-2: Location reporting Triggering criteria

Information element	Status	Description
Frequency of reporting	O	It indicates the requested frequency of reporting. The reporting frequency may be periodic or event-triggered.
Reporting periodicity	O	If the Frequency of reporting is periodic, the reporting periodicity shall be provided.
Location change condition	O (see NOTE)	It indicates the location change condition when the reporting shall occur, e.g., VAL user or VAL UE changes a cell, NodeB, TA, RA, WLAN access network, civic address, GPS coordinates, SAI, ECGI, RAT, VAL service area. If the Frequency of reporting is event-triggered, this IE shall be provided.
Inside or outside indication	O (see NOTE)	It indicates the condition when the reporting shall occur, i.e., the VAL user or VAL UE is inside or outside the locations represented by the VAL service area ID(s).
Reporting schedule	O	It indicates the requested reporting schedule, e.g., days of the week and/or time period for the location reporting.
NOTE: Triggering criteria based on the VAL service area represented by the VAL service area ID(s) may be provided when this information flow is from the VAL server to the location management server.		

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 or for updating an existing location information subscription.

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 (see NOTE 3)
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
Supplementary location information indication	O	Indicates that supplementary location information is required.
Location QoS	O (NOTE 2).	Definition of the location Quality of Service for which the location information is requested (see NOTE 1).
NOTE 1: The definition of location QoS has been defined in clause 4.1b of TS 23.273 [50] and the clause 6.1.6.2.13 of TS 29.572 [51]. NOTE 2: The element is only applicable for the information flow from the VAL server to the location management server. NOTE 3: This information element shall not be updated via location information subscription update procedure in clause 9.3.2.7a.		

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 or location information subscription update 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 (see NOTE 2)	O	Identity of the VAL user or VAL UE subscribed to location of another VAL user or VAL UE (see NOTE 1)
Subscription ID (see NOTE 2)	O	Subscription identity related to VAL server subscription with Location management server for location information notification.
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 1: This is only used for location management server sends location information notification to the VAL user or VAL UE who has subscribed the location. NOTE 2: Either Identity or Subscription ID shall be included.		

9.3.2.7a Location information subscription update procedure

Figure 9.3.2.7a-1 illustrates the high level procedure for allowing a VAL server update an existing subscription about location information at the location management server.

Pre-conditions:

- the VAL server has an active location information subscription at the location management server.

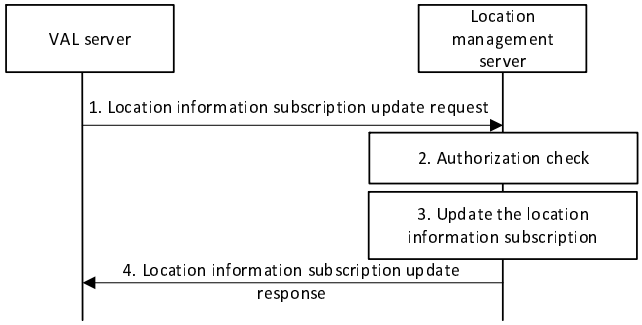

Figure 9.3.2.7a-1: Location information subscription update procedure

1. When the VAL server decides to update an active location information subscription, it sends a location information subscription update request to the location management server including the information specified in table 9.3.2.5-1.

2. The location management server shall check if the VAL server is authorized to update the subscription.

3. If the VAL server is authorized to update the subscription, the location management server updates the location information subscription.

4. The location management server sends a location information subscription update response to the VAL server including the information as specified in table 9.3.2.6-1.

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 or from the location management server to the location management client.

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 or VAL server
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 cancelled.

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 (e.g. geographic area or VAL service area ID).
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 VAL UE or VAL user.
>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) or for updating an existing monitor location subscription.

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 (see NOTE).
Area of Interest	M	Geographic area location information where the VAL server wishes to monitor the VAL UE's location adherence. This could be geographical co-ordinates or VAL service area identified by the VAL service area ID.
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.
NOTE: This information element shall not be updated via monitor location subscription update procedure in clause 9.3.2.12a.		

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 or monitor location subscription update response.

Table 9.3.2.12-1: Monitor Location Subscription Response

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

9.3.2.12a Monitor location subscription update procedure

Figure 9.3.2.12a -1 illustrates the high level procedure for allowing a VAL server update an existing monitor location subscription at the location management server.

Pre-conditions:

- the VAL server has an active monitor location subscription at the location management server.

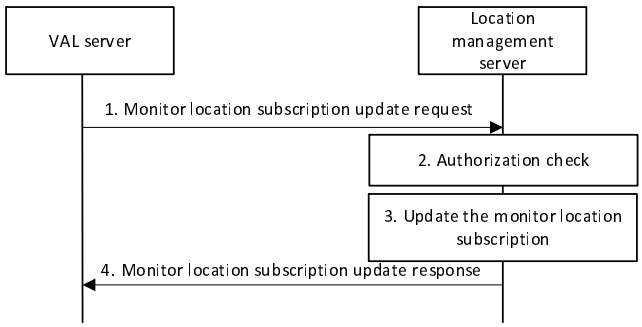

Figure 9.3.2.12a -1: Monitor location subscription update procedure

1. When the VAL server decides to update an active monitor location subscription, it sends a monitor location subscription update request to the location management server including the information specified in table 9.3.2.11.

2. The location management server shall check if the VAL server is authorized to update the subscription.

3. If the VAL server is authorized to update the subscription, the location management server updates the monitor location subscription.

4. The location management server sends a monitor location subscription update response to the VAL server including the information as specified in table 9.3.2.12.

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, or when the LM server determined area of interest result based on LM client location and the core network reported area of interest result 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.

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 VAL service area identified by the VAL service area ID 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)
Notification Target URI	M	Target URI where the VAL server wishes to receive the notifications about location area monitoring.

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 VAL service area ID 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)
Notification Target URI	O	Target URI where the VAL server wishes to receive the notifications about location area monitoring.

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.

Table 9.3.2.19-1: Location information 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
Request status	M	It indicates the request result

9.3.2.21 VAL service area configuration request

Table 9.3.2.21-1 describes the information flow from the VAL server to the location management server for VAL service area configuration request.

Table 9.3.2.21-1: VAL service area configuration request

Information element	Status	Description
Identity	M	Identity of the requesting VAL server
List of VAL service area information	M	List of one or more VAL service area identifiers.
> VAL service area ID	M	The VAL service area identifier.
> Geographical location list	M	List of one more geographical locations (e.g., co-ordinates) corresponding to the VAL service area ID

9.3.2.22 VAL service area configuration response

Table 9.3.2.22-1 describes the information flow from the location management server to the VAL server for VAL service area configuration response.

Table 9.3.2.22-1: VAL service area configuration response

Information element	Status	Description
VAL Service area configuration status	M	It indicates the result of VAL service area configuration request.
List of VAL service area IDs	O	List of VAL service area IDs
NOTE: This IE shall be present only if the configuration status is set to success.		

9.3.2.23 Location service registration request

Table 9.3.2.23-1 describes the information flow from the location management client to the location management server for registration of the location service.

Table 9.3.2.23-1: Location service registration 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 service is registered.
Location capability	O	The information of location capability of VAL UE for which the location service is registered.
> Location access type (NOTE 2)	O (NOTE 1)	Identifies the available location access type of the VAL UE. E.g. as described in TS 23.273[50] and TS 29.572[51].
>Positioning method	O (NOTE 1)	Identifies the available positioning methods of the VAL UE. E.g. as described in TS 23.273[50] and TS 29.572[51].
NOTE 1: At least one of these rows shall be present. NOTE 2: The non-3GPP access as defined in TS 23.273[50] and TS 29.572 [51] is out of scope of the present specification.		

9.3.2.24 Location service registration response

Table 9.3.2.24-1 describes the information flow from the location management server to the location management client for the location service registration response.

Table 9.3.2.24-1: Location service registration response

Information element	Status	Description
Registration status	M	It indicated the registration result.

9.3.2.25 Location reporting configuration cancel response

Table 9.3.2.25-1 describes the location reporting configuration cancel response information flow from the location management server to the location management client or from the location management client to the location management server.

Table 9.3.2.25-1: Location reporting configuration cancel response

Information element	Status	Description
Cancel status	M	It indicates the cancelled result.

9.3.2.26 VAL service area obtain request

Table 9.3.2.26-1 describes the information flow from a VAL server to a location management server for obtain VAL service area identifiers at the LM server.

Table 9.3.2.26-1: Obtain VAL service area request

Information element	Status	Description
Identity	M	Indicates the VAL server identity.
VAL service area IDs	M	Indicates the list of the requested VAL service area identifiers.

9.3.2.27 VAL service area obtain response

Table 9.3.2.27-1 describes the information flow from a location management server to the VAL server for obtain VAL service area identifiers at the LM server.

Table 9.3.2.27-1: Obtain VAL service area response

Information element	Status	Description
Result	M	Indicates the success or failure for the operation.
List of VAL service area information	O (see NOTE)	List of one or more VAL service area identifiers.
> VAL service area ID	M	The VAL service area identifier.
> Geographical locations list	M	List of one more geographical locations (e.g., co-ordinates) corresponding to the VAL service area ID.
NOTE: This information element shall be present only if the obtain VAL service area identifier(s) is successful.		

9.3.2.28 VAL service area update request

Table 9.3.2.28-1 describes the information flow from a VAL server to a location management for update VAL service area identifiers at the LM server.

Table 9.3.2.28-1: Update VAL service area request

Information element	Status	Description
Identity	M	Indicates the VAL server identity.
List of VAL service area information	M	List of one or more VAL service area identifiers that shall be updated.
> VAL service area ID	M	Indicates the VAL service area identifier.
> Geographical locations	M	Indicates the list of the updated geographical locations (e.g., the geographical coordinates) corresponding to the VAL service area ID.

9.3.2.29 VAL service area update response

Table 9.3.2.29-1 describes the information flow from a location management server to the VAL server for update VAL service area identifiers at the LM server.

Table 9.3.2.29-1: Update VAL service area response

Information element	Status	Description
Result	M	Indicates the success or failure for the operation.
VAL service area IDs	O (see NOTE)	Indicates the list of the updated VAL service area identifiers.
NOTE: This information element shall be present only if the update VAL service area identifier(s) is successful.		

9.3.2.30 VAL service area delete request

Table 9.3.2.30-1 describes the information flow from a VAL server to a location management for delete VAL service area identifiers at the LM server.

Table 9.3.2.30-1: Update VAL service area request

Information element	Status	Description
Identity	M	Indicates the VAL server identity.
List of VAL service IDs	M	List of one or more VAL service area identifiers that shall be deleted.

9.3.2.31 VAL service area delete response

Table 9.3.2.31-1 describes the information flow from a location management server to the VAL server for delete VAL service area identifiers at the LM server.

Table 9.3.2.31-1: Update VAL service area response

Information element	Status	Description
Result	M	Indicates the success or failure for the operation.
VAL service area IDs	O (see NOTE)	Indicates the list of the deleted VAL service area identifiers.
NOTE: This information element shall be present only if the delete VAL service area identifier(s) is successful.		

9.3.2.32 Location information unsubscribe request

Table 9.3.2.32-1 describes the information flow from the VAL server or location management client to the location management server for location information unsubscribe request.

Table 9.3.2.32-1: Location information unsubscribe request

Information element	Status	Description
Requestor ID	M	Identity of the VAL server or VAL UE's requesting ID.

9.3.2.33 Location information unsubscribe response

Table 9.3.2.33-1 describes the information flow from the location management server to the VAL server or location management client for location information unsubscribe response.

Table 9.3.2.33-1: Location information unsubscribe response

Information element	Status	Description
Request status	M	It indicates the unsubscribe request result

9.3.2.34 Monitor location unsubscribe request

Table 9.3.2.34-1 describes the information flow from the VAL server to the LM server for monitor location unsubscribe request.

Table 9.3.2.34-1: Monitor location unsubscribe request

Information element	Status	Description
Requestor ID	M	Identity of the VAL server's requesting ID.

9.3.2.35 Monitor location unsubscribe response

Table 9.3.2.35-1 describes the information flow from LM server to the VAL server for monitor location unsubscribe response.

Table 9.3.2.35-1: Monitor location unsubscribe response

Information element	Status	Description
Request status	M	It indicates the unsubscribe request result

9.3.2.36 Location service registration update request

Table 9.3.2.36-1 describes the information flow from the location management client to the location management server for update the registered location service.

Table 9.3.2.36-1: Location service registration update 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 service is updated.
Location capability	O	The information of location capability of VAL UE for which the location service is updated.
>Location access type (NOTE 2)	O (NOTE 1)	Identifies the updated location access type of the VAL UE. E.g. as described in TS 23.273[50] and TS 29.572[51].
>Positioning method	O (NOTE 1)	Identifies the updated positioning methods of the VAL UE. E.g. as described in TS 23.273[50] and TS 29.572[51].
NOTE 1: At least one of these rows shall be present. NOTE 2: The non-3GPP access as defined in TS 23.273[50] and TS 29.572[51] is out of scope of the present specification.		

9.3.2.37 Location service registration update response

Table 9.3.2.37-1 describes the information flow from the location management server to the location management client for the location service registration update response.

Table 9.3.2.37-1: Location service registration update response

Information element	Status	Description
Update status	M	It indicated the update result.

9.3.2.38 Location service deregistration request

Table 9.3.2.38-1 describes the information flow from the location management client to the location management server for deregistration of the location service.

Table 9.3.2.38-1: Location service deregistration request

Information element	Status	Description
Identity	M	Identity of the VAL user or the VAL UE.

9.3.2.39 Location service deregistration response

Table 9.3.2.39-1 describes the information flow from the location management server to the location management client for the location service deregistration response.

Table 9.3.2.39-1: Location service deregistration response

Information element	Status	Description
Deregistration status	M	It indicated the deregistration result.

9.3.2.40 Location reporting configuration update request

Table 9.3.2.40-1 describes the information flow from the location management server to the location management client for the location reporting configuration update when LM server needs to deliver the new or update location reporting configuration to LM client if the LM server received the new requests/parameters from other entities (e.g. the VAL

server or other LM client). This information flow may be sent individually addressed or group addressed on unicast or multicast.

Table 9.3.2.40-1: Location reporting configuration update request

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 1)	Identifies what location information is requested
Requested location access type (see NOTE 2)	O (see NOTE 1)	Identifies the location access type for which the location information is requested, e.g. as described in TS 23.273 [50] and TS 29.572 [51].
Requested positioning method	O (see NOTE 1)	Identifies the positioning method for which the location information is requested, e.g. as described in TS 23.273 [50] and TS 29.572 [51].
Triggering criteria	O (see NOTE 1)	Identifies when the location management client will send the location report as specified in table 9.3.2.4-2. The triggering may be e.g., SAI changes, ECGI changes, RAT changes.
Minimum time between consecutive reports	O (see NOTE 1)	Defaults to 0 if absent otherwise indicates the time interval between consecutive reports
NOTE 1: If none of the information element is present, this represents a cancellation for location reporting. NOTE 2: The non-3GPP access as defined in TS 23.273[50] and TS 29.572[51] is out of scope of the present specification.		

9.3.2.41 Location reporting configuration update response

Table 9.3.2.41-1 describes the information flow from the location management client to the location management server for the location reporting configuration update response. This information flow may be sent individually addressed or group addressed on unicast or multicast.

Table 9.3.2.41-1: Location reporting configuration update response

Information element	Status	Description
Update status	M	It indicates the update result.

9.3.2.42 VAL service area subscription request

Table 9.3.2.42-1 describes the information flow from a SEAL server to a location management server to subscribe VAL service area identifier update events or update an existing subscription at the LM server.

Table 9.3.2.42-1: VAL service area subscription request

Information element	Status	Description
Identity	M	Indicates the SEAL server identity (see NOTE).
List of the subscribed events	M	Indicates the list of the requested events.
> Event type	M	Indicates the subscribed event (e.g., update/deletion of the VAL service area ID)
> VAL service area IDs	O	Indicates the list of the VAL service area identifiers. This information element shall be provided when the requested event type is update or delete VAL service area ID.
Notification Target URI	M	Target URI where the VAL server wishes to receive the notifications about VAL service area update events.
Subscription duration	O	It indicates the subscription duration.
NOTE: This information element shall not be updated via the update VAL service area subscription request.		

9.3.2.43 VAL service area subscription response

Table 9.3.2.43-1 describes the information flow from a location management server to a SEAL server for VAL service area subscription response or update VAL service area subscription response.

Table 9.3.2.43-1: VAL service area subscription response

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

9.3.2.44 VAL service area notification

Table 9.3.2.44-1 describes the information flow for VAL service area notification from a location management server to a SEAL server.

Table 9.3.2.44-1: VAL service area notification

Information element	Status	Description
List of events	M	Indicates the list of the occurred events.
> Event type	M	Indicates the subscribed event (e.g., update/deletion of the VAL service area ID).
> List of VAL service area information	M	List of one or more VAL service area identifiers.
>> VAL service area ID	M	The VAL service area identifier.
>> Geographical locations list	M	List of one more geographical locations (e.g., co-ordinates) corresponding to the VAL service area ID.

9.3.2.45 VAL service area unsubscribe request

Table 9.3.2.45-1 describes the information flow from a SEAL server to a location management server for VAL service area unsubscribe request.

Table 9.3.2.45-1: VAL service area unsubscribe request

Information element	Status	Description
Identity	M	Indicates the SEAL server identity.

9.3.2.46 VAL service area unsubscribe response

Table 9.3.2.46-1 describes the information flow from the location management server to the SEAL server for VAL service area unsubscribe response.

Table 9.3.2.46-1: Location information unsubscribe response

Information element	Status	Description
Request status	M	It indicates the unsubscribe 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.

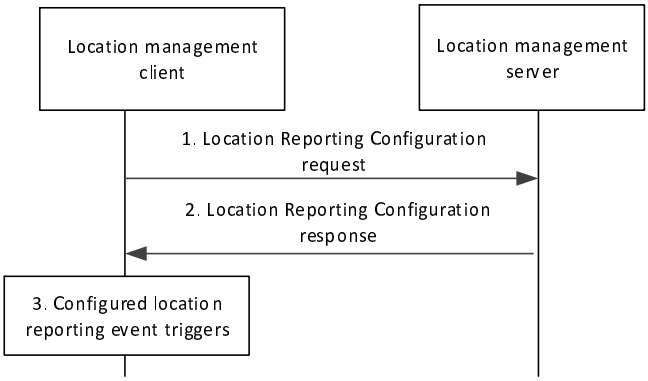

Figure 9.3.3.2-1: Fetching location reporting configuration procedure

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, access RAT 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.

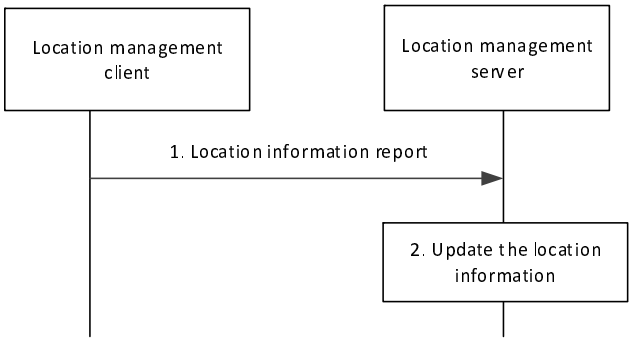

Figure 9.3.3.3-1: Location reporting procedure

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.

9.3.3.4 Update Location reporting configuration

The location management server may update the location reporting configuration information and inform the location management client of the update ones at any time by triggering the location reporting configuration update procedure.

Figure 9.3.3.4-1 illustrates the procedure for location reporting configuration update.

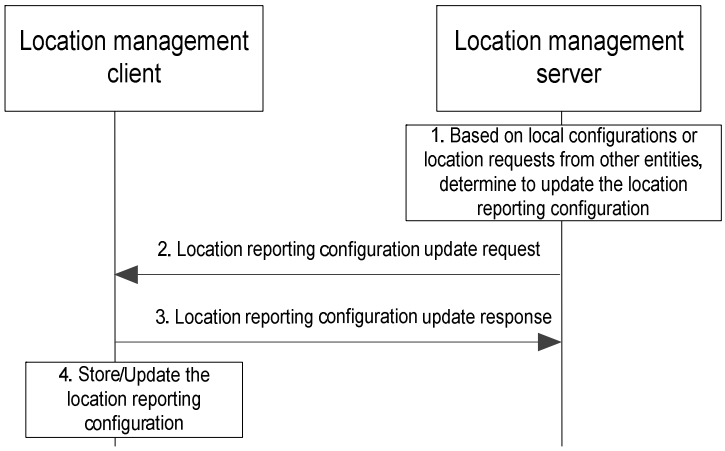

Figure 9.3.3.4-1: Location reporting configuration update procedure

1. Based on the local configurations or the location information request from other entities (e.g., another location management client, VAL server) or if the VAL server updates the geographical location information of the existing VAL service area ID and there is triggering criteria corresponding to the updated VAL service area ID, the location management server decides to update the location reporting configuration and informs the updated information to the location management client.

2. The location management server sends location reporting configuration update request message to the location management client(s) which may contain the updated location reporting configuration, e.g. the event triggers, the minimum time between consecutive reports, the requested location access type and positioning methods when

VAL UE fetches the UE location report. 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. If the location reporting trigger from VAL server contains the triggering criteria based on the VAL service area ID, then the location management server converts those triggers into geographical area based triggers while sending it to the location management client.

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

3. The location management client(s) reply with location reporting configuration update response to the location management server with the update result.

4. The location management client stores or updates the new location reporting configuration received in step 2.

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.

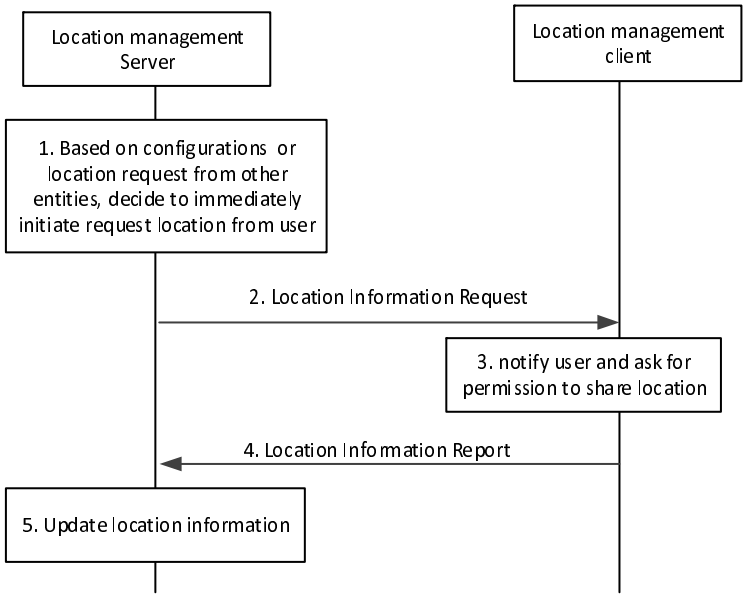

Figure 9.3.4-1: On-demand location information reporting procedure

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.

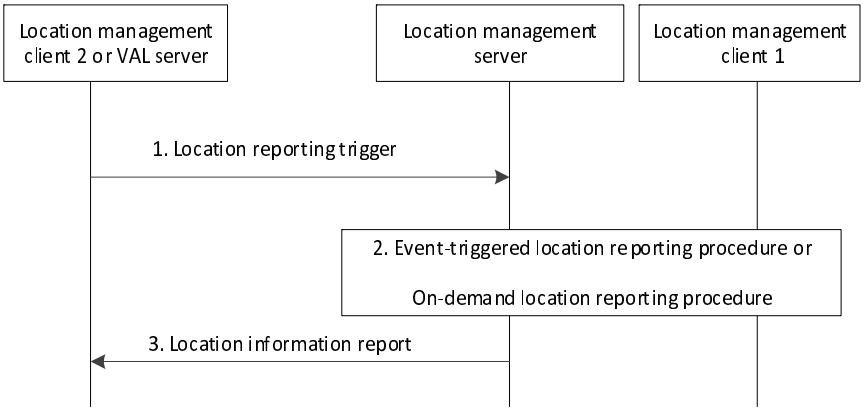

Figure 9.3.5-1: Client-triggered location reporting procedure

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. The location reporting event triggers e.g. minimum time between consecutive reports, SAI changes, access RAT changes, or ECGI changes for reporting the location of the VAL UE, are included.

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

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.

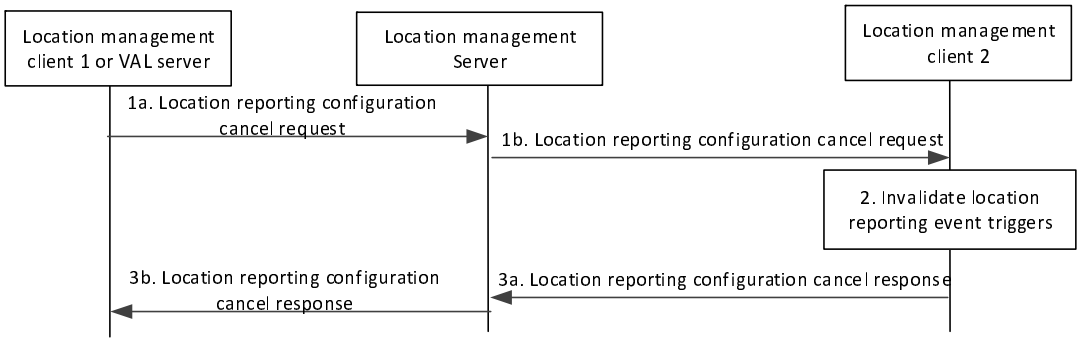

Figure 9.3.6-1: Location reporting triggers configuration cancel

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 initiating tracking a UE's location.

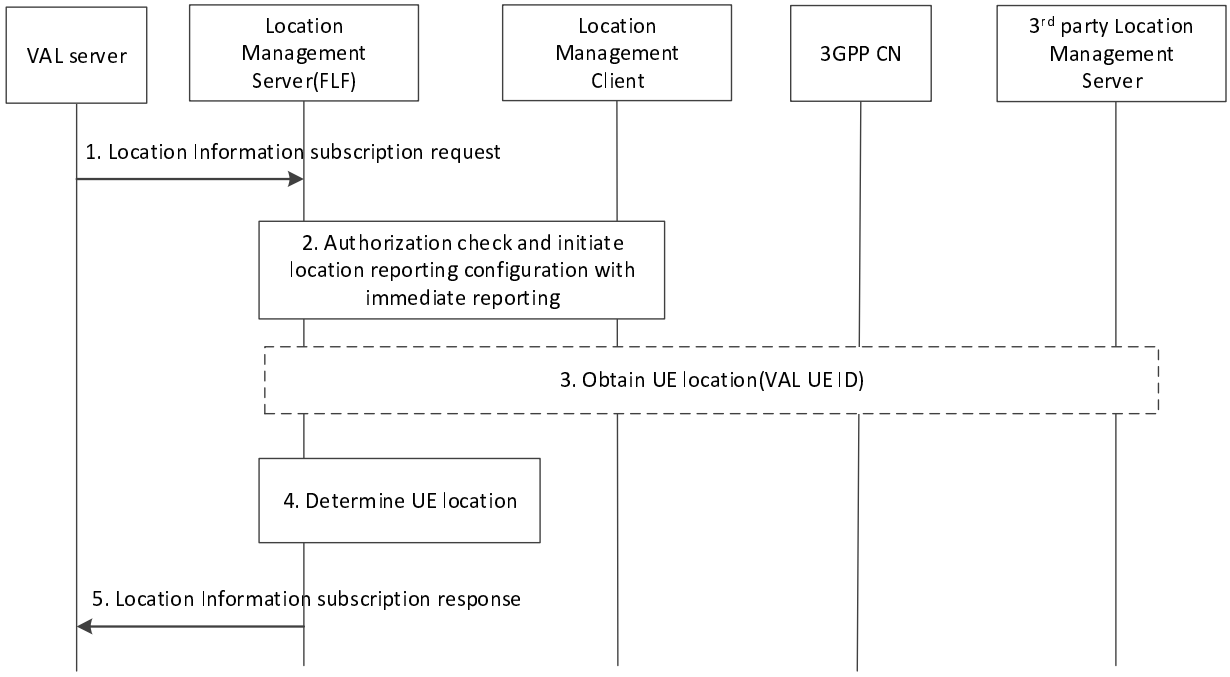

Figure 9.3.7-1: Location information subscription request procedure

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 and the location QoS which contains the location accuracy, response Time and QoS class as defined in clause 4.1b of TS 23.273 [50].

2. The location management server shall check if the VAL server is authorized to initiate the location information subscription request and may retrieve the available and proper location access type and positioning methods (e.g. as described in TS 23.273 [50] and TS 29.572 [51]) for the target VAL UE based on the received location QoS. Further, the location management server may initiate location reporting configuration optionally including the retrieved location access type and positioning methods 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 and/or the 3rd party location management server.

NOTE: How the location management server obtains the UE location from the 3rd party location management server is out of scope of this specification.

4. The location management server determines the UE location information of the UE as received in steps 2 and 3 and checks if it meets the location QoS requirements (if any) or not.

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.

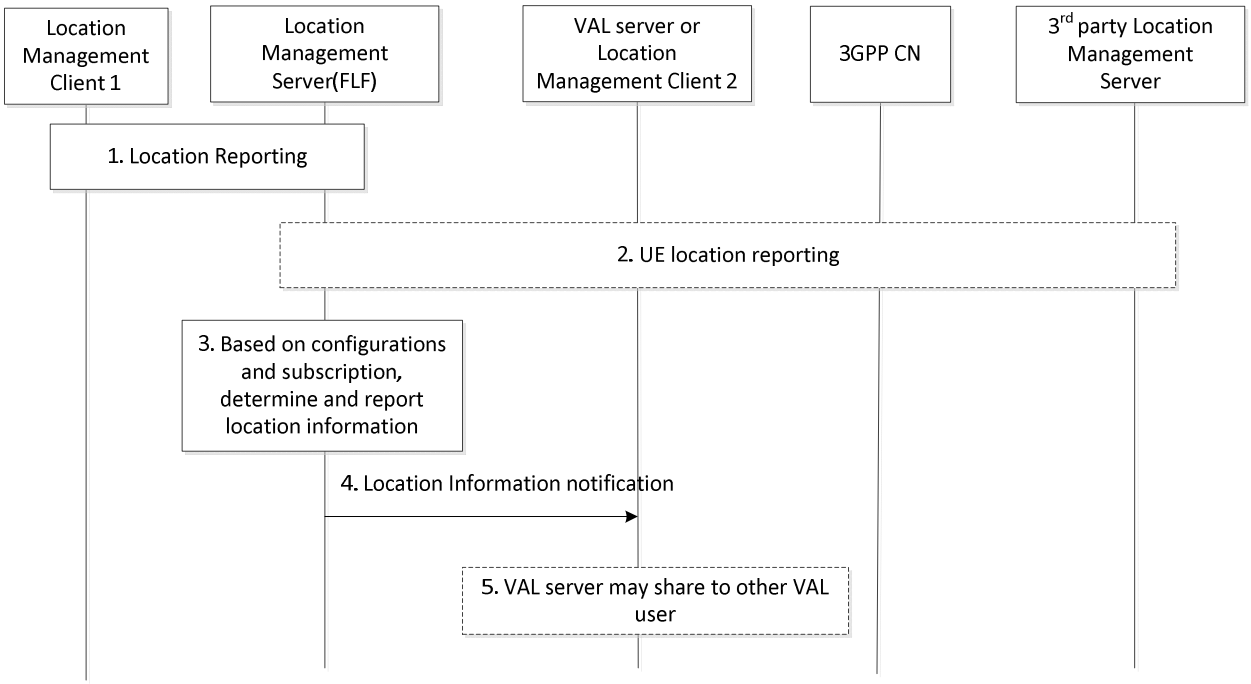

Figure 9.3.8-1: Event-trigger usage of location information procedure

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 and/or the 3rd party location management server network. If the indication for supplementary location

information is included in the subscription, then UE location information is obtained from the 3GPP core network and/or the 3rd party location management server.

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). The Location management server may report the location to the VAL server considering the location information received via non-3GPP positioning technologies (e.g. GNSS, Bluetooth), for instance, to improve the location accuracy.

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.

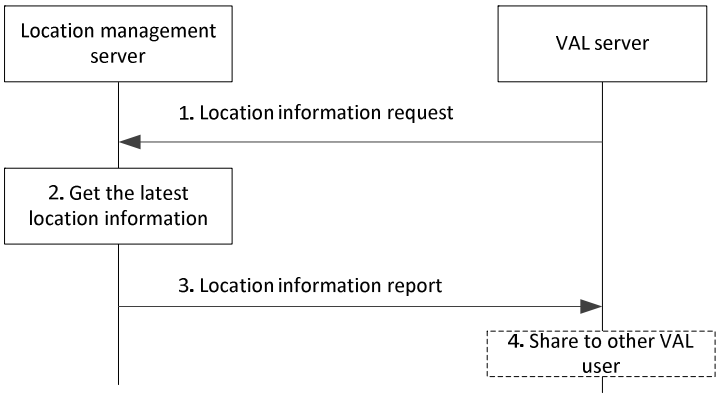

Figure 9.3.9-1: On-demand usage of location information procedure

1. VAL server sends a location information request to the location management server which may include the location QoS that contains the location accuracy, response Time and QoS class as defined in clause 4.1b of TS 23.273 [50].

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, and checks if the obtained location of the VAL UE could meet the location QoS requirements (if any).

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. The Location management server may report the location to the VAL server considering the location information received via non-3GPP positioning technologies (e.g. GNSS, Bluetooth), for instance, to improve the location accuracy.

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 4 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.

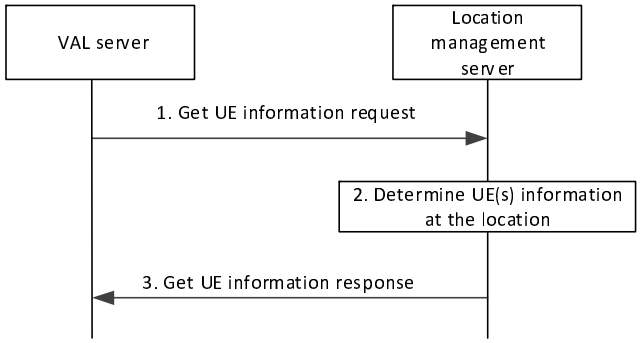

Figure 9.3.10-1: Obtaining UE(s) information at a location

1. The VAL server sends get UE information request to the location management server. The request contains a location information or VAL service area identified by the VAL service area ID 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 or VAL service area identified by the VAL service area ID provided in step 1.
3. The location management server sends get UE information response to the VAL server with a list of VAL UE(s) or VAL user(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 LM server authorized to consume the 3GPP core network service (Monitoring events provided by NEF as specified in 3GPP TS 23.502 [11]).

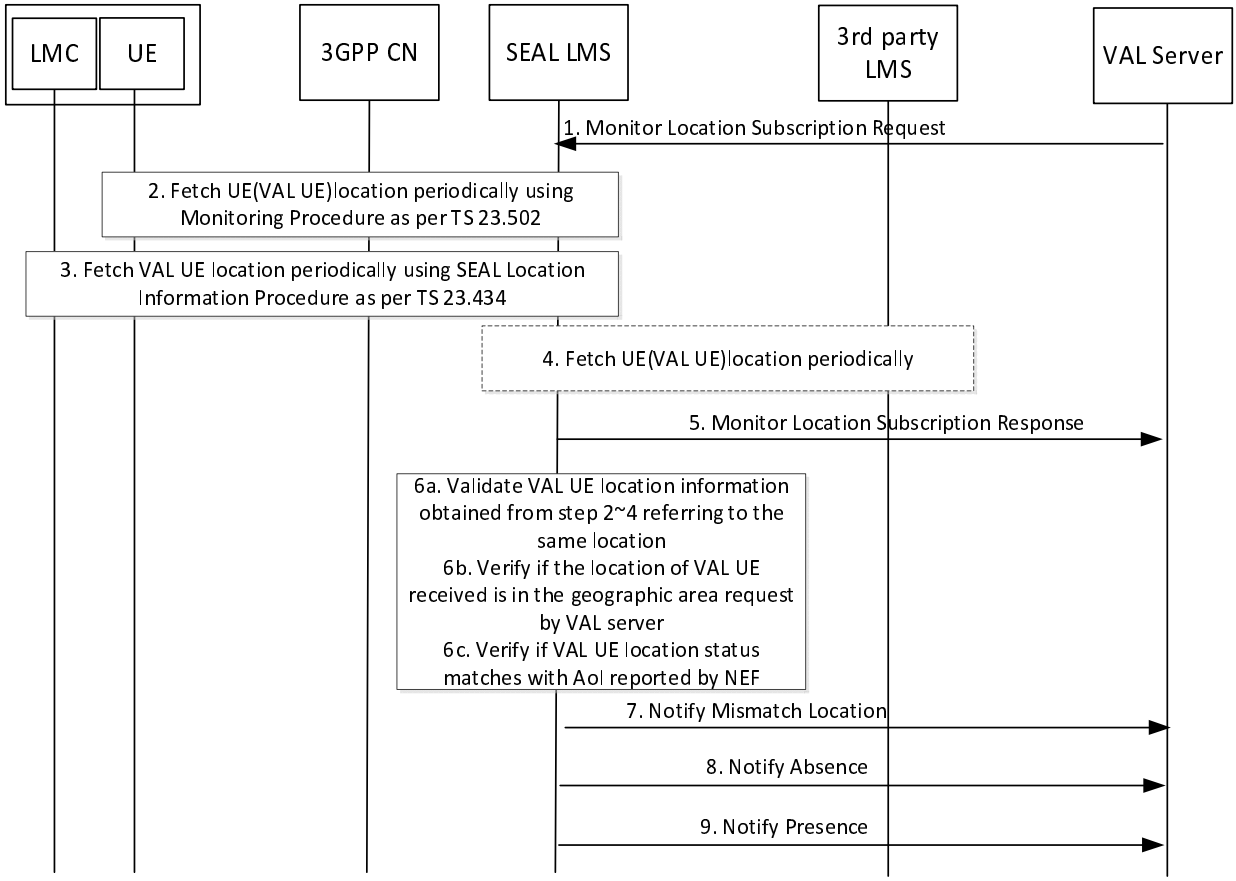

Figure 9.3.11.2-1: Monitoring VAL UE's location at a given location

1. The VAL server sends Monitor Location Subscription Request to LM 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 LM 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 LM 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 LM server ignores the "Notify_Interval" and sends the location notification to the VAL server immediately.

2. LM server 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 LM server receives the VAL UE location information periodically from the 3GPP core network. The LM server also invokes NEF service for Area of Interest monitoring as specified in clause 5.3.3 of 3GPP TS 23.256 [52] to know whether the VAL UE is in the VAL server's predetermined area of interest.

3. LM server 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 LM server may determine to additionally include the positioning methods in SEAL LMS procedures to obtain location information.

4. LMS may periodically obtain the VAL UE location information from the 3rd party location management server based on the geographic information from the VAL server.

NOTE 1: How the LMS obtains the UE location from the 3rd party location management server is out of scope of this specification.

5. LM server, after successful subscription according to steps 2~4, sends Monitor Location Subscription response, indicating that the LM 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.

6a and 6b. LM server processes the location information received from SEAL Location Information procedures, the 3GPP core network and/or the 3rd party location management server, and validates the information. If the location information is matching, then the LM server shall check if the VAL UE's current location is within the predetermined area of interest received in step 1.

NOTE 2: The location information received from the 3GPP core network and from LM client does not necessarily be exactly the same, the LM server can aggregate the location information if there is no big deviation.

6c. LM server verifies its determined VAL UE location status (i.e. presence or absence with regard to the predetermined area of interest) with the retrieved 3GPP core network result from the NEF monitoring service for Area of Interest. The LM server will continue with step 7, step 8 and step 9 as applicable.

7. If the location information received from Location management client, the 3GPP core network and/or the 3rd party location management server do not match or the NEF reported Area of Interest monitoring result does not match with the determined VAL UE location status (present/absence) in LM server, then the LM 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 LM server,the 3GPP core network and/or the 3rd party location management server in the notification message.

8. If the VAL UE's current location is from Location management client, the 3GPP core network and/or the 3rd party location management server matches, and not in the area of interest received from VAL server in Monitor Location Subscription Request message, and such out of area of interest result is also aligned with the NEF reported area of interest monitoring result, then the LM server 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.

9. When the VAL UE's current location is in area of interest, and such in area of interest result is also aligned with the NEF reported area of interest monitoring result, then the LM server 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.

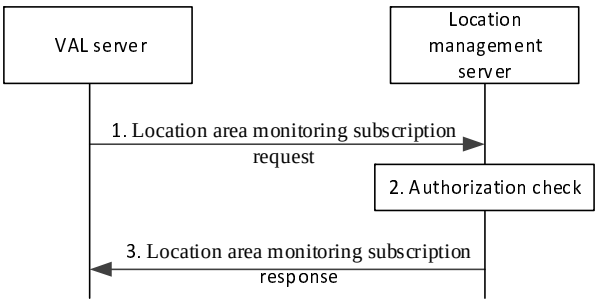

Figure 9.3.12.1-1: Location area monitoring subscription procedure

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 or the VAL service area identified by the VAL service area ID 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.

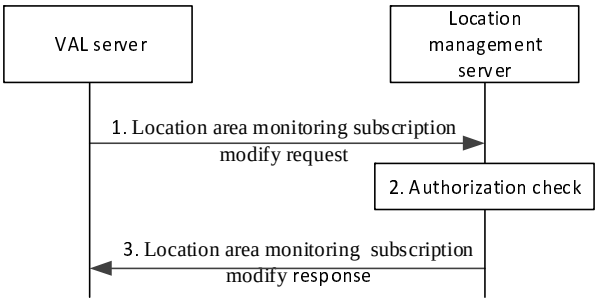

Figure 9.3.12.2-1: Location area monitoring subscription modify procedure

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.

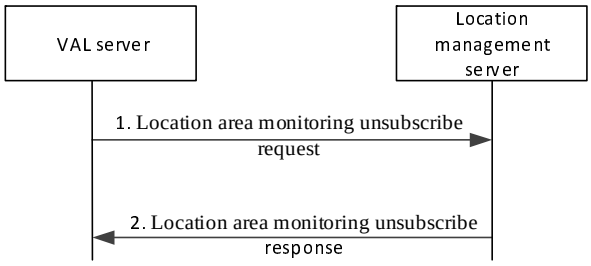

Figure 9.3.12.3-1: Location area monitoring unsubscribe procedure

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.

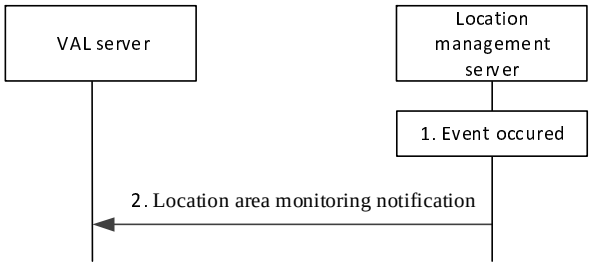

Figure 9.3.12.4-1: Location are monitoring notification procedure

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.

9.3.13 VAL Service Area configuration

9.3.13.1 General

The VAL service area refers to the geographical area(s) (e.g., coordinates, civic addresses, network areas) served by a VAL server. The VAL service area is identified by the VAL service area identifier (ID). The VAL server may have more than one VAL service area defined. These VAL service areas are configured by the VAL server to the location management server and are assigned with a unique VAL service area identifier. When the VAL service area configurations are in place the VAL server may use the VAL service area ID as part of the location information in the SEAL APIs requiring location information. These configurations can be updated by the VAL server in-order to modify the geographical area(s) associated with the VAL service area and when is updated, the SEAL internally manage the updates without requiring the VAL server to re-invoke the APIs where the updated VAL service area are being used.

9.3.13.2 Configure VAL service area identifier procedure

Figure 9.3.13.2-1 illustrates the high level procedure of the VAL service area identifier configuration.

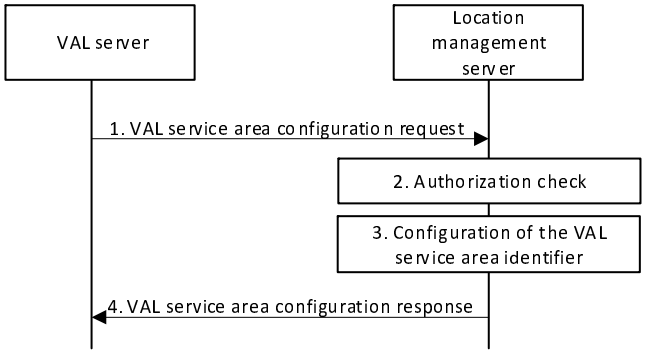

Figure 9.3.13.2-1: Configure VAL service area identifier procedure

1. The VAL server sends the VAL service area configuration request to the location management server to configure a new VAL service area identifier. In the request message, the VAL server includes the information as specified in table 9.3.2.21-1.

2. The location management server shall check if the VAL server is authorized to initiate VAL service area identifier configuration request.

3. If the VAL server is authorized to configure the VAL service area identifiers, the VAL server checks the consistency of the provided identifiers (e.g., all VAL service area identifiers shall be unique) and configures the provided VAL service area identifiers.

4. The location management server sends the VAL service area configuration response with the information as specified in table 9.3.2.22-1.

9.3.13.3 Obtain VAL service area identifier procedure

Figure 9.3.13.3-1 illustrates the high level procedure of the VAL service area retrieval.

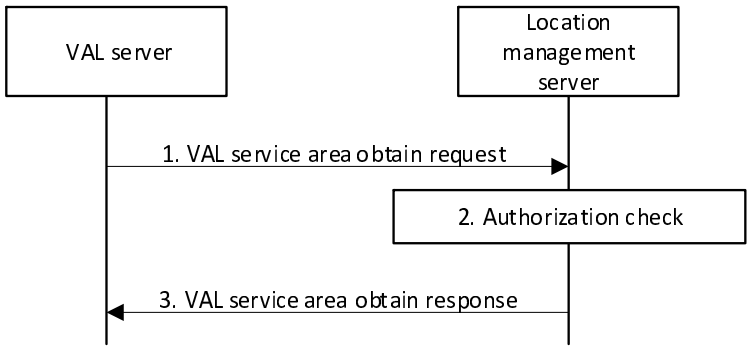

Figure 9.3.13.3-1: Obtain VAL service area procedure

1. The VAL server sends the VAL service area obtain request to the location management server to retrieve the VAL service area identifiers. In the request message, the VAL server includes the information as specified in table 9.3.2.26-1.

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

3. If the VAL server is authorized to obtain the VAL service area identifiers, the location management server sends the VAL service area obtain response with the information as specified in table 9.3.2.27-1.

9.3.13.4 Update VAL service area identifier procedure

Figure 9.3.13.4-1 illustrates the high level procedure of the VAL service area update.

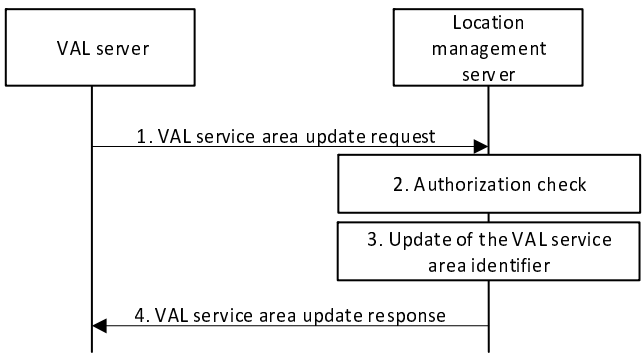

Figure 9.3.13.4-1: Update VAL service area procedure

1. The VAL server sends the VAL service area update request to the location management server to update the VAL service area identifier(s) configured by the VAL server. In the request message, the VAL server includes the information as specified in table 9.3.2.28-1.
2. The location management server shall check if the VAL server is authorized to initiate VAL service area update request.
3. The location management server checks whether the VAL service area IDs exist and then updates the VAL service area identifier(s).
4. The location management server sends the VAL service area update response with the information as specified in table 9.3.2.29-1.

9.3.13.5 Delete VAL service area identifier procedure

Figure 9.3.13.5-1 illustrates the high level procedure of the VAL service area delete.

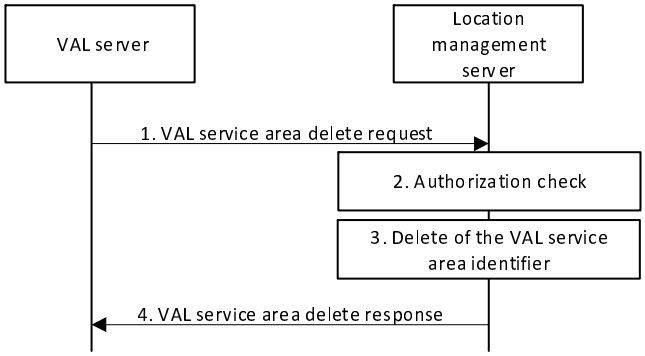

Figure 9.3.13.5-1: Delete VAL service area procedure

1. The VAL server sends the VAL service area delete request to the location management server to delete the VAL service area identifier(s) configured by the VAL server. In the request message, the VAL server includes the information as specified in table 9.3.2.30-1.
2. The location management server shall check if the VAL server is authorized to initiate VAL service area delete request.
3. The location management server checks whether the VAL service area IDs exist and then deletes the VAL service area identifier(s).

NOTE: An deletion of the VAL service area ID(s) does not affect the existing subscriptions in the SEAL layer.

4. The location management server sends the VAL service area delete response with the information as specified in table 9.3.2.31-1.

9.3.13.6 VAL service area identifier subscribe procedure

Figure 9.3.13.6-1 illustrates the high level procedure of the subscribe VAL service area update events.

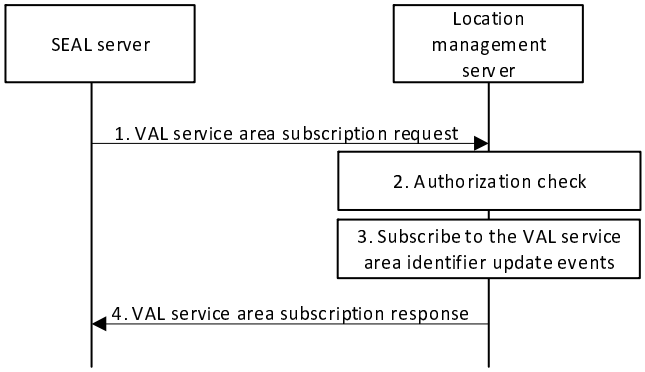

Figure 9.3.13.6-1: Subscribe VAL service area procedure

1. The SEAL server sends the VAL service area subscription request to the location management server to subscribe for the VAL service area identifier(s) update events. In the request message, the SEAL server includes the information as specified in table 9.3.2.42-1.
2. The location management server shall check if the SEAL server is authorized to susbcribe for the VAL service area identifier(s) update event(s).
3. if the SEAL server is authorized to subscribe for the VAL service area identifier(s) update events, the location management server creates the subscription based on the provided parameters in the request.
4. The location management server sends the VAL service area subscription response with the information as specified in table 9.3.2.43-1.

9.3.13.7 VAL service area identifier notify procedure

Figure 9.3.13.7-1 illustrates the high level procedure for notification of a SEAL server about the VAL service area identifier update events at the location management server.

Pre-conditions:

- the SEAL server has an active VAL service area subscription at the location management server; and
- the subscribed event has occurred.

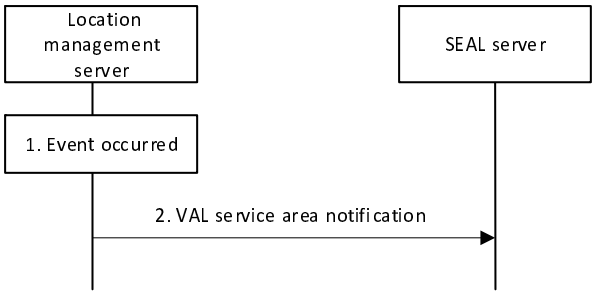

Figure 9.3.13.7-1: Notify VAL service area procedure

1. The location management server identifies the list of the occurred events for which the SEAL server subscribed.
2. The location management server sends a VAL service area notification to the SEAL server. In the notification message, the location management server includes the information as specified in table 9.3.2.44-1.

9.3.13.8 VAL service area identifier unsubscribe procedure

Figure 9.3.13.8-1 illustrates the high level procedure for a SEAL server to unsubscribe the notifications about the VAL service area identifier update events at the location management server.

Pre-conditions:

- the SEAL server has an active VAL service area subscription at the location management server.

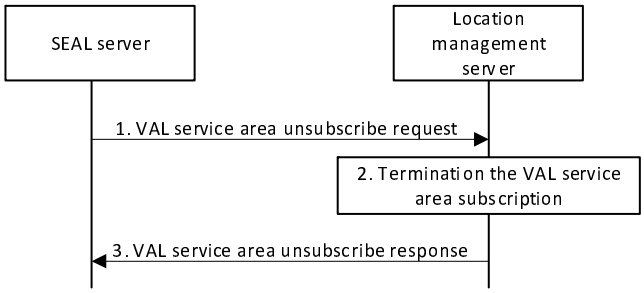

Figure 9.3.13.8-1: Unsubscribe VAL service area procedure

1. When the SEAL server decides to terminate a VAL service area subscription, it sends a VAL service area unsubscribe request to the location management server. In the request message, the SEAL server includes the information as specified in table 9.3.2.45-1.

2. If the SEAL server is authorized to terminate the subscription, the location management server terminates the VAL service area subscription.

3. The location management server sends a VAL service area unsubscribe response to the SEAL server, the location management server includes the information as specified in table 9.3.2.46-1.

9.3.13.9 VAL service area identifier subscription update procedure

Figure 9.3.13.9-1 illustrates the high level procedure of the update subscription for the VAL service area update events.

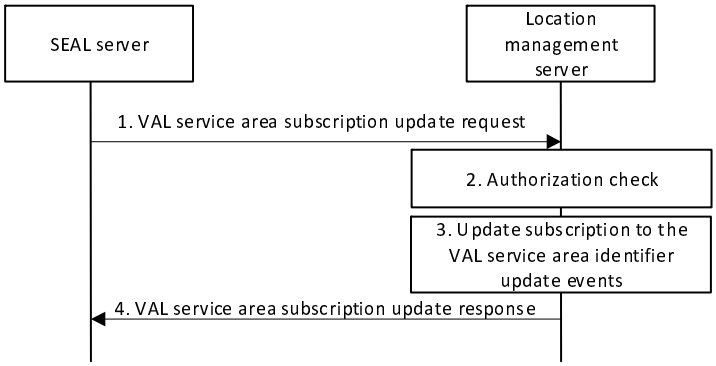

Figure 9.3.13.9-1: VAL service area identifier subscription update procedure

1. The SEAL server sends the VAL service area subscription update request to the location management server to update the existing subscription for the VAL service area identifier(s) update events. In the request message, the SEAL server includes the information as specified in table 9.3.2.42-1.

2. The location management server shall check if the SEAL server is authorized to update the subscription for the VAL service area identifier(s) update event(s).

3. if the SEAL server is authorized, the location management server checks whether the target susbcription exists and then updates the subscription for the VAL service area identifier(s) update events.

4. The location management server sends the VAL service area subscription update response with the information as specified in table 9.3.2.43-1.

9.3.14 Location profiling for supporting location service enablement

9.3.14.1 Location profiling

The location management server enhanced with the Fuse Location Function(FLF) supports the creation of location profiles for location service at the application enablement layer and the mapping of location profiles to one or more vertical applications. Location profiling is based on the vertical driven hybrid positioning requirements and policies.

The example of attributes that can be used for the location profiles is specified in Annex D.

9.3.14.2 Procedure of Location profiling for location service

The procedure includes the translation of the vertical request to a location profile and the derivation of the requested location information report.

Pre-condition: The Location Management Server has configured a set of location service profiles.

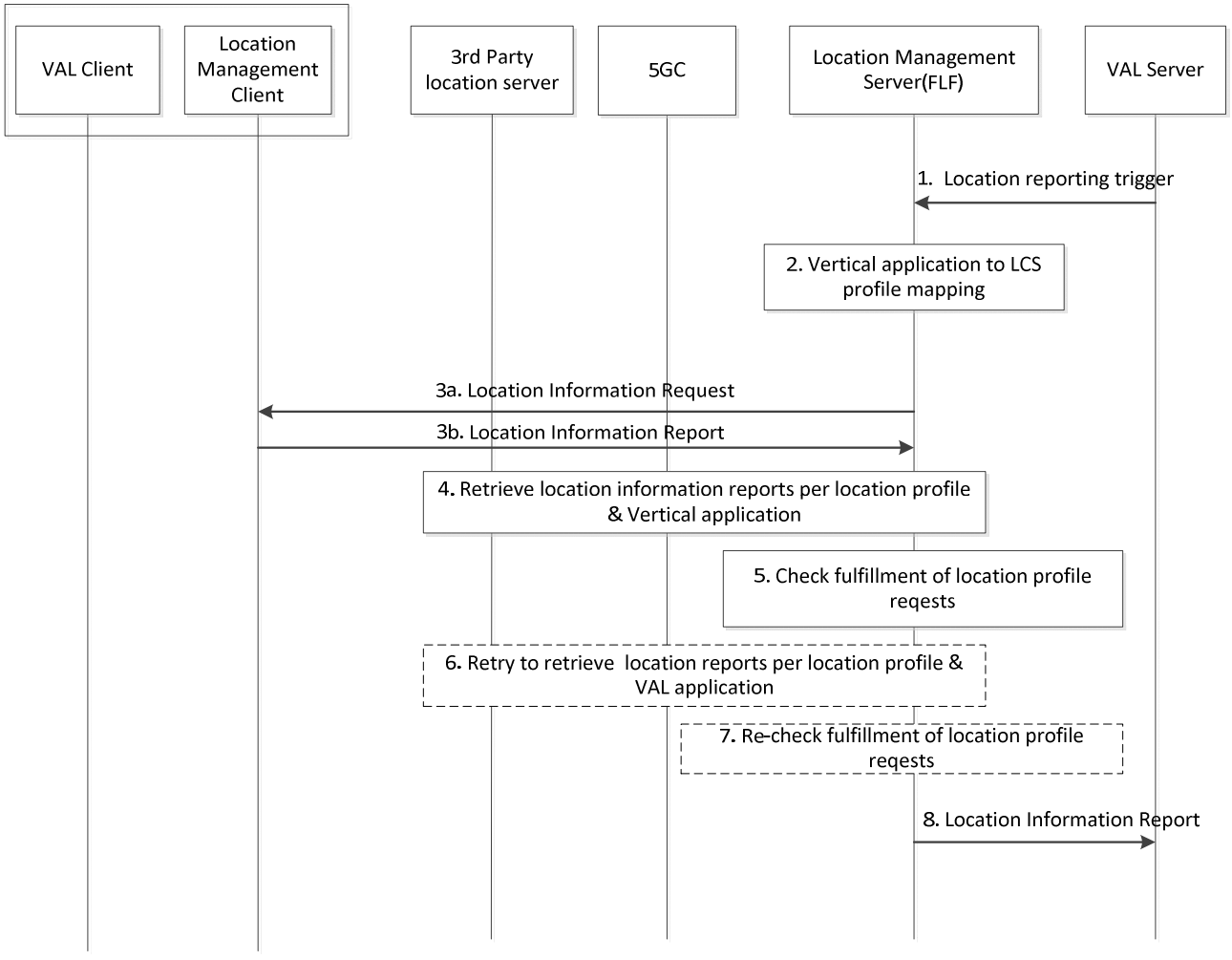

Figure 9.3.14.2-1: Location profiling for location derivation and exposure

1. The LM Server receives a location reporting trigger from VAL server and activates a location reporting procedure as defined in clause 9.3.5.

2. The Fused Location Function determines a mapping of the vertical location services to a location service profile based on the location request information, the location profiles and the location capability of VAL UE which registered to the LM Server before.

3a. The LM Server requests from the LMC the location information of the target VAL UE optionally with the requested location information (the access type, positioning method) based on the determined location profiles in LM server obtained in step 2.

3b. The LM Client responds to the LM Server the location report based on the request.

4. The LM Server performs a location information request to one or more of the following (based on the location profile):

   - to GMLC directly or via NEF (as defined in TS 23.273 [50]), acting as AF.

   - to 3rd party location servers.

5. The Fused Location Function calculates the location information based on combined location reports from step 3~4 and checks whether the location reports fulfil the location profile requirements.

6-7. If the requirements are not fulfilled, the LM Server will repeat the step 3~5 iteratively to request location information and re-check whether the requirements are met or not.

8. If the requirements are fulfilled, the LM Server sends the location information report to the VAL server.

9.3.15 Location service registration procedure

Before the Location Management Server requesting the location information for the target UE, the Location Management Client may register the available location services to the LM Server to report the UE's location capabilities.

Figure 9.3.15-1 illustrates the procedure of client-triggered location service registration.

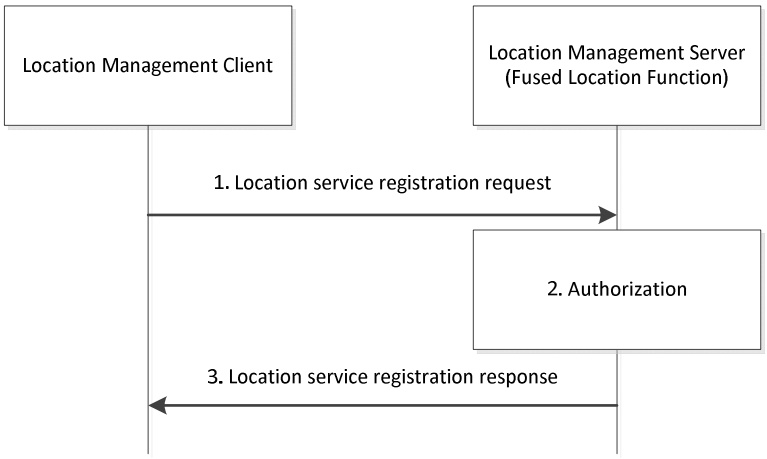

Figure 9.3.15-1: Location service registration procedure

1. The LM Client of a VAL UE sends location service registration request to the LM Server, with the identifier of the UE (e.g. GPSI) and UE-based location capabilities.

2. The LM Server checks authorization for the VAL UE's registration request.

3. After successful authorization, LM Server sends location service registration response to the LM Client and stores the UE identifier information and location capabilities.

9.3.16 Location information unsubscribe procedure

Figure 9.3.16-1 illustrates the high level procedure of location information unsubscribe request. The same procedure can be applied for the location management client and other entities that would like to unsubscribe to the VAL UE's location information.

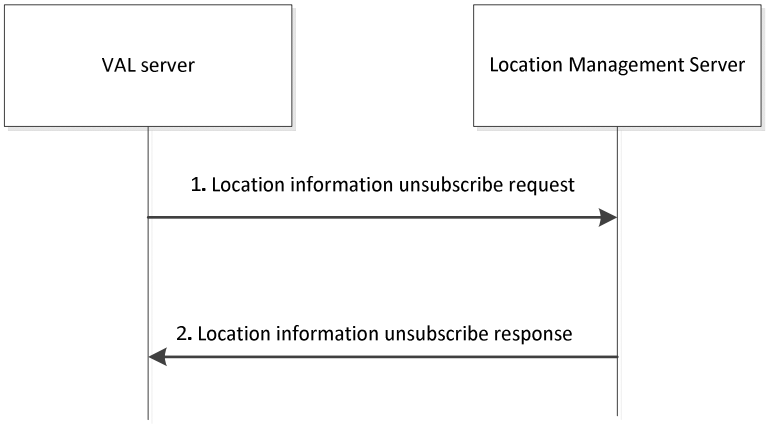

Figure 9.3.16-1: Location information unsubscribe procedure

1. The VAL server sends location information unsubscribe request to the location management server to unsubscribe the subscription to the VAL UE's location information.
2. The location management server replies with location information unsubscribe response indicating the unsubscribe status.

9.3.17 Monitor location unsubscribe procedure

Figure 9.3.17-1 illustrates the high level procedure of location monitoring unsubscribe request. The same procedure can be applied for other entities that would like to unsubscribe the subscription to monitor the VAL UE's location in a given area of interest.

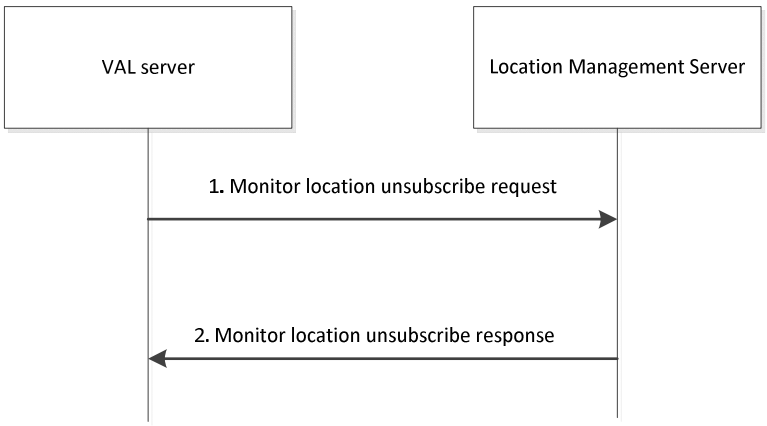

Figure 9.3.17-1: Monitor location unsubscribe procedure

1. The VAL server sends Monitor location unsubscribe request to the location management server to unsubscribe the subscription to monitor the VAL UE's location in a given area of interest.
2. The location management server replies with Monitor location unsubscribe response indicating the unsubscribe status.

9.3.18 Location service registration update procedure

Figure 9.3.18-1 illustrates the procedure of client-triggered location service registration update. The Location Management Client may update its supported location capabilities (e.g. location access type, position methods) which has registered to the Location Management Server before.

Pre-condition:

The Location Management Client has registered to the Location Management Server.

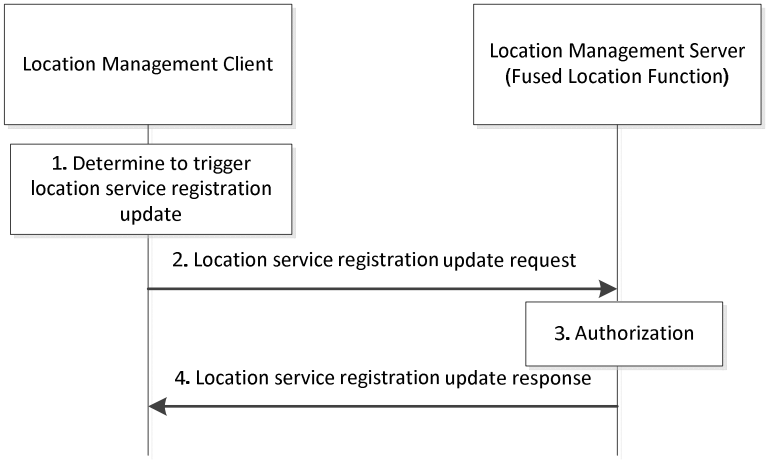

Figure 9.3.18-1: Location service registration update procedure

1. The LM Client decides to trigger the registration update request to LM Server to update the location capabilities which have registered to the LM Server before.
2. The LM Client sends location service registration update request to the LM Server with the identifier of the VAL UE, the VAL service ID and updated location capabilities.
3. The LM server checks the authorization for the VAL UE's registration update request. If the authorization is successful, the LM server will update the UE's location capabilities received in step 2.
4. The LM Server sends location service registration update response to the LM Client.

9.3.19 Location service deregistration procedure

Figure 9.3.19-1 illustrates the procedure of client-triggered location service deregistration. By deresgistration, the Location Management Client may deregister the available location services which have registered to the Location Management Server before.

Pre-condition:

The Location Management Client has registered to the Location Management Server.

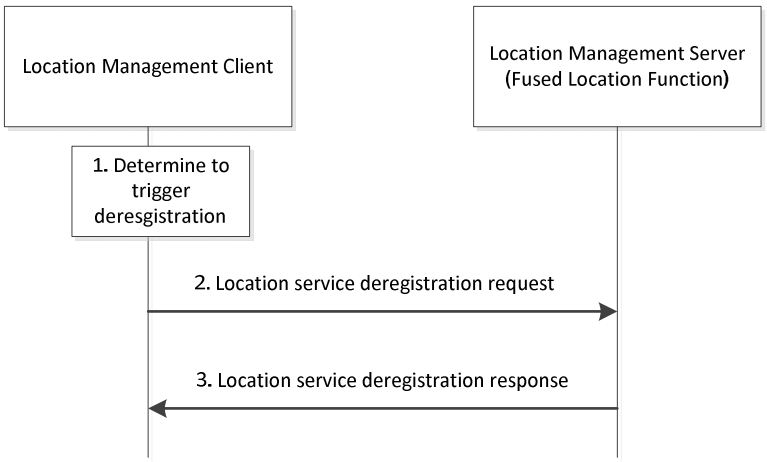

Figure 9.3.19-1: Location service deregistration procedure

1. The LM Client decides to trigger the deresgistration request to LM Server to deregister the location services which have registered to the LM Server before.
2. The LM Client sends location service deregistration request to the LM Server with the identifier of the UE.
3. The LM Server sends location service deregistration response to the LM Client and removes all registration information of the UE.

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 Notify_Trigger_Location_Reporting	VAL server	Subscribe/Notify
SS_LocationInfoEvent	Subscribe_Location_Info	VAL server	Subscribe/Notify
	Unsubscribe_Location_Info	VAL server	
	Update_Location_Info_Subscription	VAL server	
	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
	Unsubscribe_Location_Monitoring	VAL server	
	Update_Location_Monitoring_Subscription	VAL server	
	Notify_Location_Monitoring_Events	VAL server	
	Subscribe_Location_Area_Monitoring	VAL server	Subscribe/Notify
	Notify_Location_Area_Monitoring_Events		
	Update_Location_Area_Monitoring_Subscribe		
	Unsubscribe_Location_Area_Monitoring		
SS_VALServiceAreaConfiguration	Configure_VAL_Service_Area	VAL server	Request/Response
	Obtain_VAL_Service_Area	VAL server	
	Update_VAL_Service_Area	VAL server	
	Delete_VAL_Service_Area	VAL server	
	Subscribe_VAL_Service_Area_Change_Event	SEAL server	Subscribe/Notify
	Notify_VAL_Service_Area_Change_Event	SEAL server	
	Unsubscribe_VAL_Service_Area_Change_Event	SEAL server	
	Update_Subscription_VAL_Service_Area_Change_Event	SEAL 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 9.3.2.25

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

9.4.2.5 Notify_Trigger_Location_Reporting operation

API operation name: Notify_Trigger_Location_Reporting

Description: Notification for location report based on the location trigger.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.7

Outputs: None

See subclause 9.3.5 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, receive and unsubscribe the UEs location information from the location management server over LM-S, as well as modify an active subscription.

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.

9.4.3.4 Unsubscribe_Location_Info operation

API operation name: Unsubscribe_Location_Info

Description: Unsubscribe to the location information.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.32

Outputs: Refer subclause 9.3.2.33

See subclause 9.3.16 for the details of usage of this API operation.

9.4.3.5 Update_Location_Info_Subscription

API operation name: Update_Location_Info_Subscription

Description: Updating an active subscription about the UEs location information.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.5

Outputs: See subclause 9.3.2.6

See subclause 9.3.2.7a 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 operation

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 operation

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.

9.4.6.4 Unsubscribe_Location_ Monitoring operation

API operation name: Unsubscribe_Location_Monitoring

Description: Unsubscribe to the location Monitoring request.

Known Consumers: VAL server.

Inputs: Refer subclause 9.3.2.34

Outputs: Refer subclause 9.3.2.35

See subclause 9.3.17 for the details of usage of this API operation.

9.4.6.5 Update_Location_Monitoring_Subscription

API operation name: Update_Location_Monitoring_Subscription

Description: Updating an active monitor location subscription.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.11

Outputs: See subclause 9.3.2.12

See subclause 9.3.2.12a 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.

9.4.8 SS_VALServiceAreaConfiguration API

9.4.8.1 General

API description: This API enables the VAL server to configure the list of VAL service area identifiers and the corresponding geographical co-ordinates with SEAL LM server.

9.4.8.2 Configure_VAL_Service_Area

API operation name: Configure_VAL_Service_Area

Description: Configuration of VAL service area identifiers.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.21

Outputs: See subclause 9.3.2.22.

See subclause 9.3.13.2 for the details of usage of this API operation.

9.4.8.3 Obtain_VAL_Service_Area

API operation name: Obtain_VAL_Service_Area

Description: Retrieval of VAL service area identifiers.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.26

Outputs: See subclause 9.3.2.27

See subclause 9.3.13.3 for the details of usage of this API operation.

9.4.8.4 Update_VAL_Service_Area

API operation name: Update_VAL_Service_Area

Description: Update of the VAL service area identifier.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.28

Outputs: See subclause 9.3.2.29

See subclause 9.3.13.4 for the details of usage of this API operation.

9.4.8.5 Delete_VAL_Service_Area

API operation name: Delete_VAL_Service_Area

Description: Unsubscribing from VAL service area identifier update events.

Known Consumers: VAL server.

Inputs: See subclause 9.3.2.30

Outputs: See subclause 9.3.2.31

See subclause 9.3.13.5 for the details of usage of this API operation.

9.4.8.6 Subscribe_VAL_Service_Area_Change_Event

API operation name: Subscribe_VAL_Service_Area_Change_Event

Description: Subscription to the VAL service area identifiers change events.

Known Consumers: SEAL server.

Inputs: See subclause 9.3.2.42

Outputs: See subclause 9.3.2.43.

See subclause 9.3.13.6 for the details of usage of this API operation.

9.4.8.7 Notify_VAL_Service_Area_Change_Event

API operation name: Notify_VAL_Service_Area_Change_Event

Description: Notifying the SEAL server about the VAL service area identifier change events.

Known Consumers: SEAL server.

Inputs: See subclause 9.3.2.44

Outputs: None.

See subclause 9.3.13.7 for the details of usage of this API operation.

9.4.8.8 Unsubscribe_VAL_Service_Area_Change_Event

API operation name: Unsubscribe_VAL_Service_Area_Change_Event

Description: Unsubscribing from VAL service area identifier change events.

Known Consumers: SEAL server.

Inputs: See subclause 9.3.2.21

Outputs: See subclause 9.3.2.22.

See subclause 9.3.13.8 for the details of usage of this API operation.

9.4.8.9 Update_Subscription_VAL_Service_Area_Change_Event

API operation name: Update_Subscription_VAL_Service_Area_Change_Event

Description: Subscription update for the VAL service area identifiers change events.

Known Consumers: SEAL server.

Inputs: See subclause 9.3.2.42.

Outputs: See subclause 9.3.2.43.

See subclause 9.3.13.9 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.

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.

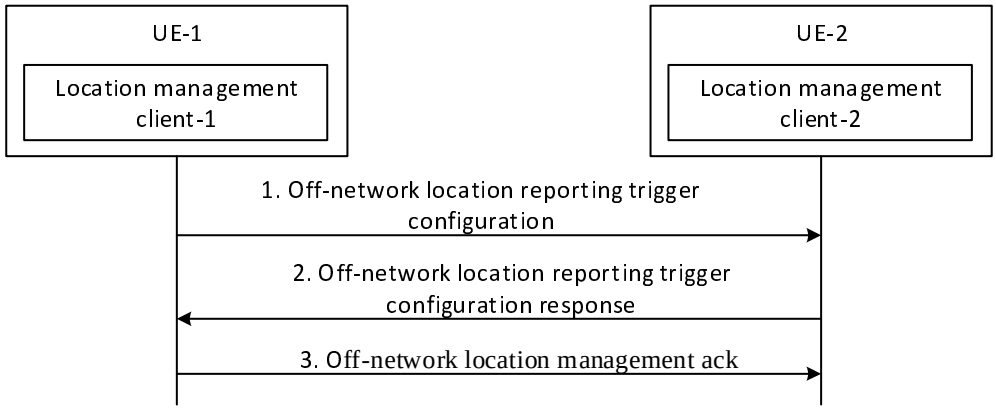

Figure 9.5.3.1-1: Location reporting trigger configuration

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.

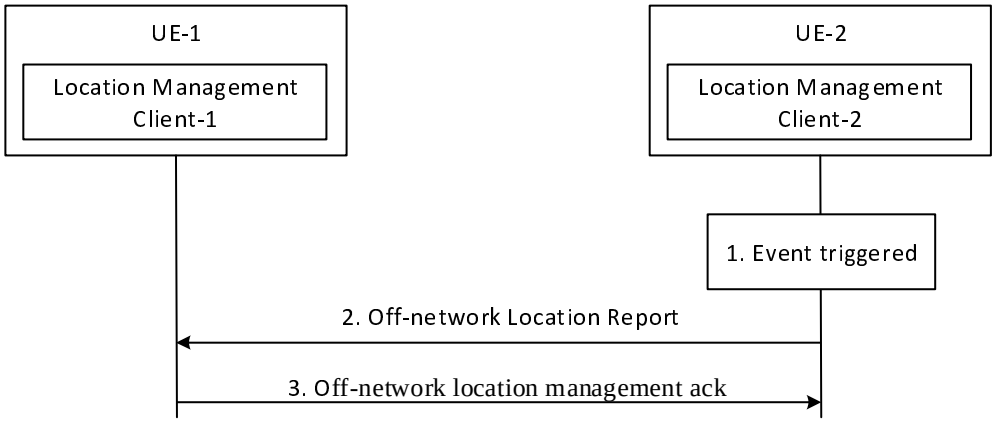

Figure 9.5.3.2-1: Location reporting

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.

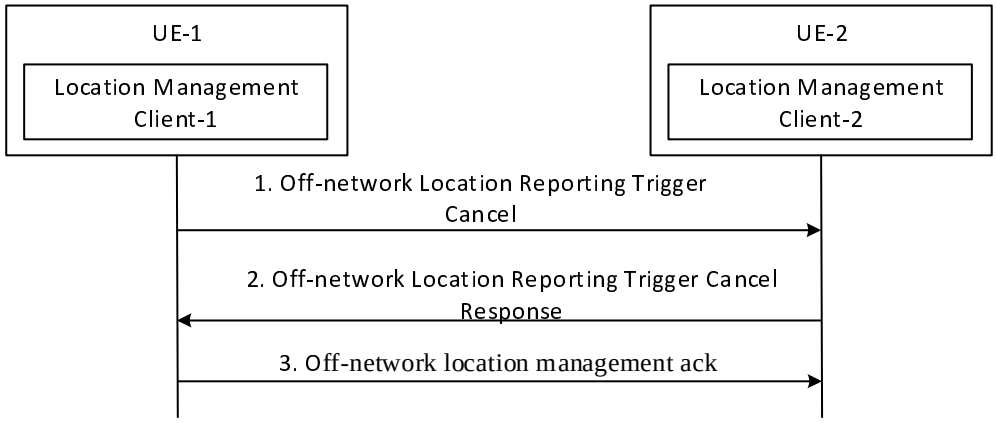

Figure 9.5.3.3-1: Location reporting trigger cancel

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.

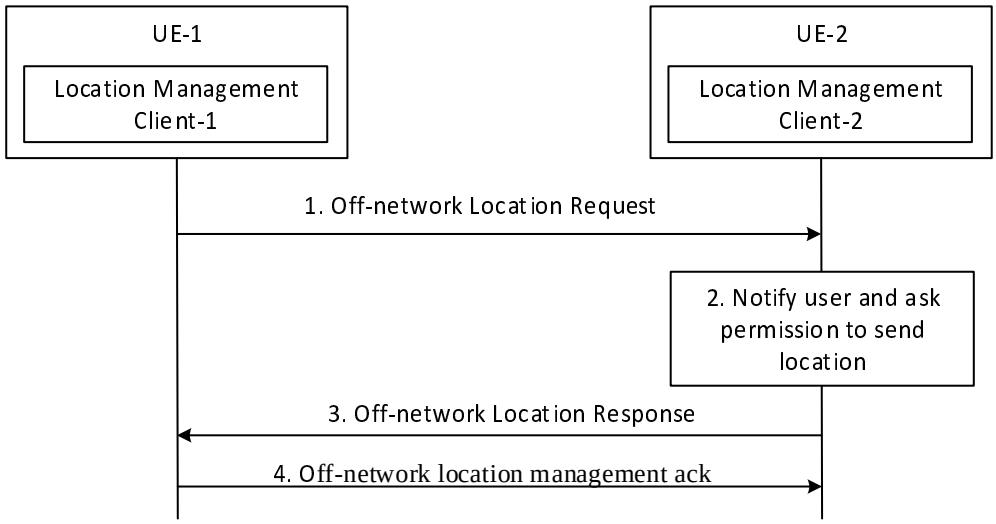

Figure 9.5.4-1: Location reporting trigger cancel

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.

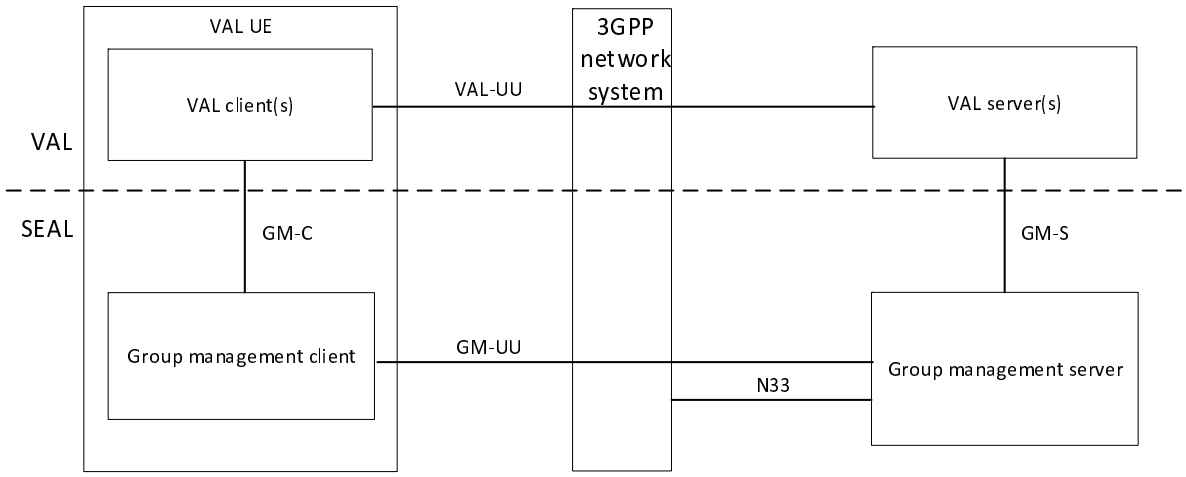

Figure 10.2.2-1: On-network functional model for group management

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.

Figure 10.2.2-2 exhibits the service-based interfaces for providing and consuming group management services. The group management server could provide service to VAL server and group management client through interface Sgm.

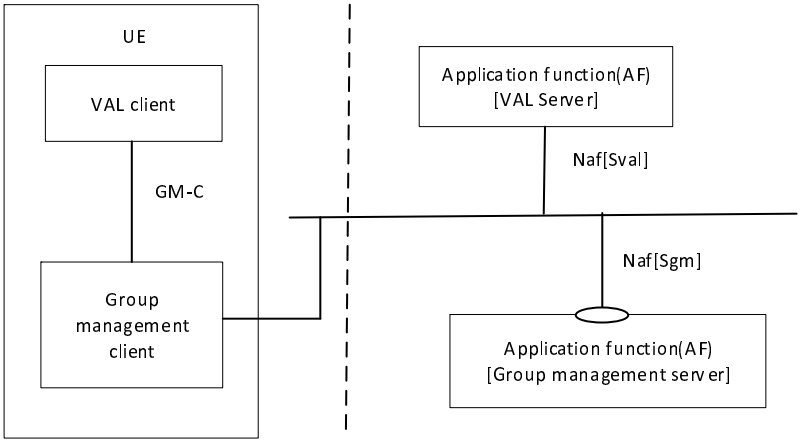

Figure 10.2.2-2: Architecture for group management – Service based representation

Figure 10.2.2-3 illustrates the service-based representation for utilization of the 5GS network services based on the 5GS SBA specified in 3GPP TS 23.501 [10].

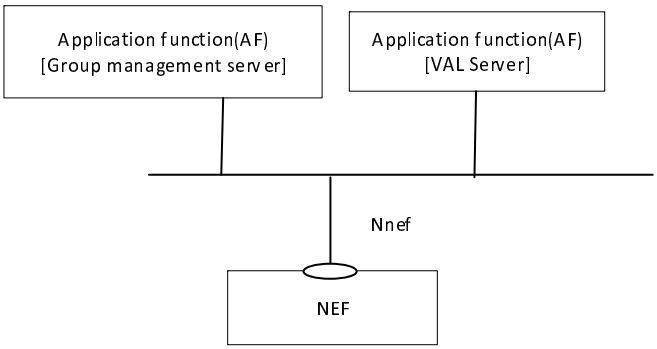

Figure 10.2.2-3: Architecture for group management utilizing the 5GS network services based on the 5GS SBA – Service based representation

Figure 10.2.2-4 illustrates the service-based representation for utilization of the Core Network northbound APIs via CAPIF.

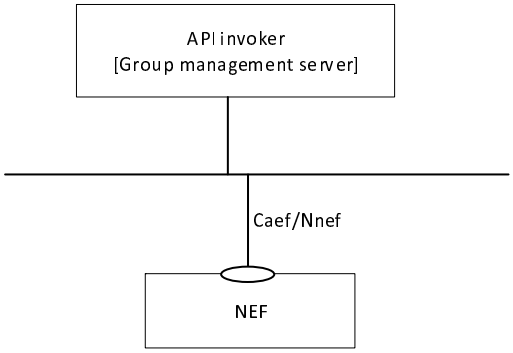

Figure 10.2.2-4: Utilization of Core Network Northbound APIs via CAPIF – service based representation

The Group management server acts as authorized API invoker to consume services from the Core Network northbound API entities like NEF which act as API Exposing Function as specified in 3GPP TS 23.222 [6].

10.2.3 Off-network functional model description

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

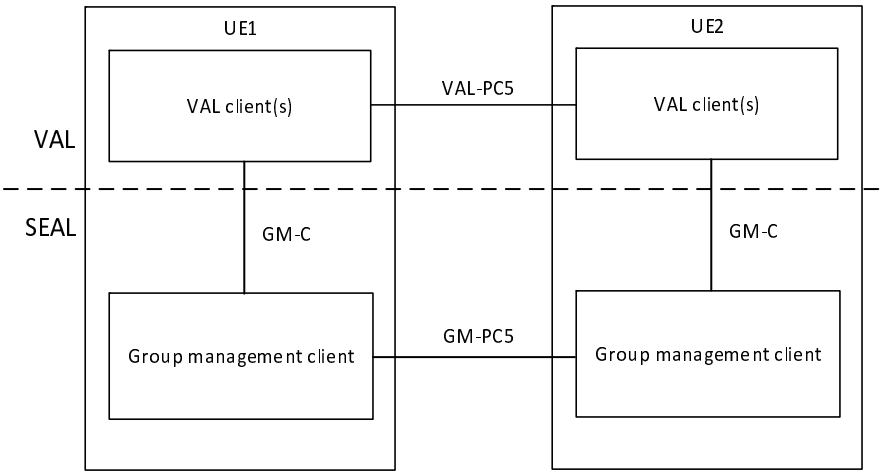

Figure 10.2.3-1: Off-network functional model for group management

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.

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 or VAL server 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 or VAL server 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 or VAL server.

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 or VAL server 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 server, 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 or VAL server.

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 or VAL server 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 or VAL server 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 or VAL server.

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
Reason	O	The reason of group deletion.

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.
Reason	O	The reason of group deletion.

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 client or VAL server to the group management server.

Table 10.3.2.14-1: Group information subscribe request

Information element	Status	Description
Requester Identity	M	The identity of the group management client or VAL server performing the request.
VAL group ID	M	VAL group ID of the group
Minimum time between consecutive notifications	O	Defaults to 0 if not provided, otherwise indicates the minimum time interval between consecutive notifications

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 to the group management client or the VAL server.

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 to the group management client or VAL server.

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 information	M	Group 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 client or VAL server to the group management server.

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 or VAL server 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 or VAL server 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 or VAL server.

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 or VAL server 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 or VAL server 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 or VAL server.

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
Notification target URI	M	Target URI where the group management client performing the request will receive the notifications.
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.		

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 or VAL server performing the request.
Location criteria	M	Criteria to combine Users or UEs in a location (e.g. geographical area or VAL service area ID).
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

10.3.2.43 Unsubscribe group configuration request

Table 10.3.2.43-1 describes the information flow from a group management client to a group management server for unsubscribe group configuration request.

Table 10.3.2.43-1: Unsubscribe 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

10.3.2.44 Unsubscribe group configuration response

Table 10.3.2.44-1 describes the information flow from a group management server to a group management client for unsubscribe group configuration response.

Table 10.3.2.44-1: Unsubscribe group configuration response

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

10.3.2.45 Group configuration subscription update request

Table 10.3.2.45-1 describes the information flow from the group management client to the group management server for group configuration subscription update request.

Table 10.3.2.45-1: Group configuration subscription update 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
Notification target URI	O	Target URI where the group management client performing the request will receive the notifications.
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.		

10.3.2.46 Group configuration subscription update response

Table 10.3.2.46-1 describes the information flow from the group management server to the group management client for group configuration subscription update response.

Table 10.3.2.46-1: Group configuration subscription update response

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

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.

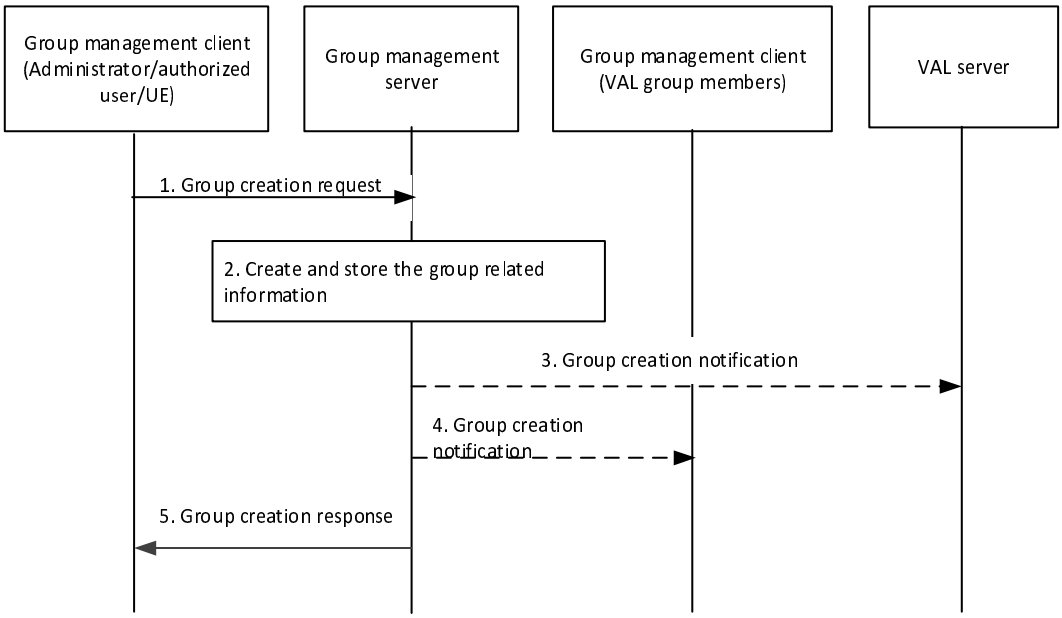

Figure 10.3.3-1: Group creation

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.

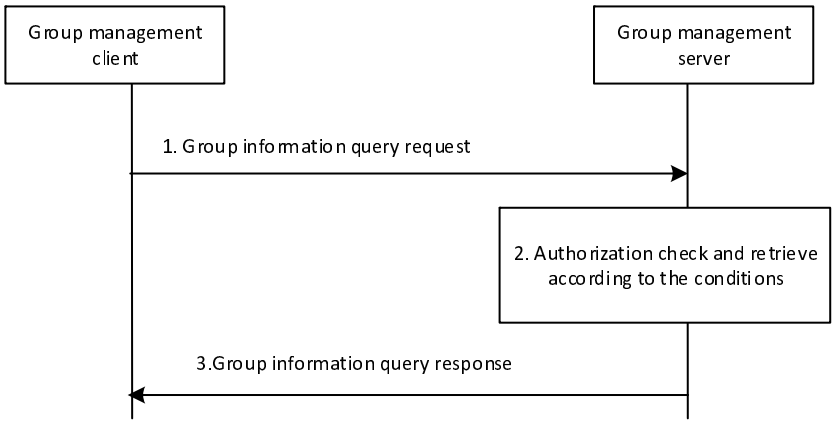

Figure 10.3.4.2-1: Group information query

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

10.3.5.0 Group membership subscription

The procedure for subscription for group membership data as described in figure 10.3.5.0-1 is used by the group management client and VAL server to indicate to the group management server that it wishes to receive updates of group membership data for groups for which it is authorized.

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;

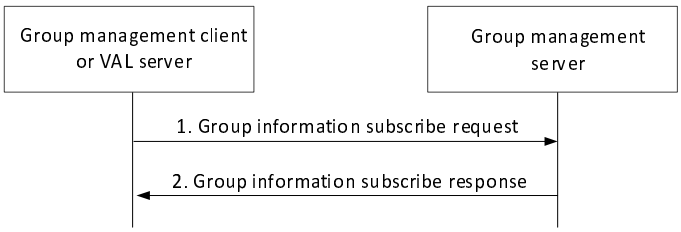

Figure 10.3.5.0-1: Subscription for group membership

1. The group management client or VAL server subscribes to the group membership information stored at the group management server using the group information subscribe request.
2. The group management server provides a group information subscribe response to the group management client or VAL server indicating success or failure of the request.

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.
2. The group management client or VAL server has subscribed to the group configuration information.

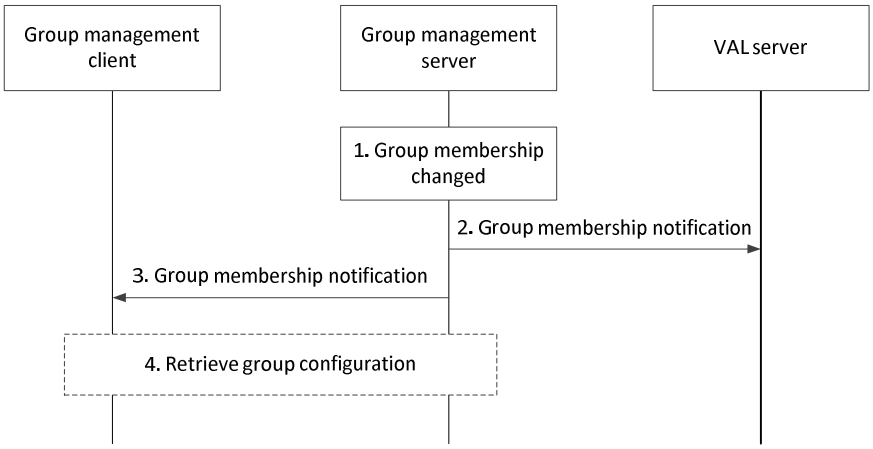

Figure 10.3.5.1-1: group membership notification

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.

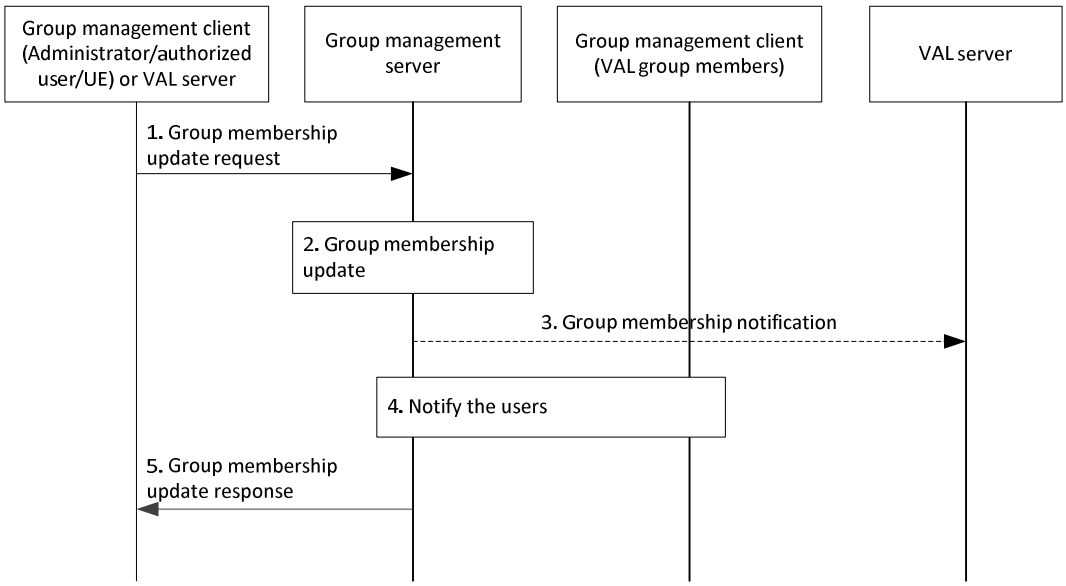

Figure 10.3.5.2-1: Group membership update by authorized user/UE/VAL server

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;

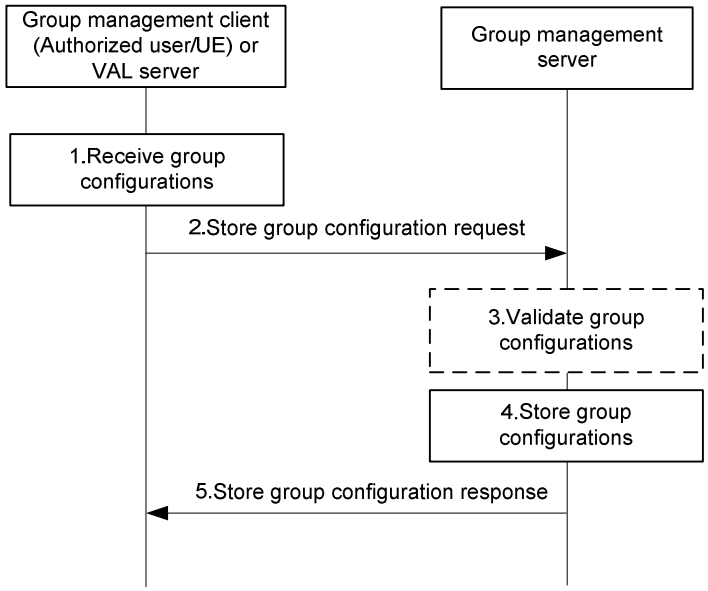

Figure 10.3.6.1-1: Store group configurations at group management server

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.

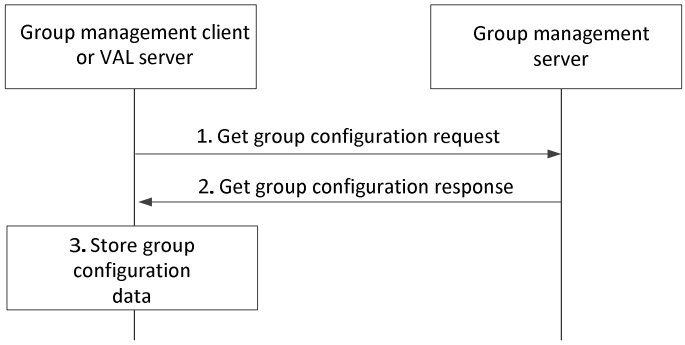

Figure 10.3.6.2-1: Retrieve group configurations

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 server.
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.

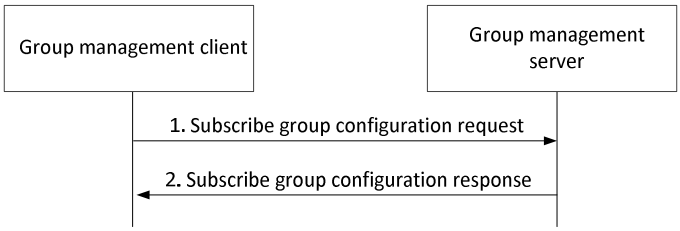

Figure 10.3.6.3-1: Subscription for group configurations

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.

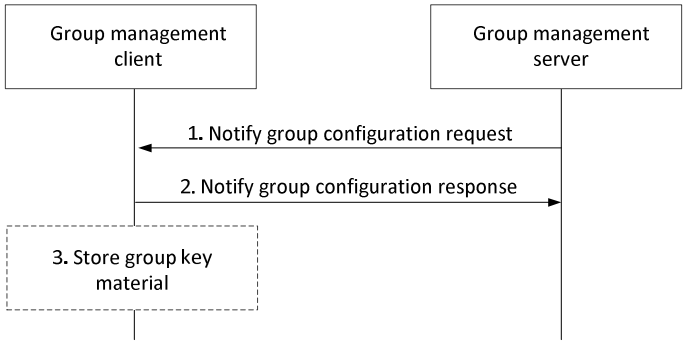

Figure 10.3.6.3-2: Notification of group configurations

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.

Figure 10.3.6.3-3 illustrates the high-level unsubscription for group configuration procedure used by a group management client to indicate to a group management server to stop sending notifications of group configuration data changes for groups for which it is authorized.

Pre-conditions:

- The group management client has an active subscription to group configuration data changes.

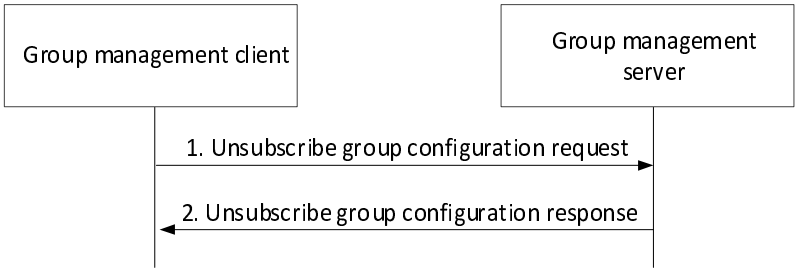

Figure 10.3.6.3-3: Unsubscription for group configurations

1. The group management client decides to unsubscribe notifications about group configuration data changes and sends an unsubscribe group configuration request to the group management server including the information specified in table 10.3.2.43-1.
2. The group management server shall check if the group management client is authorized to perform the unsubscribe operation. If so, the group management server cancels the subscription and provides an unsubscribe group configuration response to the group management including the information specified in table 10.3.2.44-1.

Figure 10.3.6.3-4 describes a procedure used by the group management client to update some parameters related to an existing subscription, for instance the notification target URI or the minimum time between consecutive notifications.

Pre-conditions:

- The group management client has an active subscription to group configuration data changes.

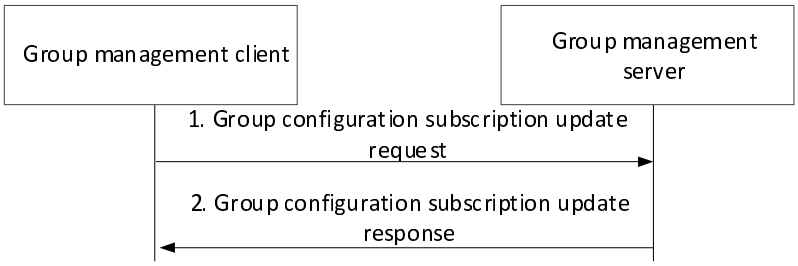

Figure 10.3.6.3-4: Update an existing subscription for group configurations

1. The group management client decides to update an active subscription and sends a group configuration subscription update request to the group management server including the information specified in table 10.3.2.45-1.

2. The group management server shall check if the group management client is authorized to update the subscription. If so, the group management server updates the subscription and provides a group configuration subscription update response to the group management including the information specified in table 10.3.2.46-1.

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 or VAL server is not aware of the users' or UE identities which will be combined to form the VAL group.

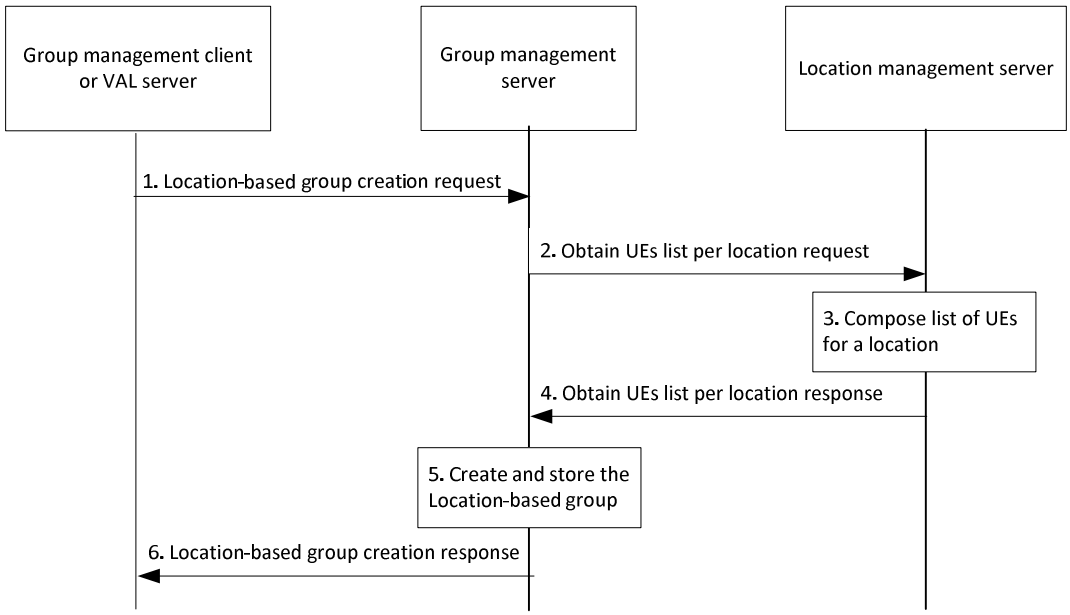

Figure 10.3.7-1: Location-based group creation

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 and the location criteria may be the VAL service area identified by the VAL service area ID.

2. The group management server requests the location management server for obtaining the users or UEs corresponding to the location information or the VAL service area identified by the VAL service area ID.

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. The location management server may include VAL service IDs associated with the list of users or UEs.

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. If VAL service ID list was received in step 1 as part of group formation criteria and not in step 4 for the composed list of users or UEs, the group management server shall retrieve the VAL service data from the configuration management server as described in clause 11.3.2.13 and form the group with relevant users or UEs.

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.

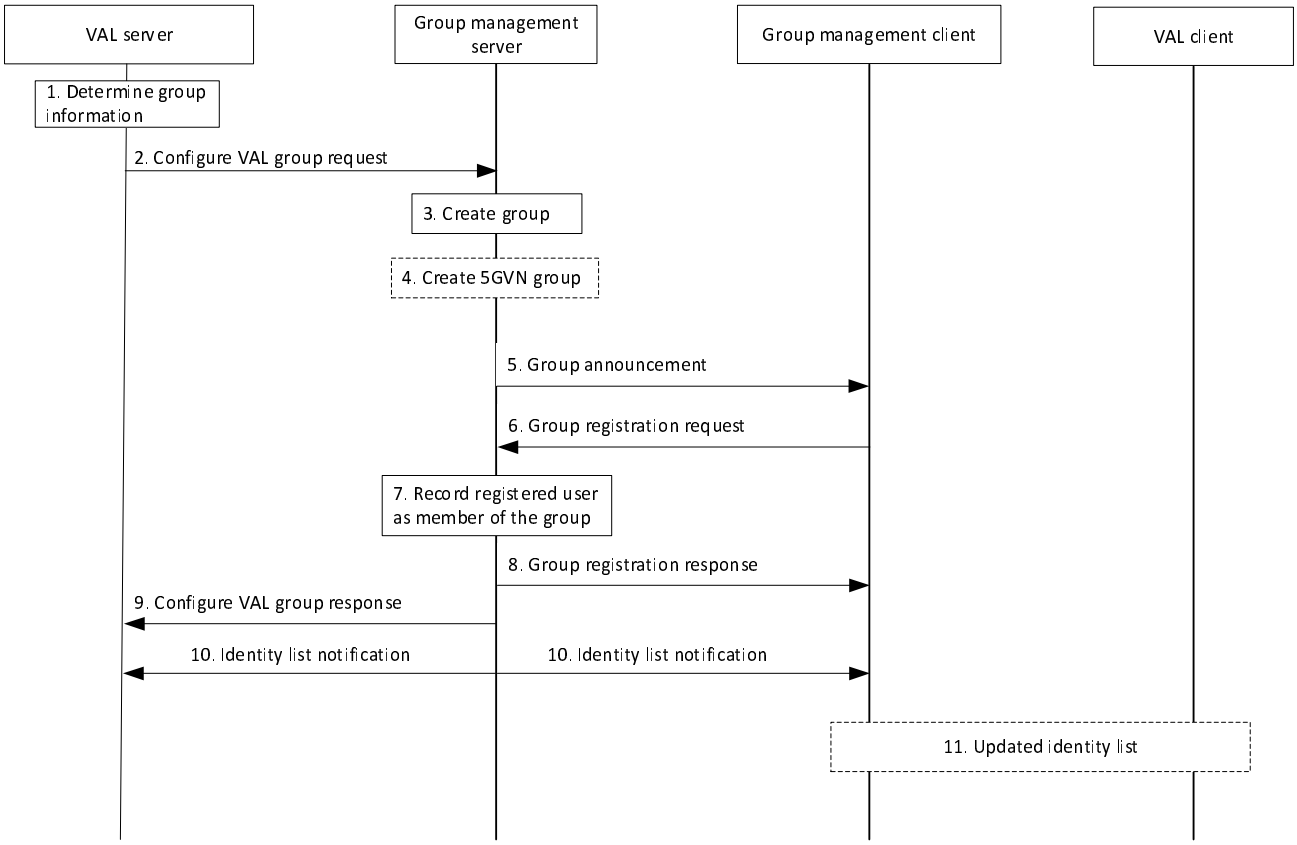

Figure 10.3.8.2-1: Procedure for establishing VAL group communication between the group management server and group management client1.

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.

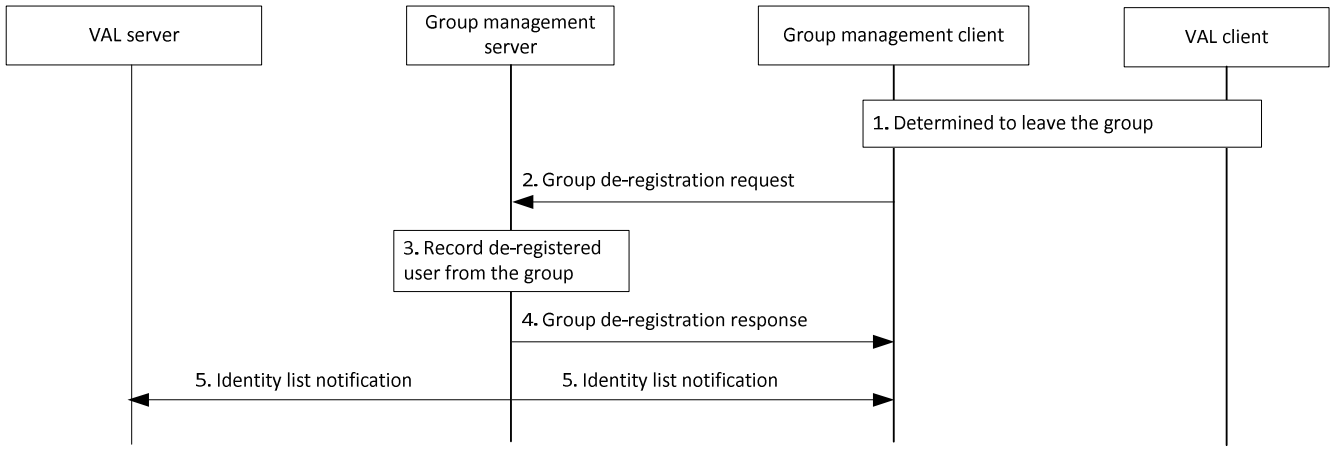

Figure 10.3.9.2-1: Procedure for group member leaving the group.

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.

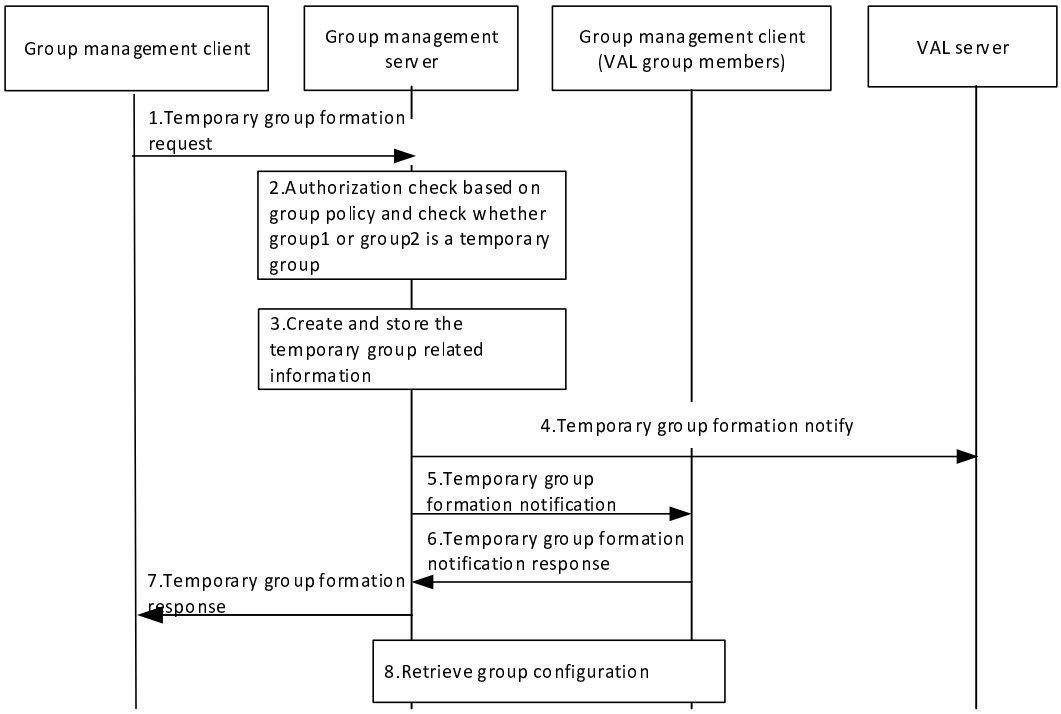

Figure 10.3.10.1-1: Temporary group formation within a VAL system

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.

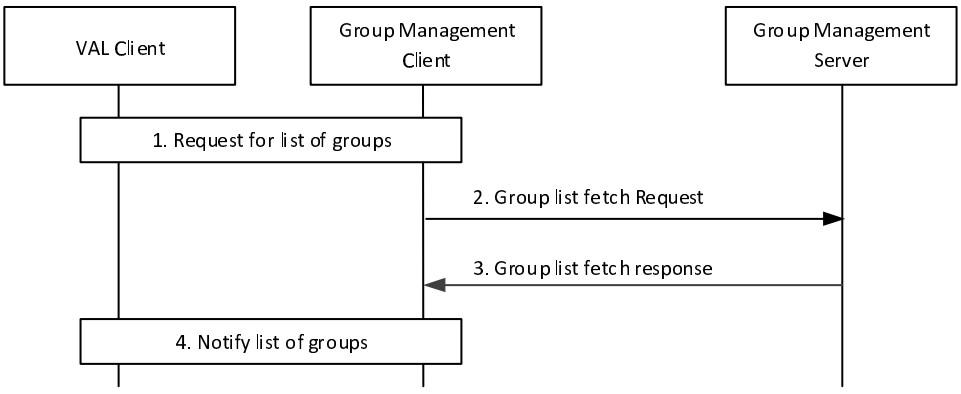

Figure 10.3.11-1: Group list fetch

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.

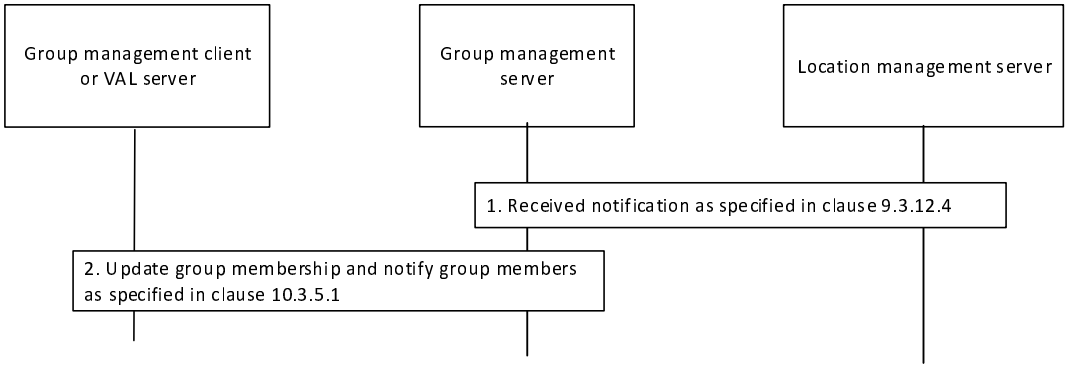

Figure 10.3.12-1: Location-based group update

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.

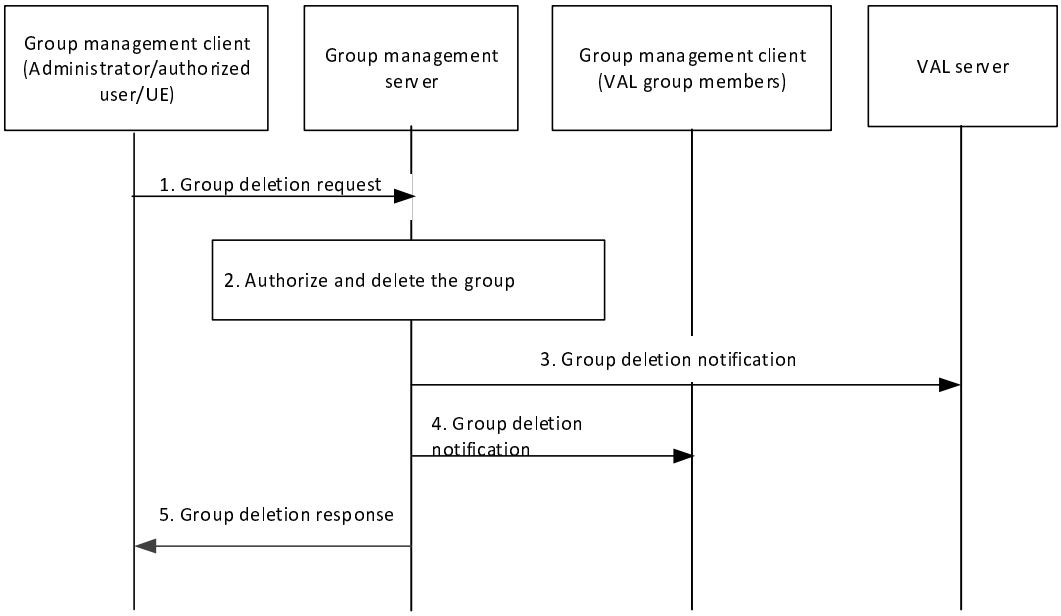

Figure 10.3.13-1: Group deletion

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
	Create_Group	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 the group creation, querying group information, obtaining stored group configuration, modify the group membership and configuration information on the group management server over GM-S and GM-Uu.

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.

10.4.2.5 Create_Group operation

API operation name: Create_Group

Description: Create the group.

Known Consumers: VAL server.

Inputs: See subclause 10.3.2.1, 10.3.2.26

Outputs: See subclause 10.3.2.2, 10.3.2.27

See subclause 10.3.3 and 10.3.8.2 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, 10.3.2.22

Outputs: See subclause 10.3.2.15, 10.3.2.23

See subclause 10.3.5.0 and 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 10.3.6.3 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.

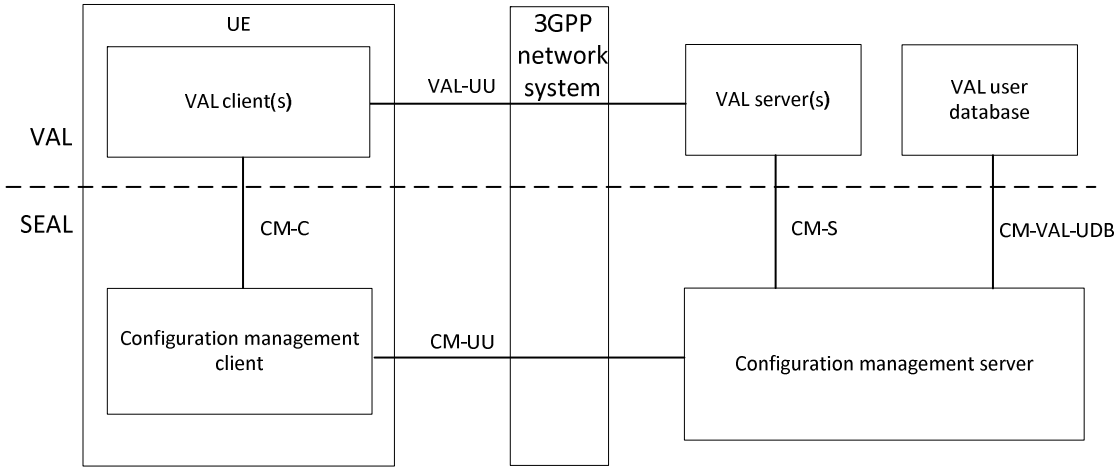

Figure 11.2.2-1: On-network functional model for configuration management

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.

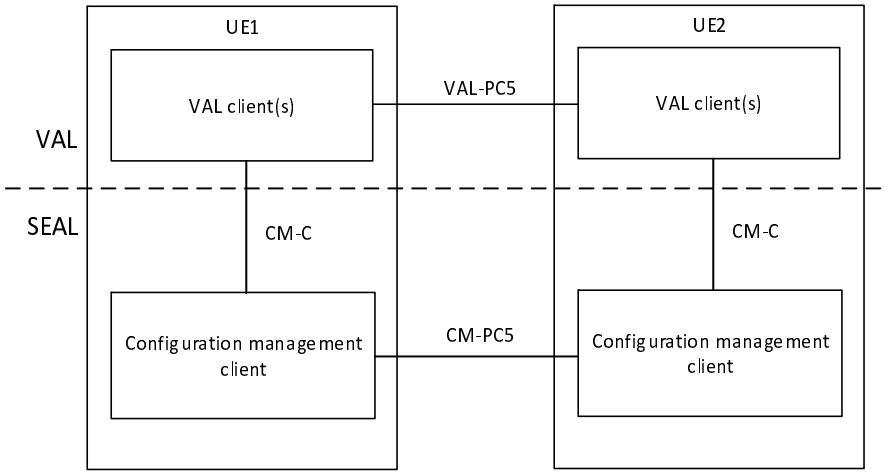

Figure 11.2.3-1: Off-network functional model for configuration management

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.

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;
- the configuration management server to obtain the user profile from the specific VAL user database for further configuration in the VAL UE.

- the configuration management server to update the user profile data in the specific VAL user database; and
- the configuration management server to delete the user profile data from the specific VAL user database

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 or VAL server 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 or VAL server 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 or VAL server.

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.

11.3.2.13 Get VAL service request

Table 11.3.2.13-1 describes the information flow get VAL service request from the consumer (e.g. group management) server to the configuration management server.

Table 11.3.2.13-1: Get VAL service request

Information element	Status	Description
Requester Identity	M	The identity of the entity performing the request.
Identity list	O (see NOTE)	The VAL user IDs or VAL UE IDs.
VAL service ID list	O (see NOTE)	The requested VAL service IDs for the identity list.
NOTE: At least one of Identity list or VAL service ID list shall be included. With both Identity list and VAL service ID in the request, the response only contains common VAL services (as requested) for the requested VAL users or VAL UEs.		

11.3.2.14 Get VAL service response

Table 11.3.2.14-1 describes the information flow get VAL service response from the configuration management server to the consumer (e.g. group management server).

Table 11.3.2.14-1: Get VAL service response

Information element	Status	Description
A list of VAL service data	O (see NOTE 1)	One or more VAL service data associated with the VAL user ID or VAL UE ID.
> Identity	M	The VAL user ID or VAL UE ID.
> VAL service IDs	M	The supported VAL service IDs.
> VAL service specific information	O (see NOTE 2)	Placeholder for VAL service specific information.
Result	M	Indicates the success or failure for the operation.
NOTE 1: It is valid when the Result information element indicates success. NOTE 2: The details of this information element are specified in VAL service specific specification and are out of scope of the present document.		

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.

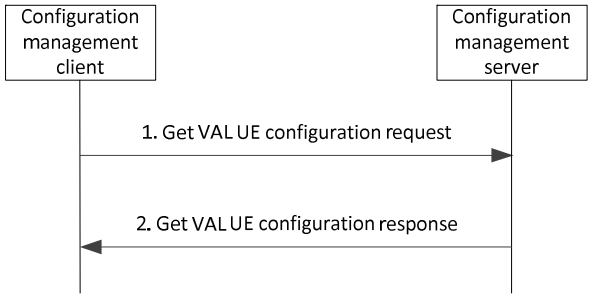

Figure 11.3.3.2-1: VAL UE obtains the configuration data

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.

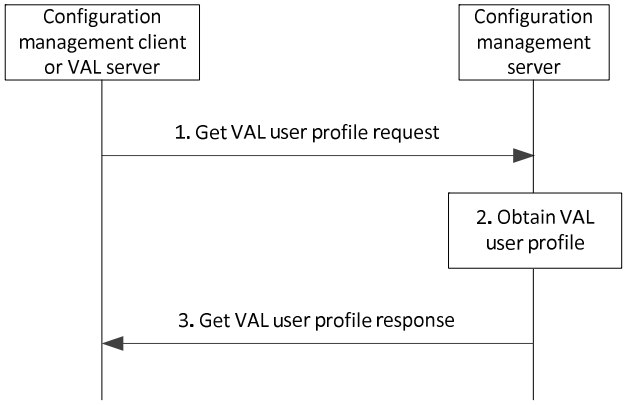

Figure 11.3.4.2.1-1: VAL user obtains the VAL user profile(s) from the network

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.

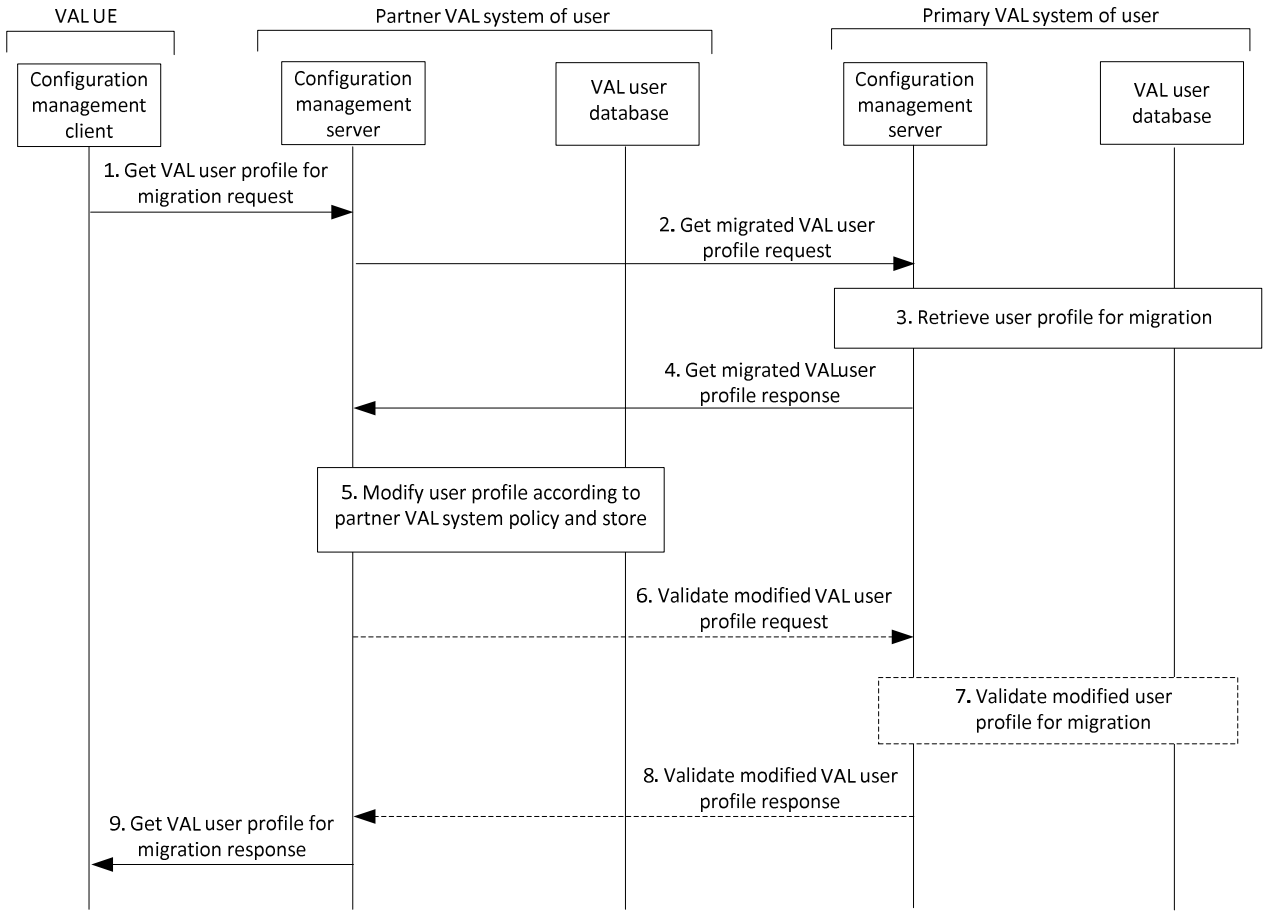

Figure 11.3.4.2.2-1: Retrieval of user profile in partner VAL system

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.

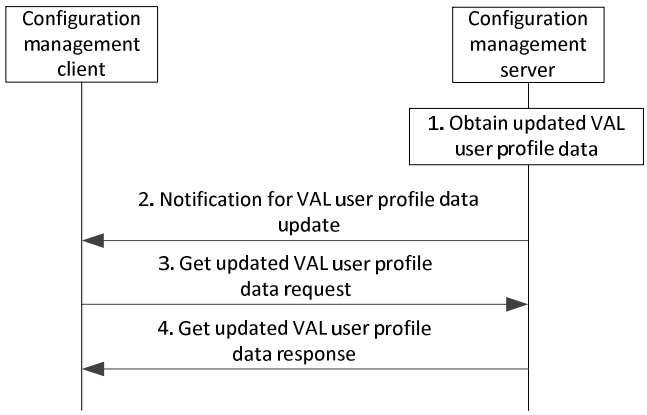

Figure 11.3.4.3-1: VAL user receives updated VAL user profile data from the network

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.

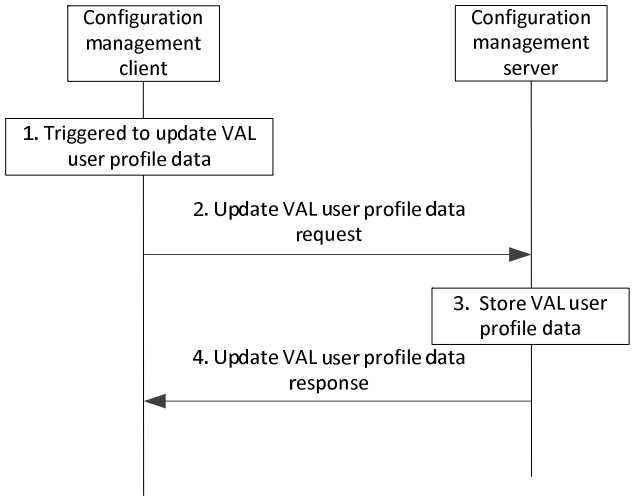

Figure 11.3.4.4-1: VAL user updates VAL user profile data to the network

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.

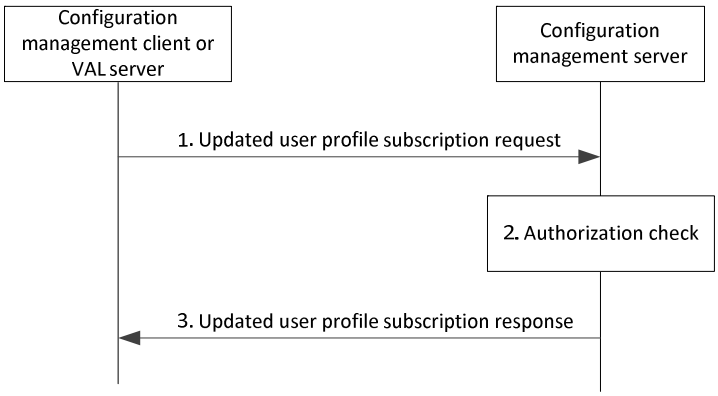

Figure 11.3.4.5-1: Updated user profile subscription procedure

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.

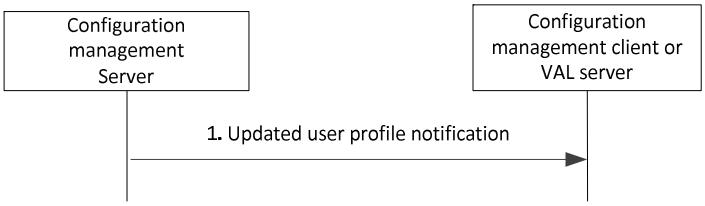

Figure 11.3.4.5-2: Updated user profile notification

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.

11.3.5 VAL service data

11.3.5.1 General

The VAL service data related procedures are described in the following subclauses.

11.3.5.2 Procedures

The procedure for consumer (e.g. group management server) obtaining the VAL service data is illustrated in figure 11.3.5.2-1.

Pre-conditions:

- The consumer has the secure access to the configuration management server.
- The configuration management server has VAL service data maintained for VAL UE or user.

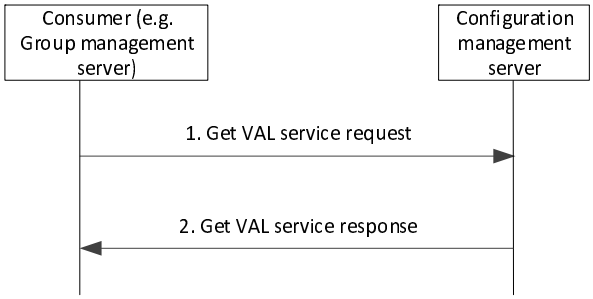

Figure 11.3.5.2-1: Obtains the VAL service data for VAL UE(s) or VAL user(s)

1. The consumer (e.g. group management server) sends a get VAL service request to the configuration management server for obtaining VAL service data. The request includes a list of VAL UE IDs or VAL user IDs and/or a VAL service ID list as service data retrieval filters.
2. The configuration server retrieves the VAL service data for the requested VAL UEs or users or VAL services and sends get VAL service response to the consumer (e.g. group management server) with the discovered list of VAL service data.

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	
SS_VALServiceData	Obtain_VAL_Service_Data	group management server	Request /Response

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.

11.4.4 SS_VALServiceData API

11.4.4.1 General

API description: This API enables the group management server to communicate with the configuration management server for obtaining VAL service data over SEAL-X.

11.4.4.2 Obtain_VAL_Service_Data operation

API operation name: Obtain_VAL_Service_Data

Description: Obtaining VAL service data.

Known Consumers: group management server.

Inputs: See subclause 11.3.2.13

Outputs: See subclause 11.3.2.14

See subclause 11.3.5.2 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.

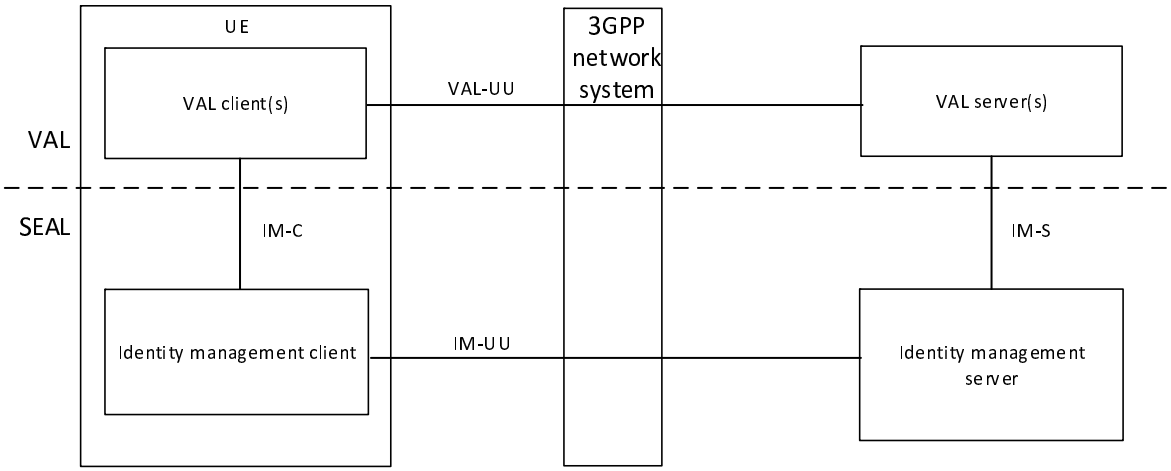

Figure 12.2.2-1: On-network functional model for identity management

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.

12.2.3 Off-network functional model description

Figure 12.2.3-1 illustrates the off-network functional model for identity management.

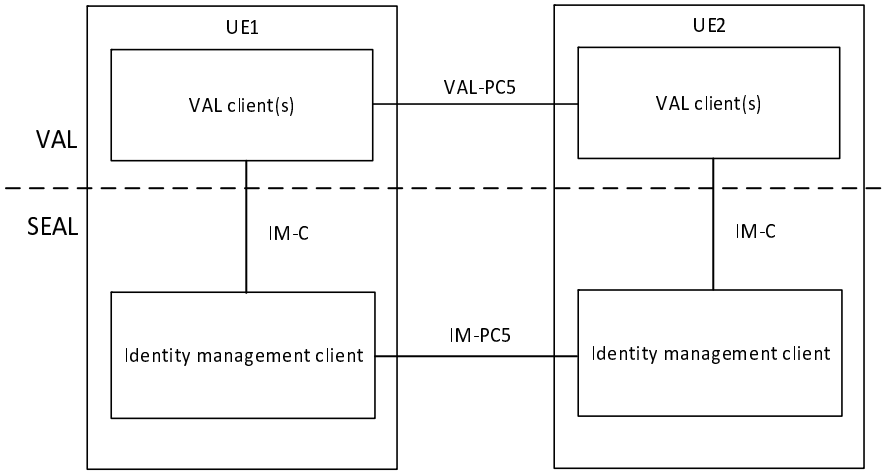

Figure 12.2.3-1: Off-network functional model for identity management

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.

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].

12.3.2.1 VAL server provisioning request

Table 12.3.2.1-1 describes the information flow from the VAL server to the identity management server for providing provisioning configuration.

Table 12.3.2.1-1: VAL server provisioning request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
List of VAL service specific information	M	Provides the list of VAL service specific information
> VAL service ID	M	Identify of the VAL service for which the configuration information is provided.
> identity list	M	Identify list of VAL users for the specific VAL service (i.e. VAL User IDs or VAL UE IDs)

12.3.2.2 VAL server provisioning response

Table 12.3.2.2-1 describes the information flow from the identity management server to the VAL server as a response for providing provisioning configuration.

Table 12.3.2.2-1: VAL server provisioning response

Information element	Status	Description
Result	M	Indicates success or failure of the request

12.3.2.3 Update VAL server provisioning request

Table 12.3.2.3-1 describes the information flow from the VAL server to the identity management server for updating provisioning configuration.

Table 12.3.2.3-1: Update VAL server provisioning request

Information element	Status	Description
Requester Identity (see NOTE)	M	The identity of the VAL server performing the request.
List of VAL service specific information	M	Provides the list of VAL service specific information
> VAL service ID	M	Identify of the VAL service for which the configuration information is to be updated.
> identity list	O	Identify list of VAL users for the specific VAL service (i.e. VAL User IDs or VAL UE IDs)
NOTE: The IE shall not be updated by the VAL server.		

12.3.2.4 Update VAL server provisioning response

Table 12.3.2.4-1 describes the information flow from the identity management server to the VAL server as a response for updating provisioning configuration.

Table 12.3.2.4-1: Update VAL server provisioning response

Information element	Status	Description
Result	M	Indicates success or failure of the request

12.3.2.5 Get VAL server provisioning request

Table 12.3.2.5-1 describes the information flow from the VAL server to the identity management server to get provisioning configuration.

Table 12.3.2.5-1: Get VAL server provisioning request

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

12.3.2.6 Get VAL server provisioning response

Table 12.3.2.6-1 describes the information flow from the identity management server to the VAL server as a response to get provisioning configuration.

Table 12.3.2.6-1: Get VAL server provisioning response

Information element	Status	Description
Result	M	Indicates success or failure of the request
List of VAL service specific information (NOTE 1)	M	Provides the list of VAL service specific information
> VAL service ID	M	Identify of the VAL service for which the configuration information is provided.
> identity list	M	Identify list of VAL users for the specific VAL service (i.e. VAL User IDs or VAL UE IDs)
NOTE 1: This IE is included only for success response		

12.3.2.7 Delete VAL server provisioning request

Table 12.3.2.7-1 describes the information flow from the VAL server to the identity management server for deleting provisioning configuration.

Table 12.3.2.7-1: Delete VAL server provisioning request

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

12.3.2.8 Delete VAL server provisioning response

Table 12.3.2.8-1 describes the information flow from the identity management server to the VAL server as a response for deleting provisioning configuration.

Table 12.3.2.8-1: Delete VAL server provisioning response

Information element	Status	Description
Result	M	Indicates success or failure of the request

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.

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.

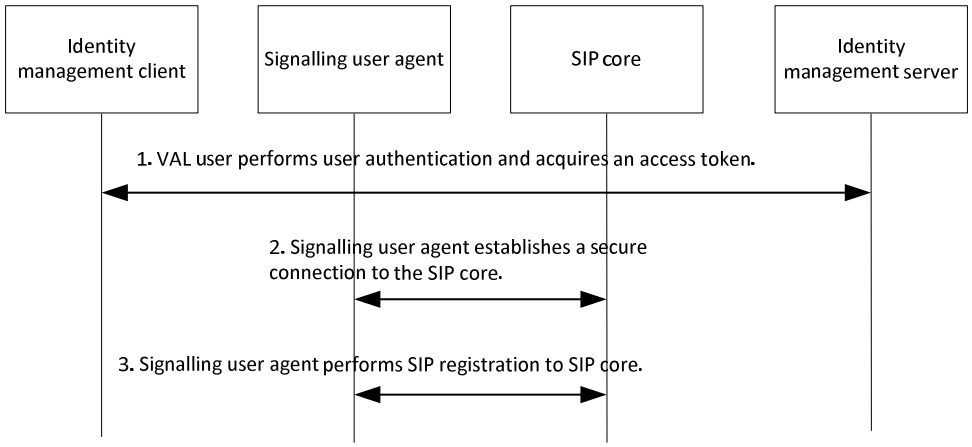

Figure 12.3.3.2-1: VAL user authentication and registration with Primary VAL system, single domain

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].

12.3.4 VAL server provisioning for identity management service

12.3.4.1 General

The high level procedure for VAL server to provision required information to SEAL identity management server in order to support VAL user authentication is described in the following subclause.

12.3.4.2 Procedure

The procedure for VAL server to provision required information to SEAL identity management server in order to support VAL user authentication is illustrated in figure 12.3.4.2-1.

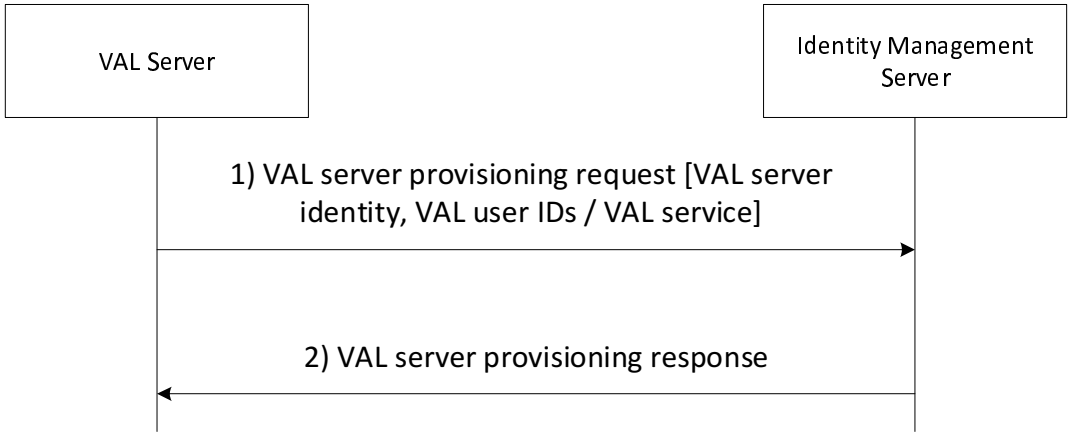

Figure 12.3.4.2-1: VAL Server provisioning to SEAL Identity Management Server

1. The VAL server sends a request message to identity management server to provision required information. The request message includes identity of the VAL server, security credentials of the VAL server, and service provider specific information like identity list per VAL service.

2. Upon receiving the request, the identity management server authorizes the request based on the security credentials provided in the request and considering the service level agreement between VAL service provider and SEAL service provider. If VAL server is authorized to use the SEAL service, then the identity management server stores the details about the VAL server including the list of VAL user IDs per VAL service. The identity management server sends the response message to the VAL server.

Editor's note: Whether the VAL server registers with Identity Management Server is FFS.

12.3.4.3 Update VAL server provisioning procedure

The procedure for VAL server to update the required provisioning information to SEAL identity management server is illustrated in figure 12.3.4.3-1.

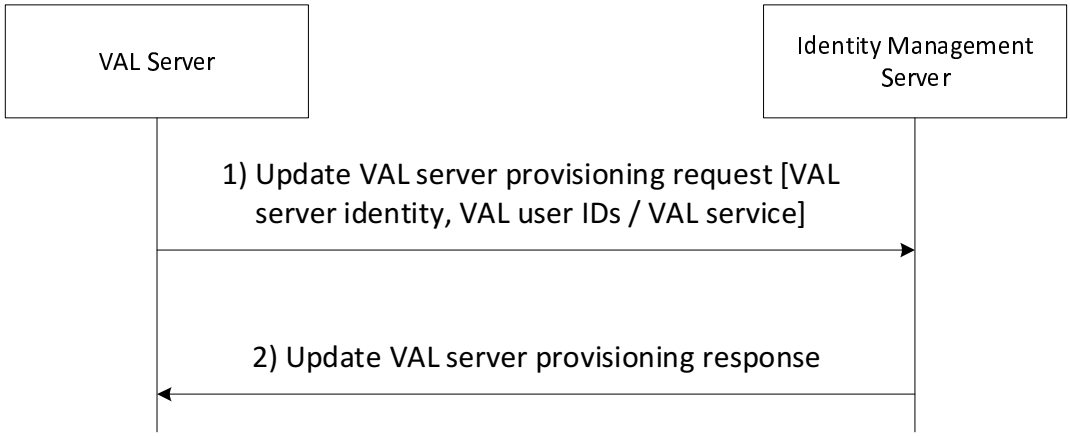

Figure 12.3.4.3-1: VAL Server updating provisioning to SEAL Identity Management Server

1. The VAL server sends a request message to identity management server to update the required provisioning information. The request message includes identity of the VAL server, security credentials of the VAL server, and service provider specific information like identity list per VAL service.

2. Upon receiving the request, the identity management server authorizes the request based on the security credentials provided in the request and considering the service level agreement between VAL service provider and SEAL service provider. If VAL server is authorized to use the SEAL service and if there exists provisioning information, then the identity management server updates the details about the VAL server for the provided VAL service IDs, including the list of VAL user IDs per VAL service. The provisioning information corresponding to a VAL server ID can be updated to add, remove or update VAL service IDs and its related information. The identity management server sends the response message to the VAL server.

12.3.4.4 Get VAL server provisioning procedure

The procedure for VAL server to get the required provisioning information to SEAL identity management server is illustrated in figure 12.3.4.4-1.

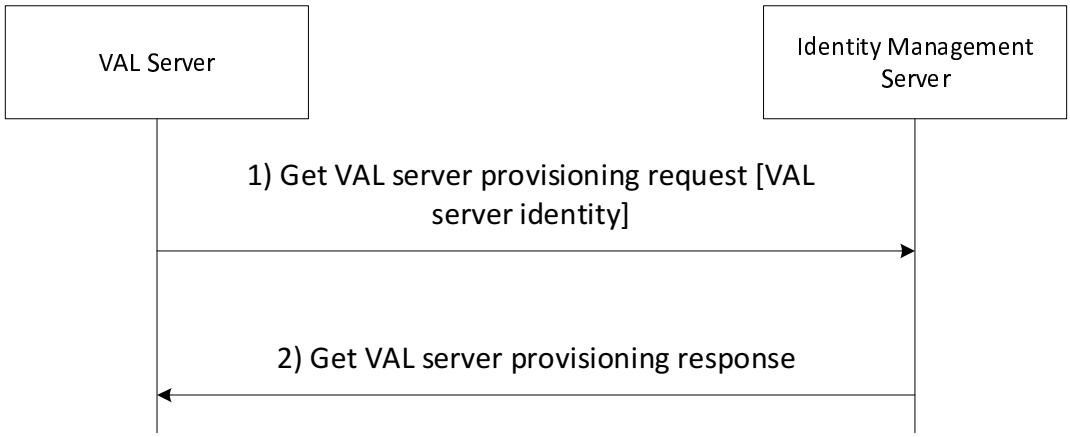

Figure 12.3.4.4-1: VAL Server requesting provisioning information to SEAL Identity Management Server

1. The VAL server sends a request message to identity management server to get the required provisioning information. The request message includes identity of the VAL server whose provisioning information is requested.

2. Upon receiving the request, the identity management server authorizes the request based on the security credentials provided in the request and considering the service level agreement between VAL service provider and SEAL service provider. If VAL server is authorized to use the SEAL service and if there exists provisioning information, then the identity management server sends success response including the list of VAL user IDs per VAL service. Otherwise, the identity management server sends failure response message to the VAL server.

12.3.4.5 Delete VAL server provisioning procedure

The procedure for VAL server to delete the provisioning information to SEAL identity management server is illustrated in figure 12.3.4.5-1.

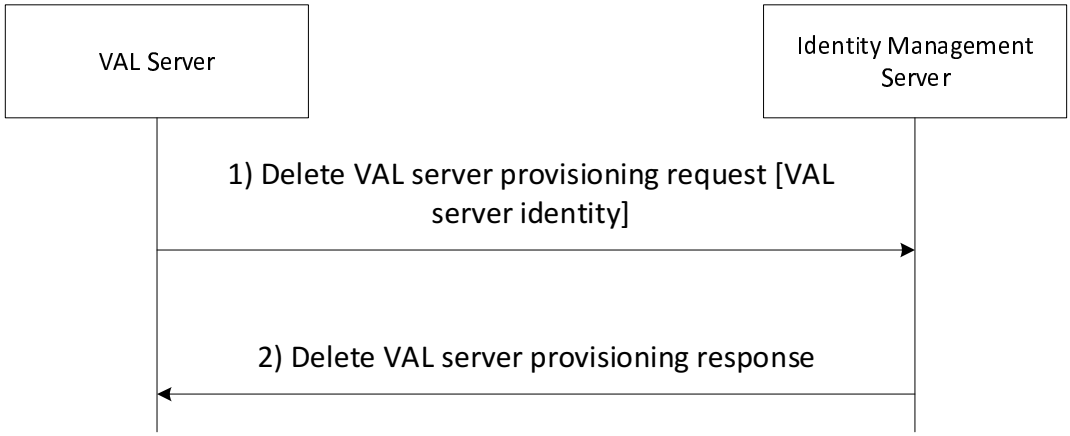

Figure 12.3.4.5-1: VAL Server deleting provisioning information to SEAL Identity Management Server

1. The VAL server sends a request message to identity management server to delete the provisioning information. The request message includes identity of the VAL server.

2. Upon receiving the request, the identity management server authorizes the request based on the security credentials provided in the request and considering the service level agreement between VAL service provider and SEAL service provider. If VAL server is authorized to use the SEAL service and if there exists provisioning information, then the identity management server deletes the provisioning information for given VAL server ID

and sends success response. Otherwise, the identity management server sends failure response message to the VAL server.

12.4 SEAL APIs for identity management

12.4.1 General

Table 12.4.1-1 illustrates the SEAL APIs for identity management.

Table 12.4.1-1: List of SEAL APIs for identity management

API Name	API Operations	Known Consumer(s)	Communication Type
SS_IdmParameterProvisioning	Provide_Configuration	VAL server	Request /Response
	Update_Configuration		
	Get_Configuration		
	Delete_Configuration		

12.4.2 Void

12.4.2.1 Void

12.4.2.2 Void

12.4.3 SS_IdmParameterProvisioning API

12.4.3.1 General

API description: This API enables the VAL server to provision configuration for the VAL service to the SEAL IM-S.

12.4.3.2 Provide_Configuration operation

API operation name: Provide_Configuration

Description: Provisioning of VAL service configuration to IM-S.

Known Consumers: VAL server.

Inputs: See subclause 12.3.2.1

Outputs: See subclause 12.3.2.2

See subclause 12.3.4.2 for the details of usage of this API operation.

12.4.3.3 Update_Configuration operation

API operation name: Update_Configuration

Description: Updating the provisioning of VAL service configuration to IM-S.

Known Consumers: VAL server.

Inputs: See subclause 12.3.2.3

Outputs: See subclause 12.3.2.4

See subclause 12.3.4.3 for the details of usage of this API operation.

12.4.3.4 Get_Configuration operation

API operation name: Get_Configuration

Description: Get provisioning of VAL service configuration from IM-S.

Known Consumers: VAL server.

Inputs: See subclause 12.3.2.5

Outputs: See subclause 12.3.2.6

See subclause 12.3.4.4 for the details of usage of this API operation.

12.4.3.5 Delete_Configuration operation

API operation name: Delete_Configuration

Description: Deleting the provisioning of VAL service configuration on IM-S.

Known Consumers: VAL server.

Inputs: See subclause 12.3.2.7

Outputs: See subclause 12.3.2.8

See subclause 12.3.4.5 for the details of usage of this API operation.

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.

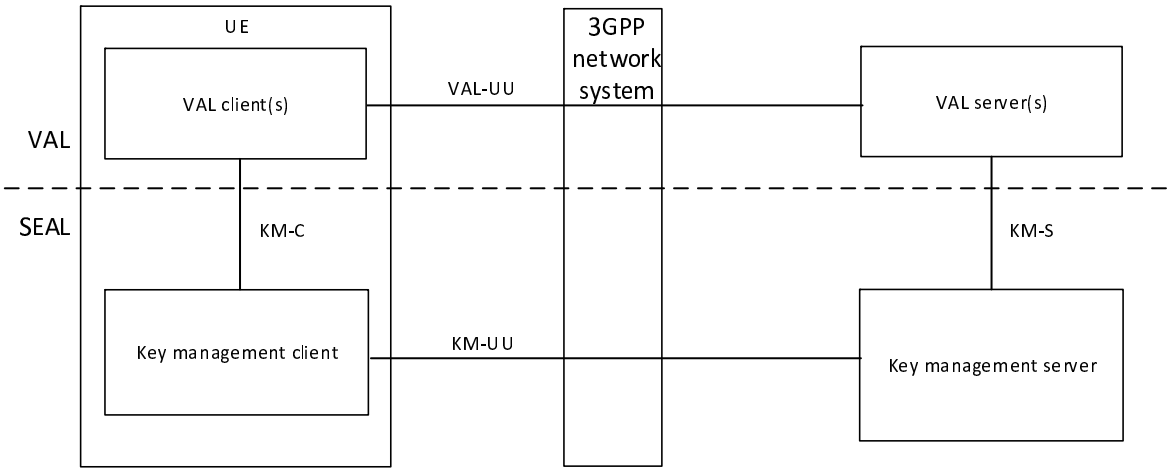

Figure 13.2.2-1: On-network functional model for key management

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.

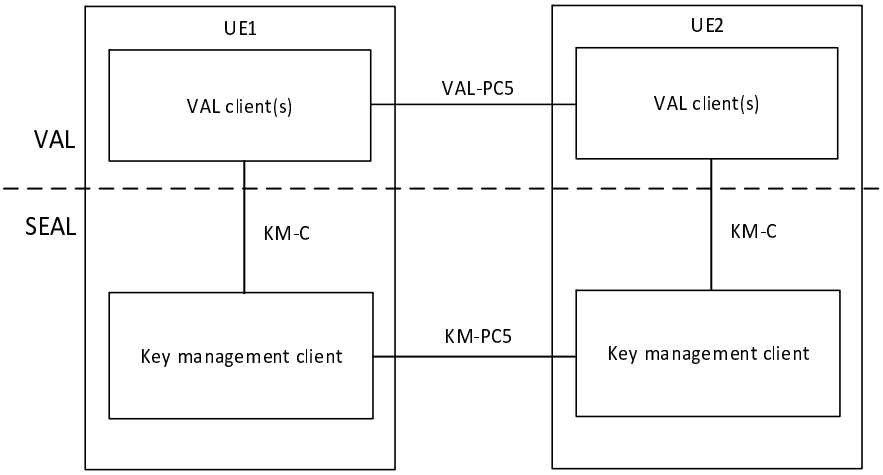

Figure 13.2.3-1: Off-network functional model for key management

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.

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].

13.3.1 Information flows

13.3.1.1 void

13.3.1.2 void

13.3.2 VAL server provisioning for key management service

13.3.2.1 General

The high level procedure for VAL server to provision required information to SEAL key management server in order to provide the format and content of a key management record is described in clause 5.8 of 3GPP TS 33.434 [29].

13.3.2.2 void

13.4 SEAL APIs for key management

13.4.1 General

Table 13.4.1-1 illustrates the SEAL APIs for key management.

Table 13.4.1-1: List of SEAL APIs for key management

API Name	API Operations	Known Consumer(s)	Communication Type
SS_KmParameterProvisioning	Provide_Configuration	VAL server	Request /Response

The other 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

13.4.3 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.

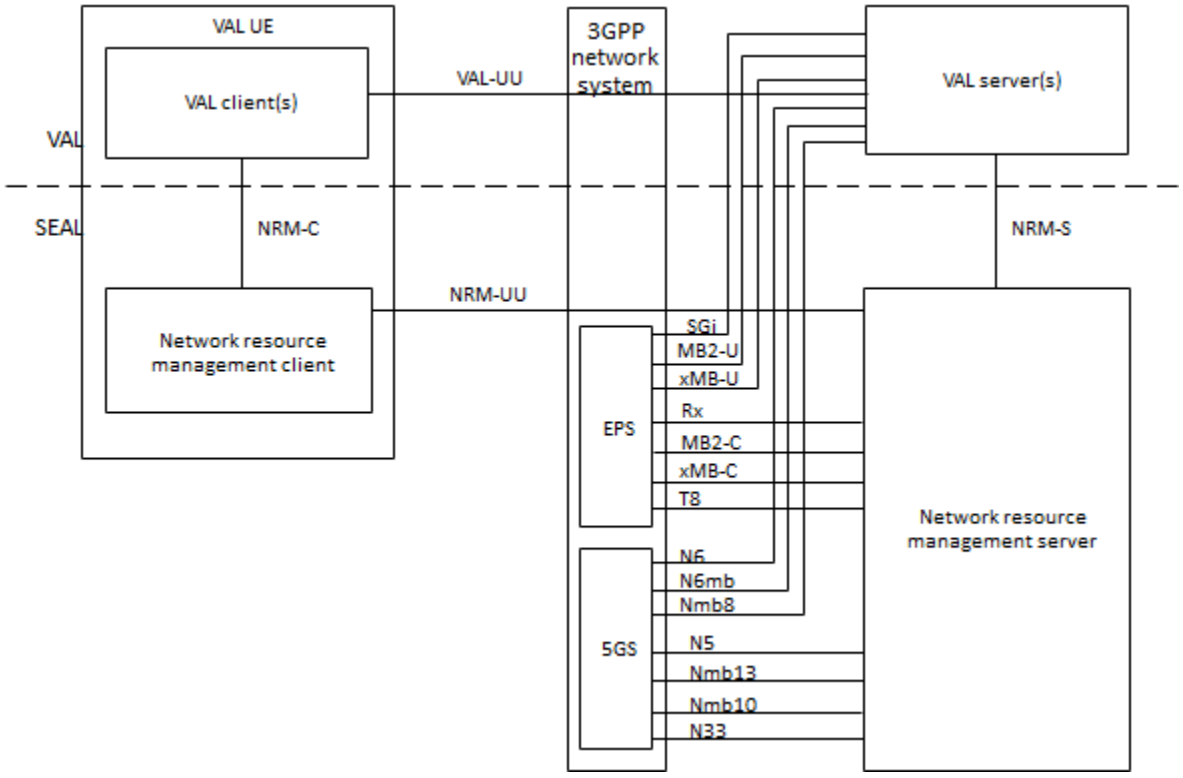

Figure 14.2.2.1-1: On-network functional model for network resource management

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 obtains and controls the multicast/broadcast resource from the underlaying 3GPP network system by communicating with the BM-SC via MB2-C and xMB-C reference points towards LTE eMBMS and with the 5G MBS control plane functions via Nmb13, Nmb10 or N33 towards the 5GS. 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.

Figure 14.2.2.1-2 exhibits the service-based interfaces for providing and consuming group management services. The network resource management server could provide service to VAL server and network resource management client through interface Snrm.

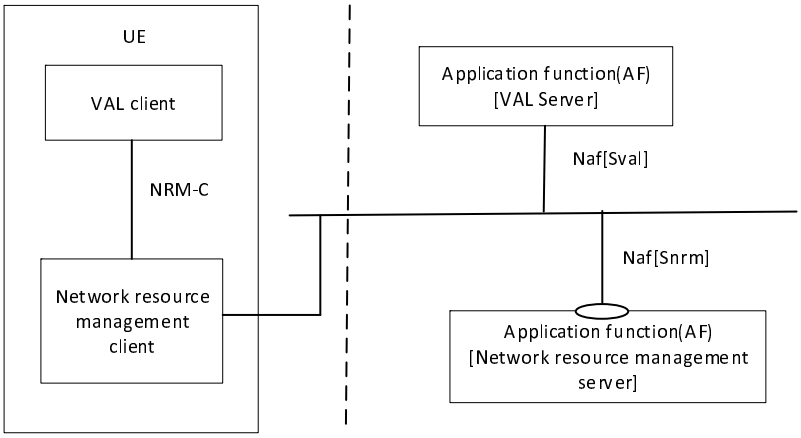

Figure 14.2.2.1-2: Architecture for network resource management – Service based representation

Figure 14.2.2.1-3 illustrates the service-based representation for utilization of the 5GS network services based on the 5GS SBA specified in 3GPP TS 23.501 [10].

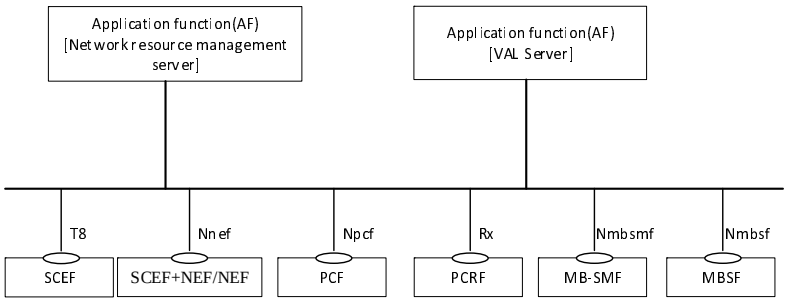

Figure 14.2.2.1-3: Architecture for network resource management utilizing the 5GS network services based on the 5GS SBA – Service based representation

Figure 14.2.2.1-4 illustrates the service-based representation for utilization of the Core Network northbound APIs via CAPIF.

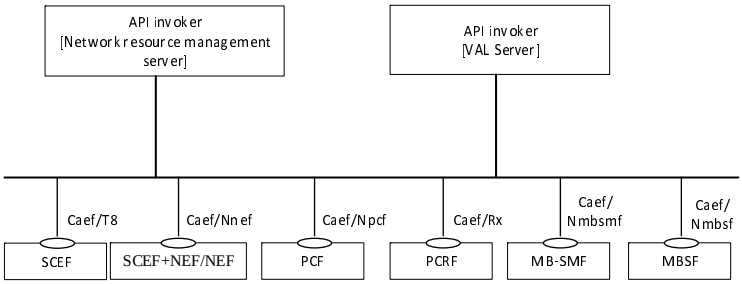

Figure 14.2.2.1-4: Utilization of Core Network Northbound APIs via CAPIF – service based representation

The Network resource management server and VAL server act as authorized API invoker to consume services from the Core Network northbound API entities like NEF which act as API Exposing Function as specified in 3GPP TS 23.222 [6].

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.

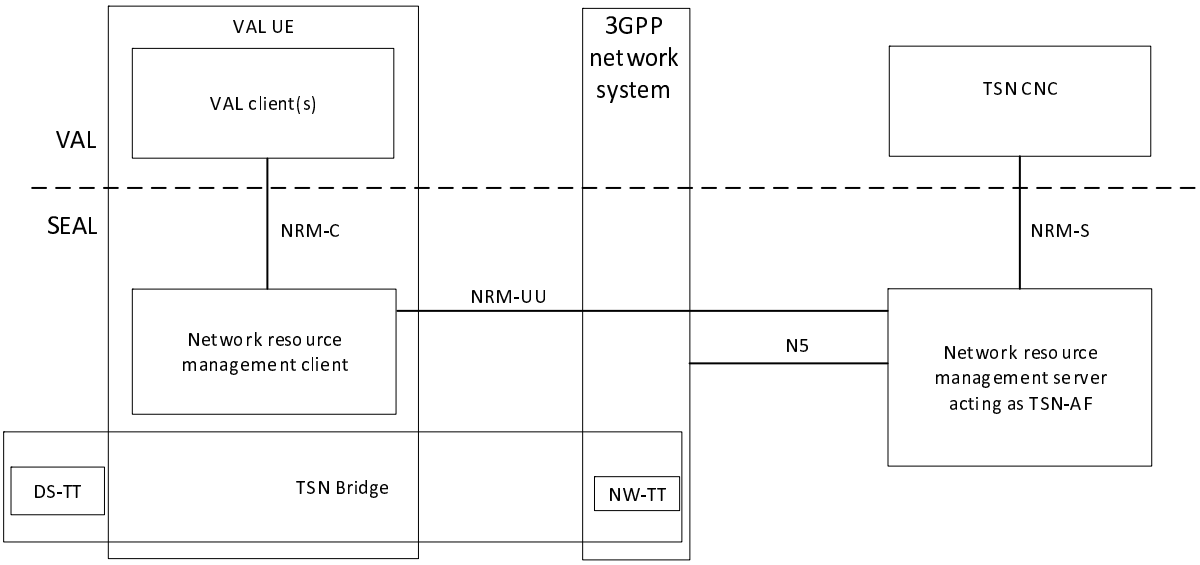

Figure 14.2.2.2-1: On-network functional model for network resource management for TSN

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 N84 reference point to configure the 5G QoS and TSCAI parameters in the 5GS.

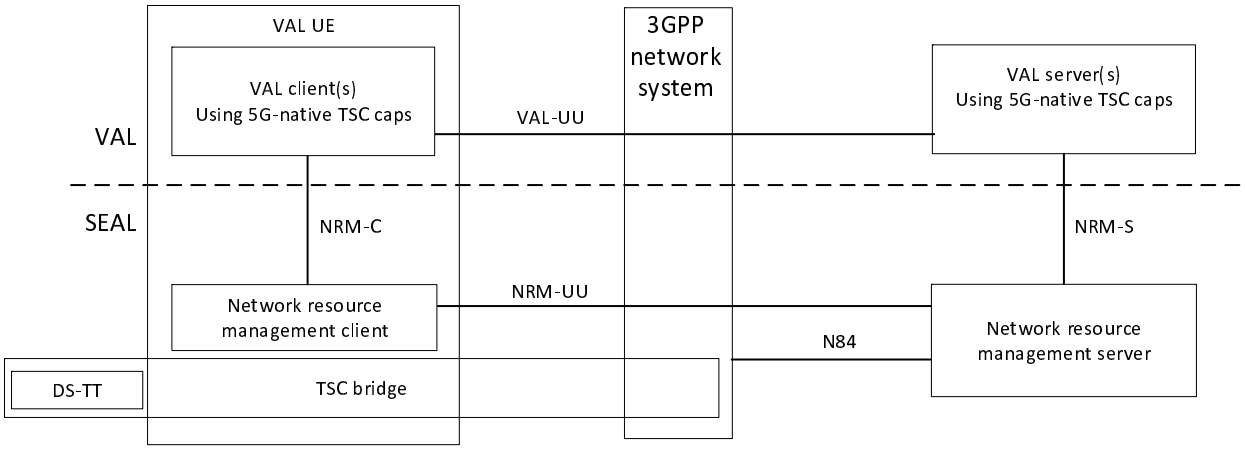

Figure 14.2.2.3-1: On-network functional model for network resource management for 5G TSC

14.2.3 Off-network functional model description

Figure 14.2.3-1 illustrates the off-network functional model for network resource management.

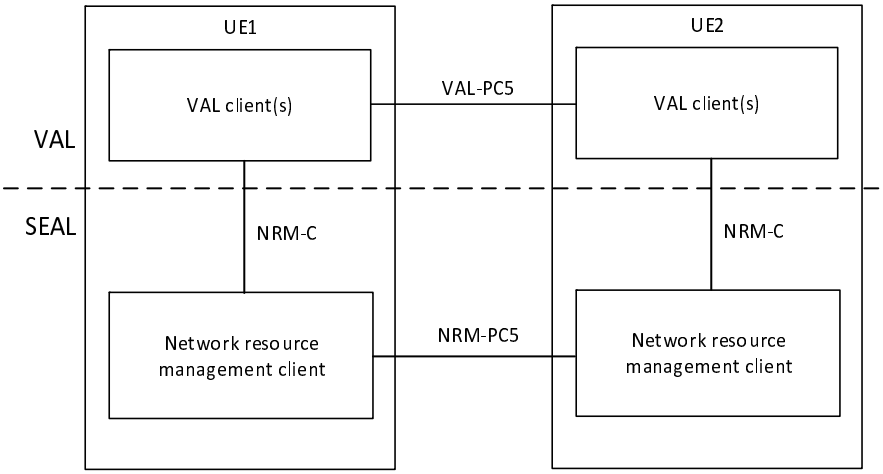

Figure 14.2.3-1: Off-network functional model for network resource management

The network resource management client of the UE1 communicates with the network resource management client of the UE2 over the NRM-PC5 reference point.

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].

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.

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.

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].

14.2.5.12 Nmb13

The reference point Nmb13 supports the interactions between the network resource management server and the MB-SMF is specified in 3GPP TS 23.247 [39].

14.2.5.13 Nmb10

The reference point Nmb10 supports the interactions between the network resource management server and the MBSF is specified in 3GPP TS 23.247 [39].

14.2.5.14 N6mb

The reference point N6mb supports the interactions between the VAL server and the MB-UPF is specified in 3GPP TS 23.247 [39].

14.2.5.15 Nmb8

The reference point Nmb8 supports the interactions between the VAL server and the MBSTF is specified in 3GPP TS 23.247 [39].

14.2.5.16 N6

The reference point N6 supports the interactions between the VAL server and the UPF 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.
MBS service area	O	Indicates the MBS service area where the delivery mode is applied
List of VAL UE IDs	O (see NOTE)	The list of UEs where the unicast mode is applied
NOTE: This information element is only applicable when the delivery mode is unicast mode.		

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 or VAL Group ID	M	List of VAL UEs or the group of VAL UEs for whom the end-to-end QoS management occurs
>VAL UE/user ID	M	Identity of the VAL UE
> IP address	O	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 Subscription status is success and 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 NOTE 4)	List of VAL UEs whose QoS monitoring data is requested.
VAL group ID	O (see NOTE 1, NOTE 4)	The group ID used for the VAL group for which QoS monitoring data is requested.
List of VAL stream IDs	O (see NOTE 1, NOTE 4)	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 (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 (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: If provided, only one of these information elements shall be present. NOTE 4: When used by the Update_Unicast_QoS_Monitoring_Subscription operation, the same information element with identical content shall be present as in the associated Subscribe_Unicast_QoS_Monitoring operation.

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 as described in IEEE 802.1Qcc [35] 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.		

14.3.2.35 Application connectivity request

Table 14.3.2.35-1 describes the information flow for application connectivity request from a NRM client to the NRM server.

Table 14.3.2.35-1: Application connectivity request

Information element	Status	Description
Source VAL UE ID	M	Identifier of the requestor VAL UE
Source IP address	M	IP address of the requestor VAL UE
VAL service ID	M	Identifier of the VAL service
List of destination VAL UE IDs	M	Identifiers of the destination VAL UEs
Application service requirements	M	Details of service requirements
>Packet size (see NOTE)	O	Size of the packet to be transmitted.
>Packet transmission interval (see NOTE)	O	Intervals at which the packet is to be transmitted
>Packet E2E latency (see NOTE)	O	E2E Latency for packet transmission
>Packet error KPI (see NOTE)	O	The KPIs related to packet error (e.g. allowed packet loss rate, packet loss amount, packet error rate)
>Bitrate (see NOTE)	O	The bitrate required
Application connectivity context	O	Application connectivity context of the requester, used for determining the destination and/or resource parameters. If this IE is included, at least one of the information elements in Table 14.3.2.35-2 shall be provided.
NOTE: At least one of information elements of the application service requirements shall be included.		

Table 14.3.2.35-2: Application connectivity context

Information element	Status	Description
Location	O	Location information of the client. The element may also indicate whether network-determined location is to be used instead.
Speed	O	Speed information for the client.
Direction	O	Direction information for the client.

14.3.2.36 Application connectivity response

Table 14.3.2.36-1 describes the information flow for application connectivity response from the NRM server to the NRM client.

Table 14.3.2.36-1: Application connectivity response

Information element	Status	Description
Result	M	Result from the NRM server in response to request indicating success or failure for accepting the request.
Cause	O	The cause of failure, if the result indicates failure.

14.3.2.37 Application connectivity notification

Table 14.3.2.37-1 describes the information flow for application connectivity notification from the NRM server to the NRM client.

Table 14.3.2.37-1: Application connectivity notification

Information element	Status	Description
Session information	M	Session information for the established connectivity for application communication
VAL service ID	M	Identifier of the VAL service
Requestor VAL UE ID	M	The identity of the source VAL UE requesting the connectivity
List of accepted destination VAL UE IDs (see NOTE)	O	The list of destination VAL UEs which are accepted for the connectivity established for the application service communication
NOTE: The List of accepted destination VAL UE IDs IE shall be included when the application connectivity notification is sent to the initiator of the application connectivity request.		

14.3.2.38 Unicast QoS monitoring subscription update request

The information flow from the VAL server to the network resource management server for unicast QoS monitoring subscription update request has the same content as unicast QoS monitoring subscription request specified in clause 14.3.2.20.

14.3.2.39 Unicast QoS monitoring subscription update response

Table 14.3.2.39-1 describes the information flow from the network resource management server to the VAL server for unicast QoS montoring subscription update response.

Table 14.3.2.39-1: Unicast QoS monitoring subscription update response

Information element	Status	Description
Update status	M	It indicates the subscription update result

14.3.2.40 Multicast/broadcast resource request

Table 14.3.2.40-1 describes the information flow for the multicast/broadcast resource request from VAL server to NRM server.

Table 14.3.2.40-1: Multicast/broadcast resource request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL group ID	O (NOTE 3)	The identity of the group that the multicast/broadcast resource is requested for.
VAL UE ID List	O (NOTE 3)	The list of VAL UE ID that the multicast/broadcast resource is requested for.
Session announcement mode	M	Indicates whether the session announcement is sent by NRM server or by the VAL server
Service requirement description	M	Indicates the service characteristics, e.g., Media type, Media format, bandwidth requirements, flow description, Application Identifier, Priority indicator, emergency indicator Application service provider.
Multicast/Broadcast area information	O	Indicate the area where the multicast/broadcast resource is requested for
Endpoint information	M	Information of the endpoint of the VAL server to which the user plane notifications have to be sent.
Network system indicator	O	Indicate if the multicast/broadcast resrouce is required from 5GS, EPS, or both
Local MBMS information (NOTE 1, NOTE 2)	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 (NOTE 1, NOTE 2)	O	Indicates whether to request the NRM server to use Local MBMS information.
NOTE 1: 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. NOTE 2: This information element is only applicable when EPS is specified in the network system indicator IE. NOTE 3: Either of the IEs shall be present.		

14.3.2.41 Multicast/broadcast resource response

Table 14.3.2.41-1 describes the information flow for the multicast/broadcast resource response from NRM server to VAL server.

Table 14.3.2.41-1: Multicast/broadcast resource response

Information element	Status	Description
Result	M	The result indicates success or failure of the multicast/broadcast resource request operation.
Identity of the multicast/broadcast resource	O (NOTE 1)	The identity of the multicast/broadcast MBS session, or/and the identity of the MBMS bearer.
User plane address	M (NOTE 2)	User plane IP address(es) and port for VAL to deliver the DL packet
Session description information	O (NOTE 2)	Indicates Multicast/broadcast related configuration information as defined in 3GPP TS 26.346 [28] (e.g. radio frequency and MBMS Service Area Identities) or/and 3GPP TS 23.247 [39] (e.g. MBS FSA ID(s), Area Session ID)
NOTE 1: This IE may not be required if the session 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 shall not present.		

14.3.2.42 Multicast/broadcast resource update request

Table 14.3.2.42-1 describes the information flow for the multicast/broadcast resource update request from VAL server to NRM server.

Table 14.3.2.42-1: Multicast/broadcast resource update request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
Identity of the multicast/broadcast resource	M	Identity of the multicast/broadcast resource to be updated.
Service requirement description	O (NOTE 3)	Indicates the service characteristics, e.g., Media type, Media format, bandwidth requirements, flow description, Application Identifier, Priority indicator, emergency indicator Application service provider.
Multicast/Broadcast area information	O(NOTE 3)	Indicate the area where the multicast/broadcast resource is requested for
Local MBMS information (NOTE 1, NOTE 2)	O(NOTE 3)	
> 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 (NOTE 1, NOTE 2)	O	Indicates whether to request the NRM server to use Local MBMS information.
NOTE 1: 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. NOTE 2: This information element is only applicable when EPS is specified in the network system indicator IE. NOTE 3: At least one of those IEs shall be present.		

14.3.2.43 Multicast/broadcast resource update response

Table 14.3.2.43-1 describes the information flow for the Multicast/broadcast resource update response from NRM server to VAL server.

Table 14.3.2.43-1: Multicast/broadcast resource update response

Information element	Status	Description
Result	M	The result indicates success or failure of the multicast/broadcast resource update request operation.
Identity of the multicast/broadcast resource	M (NOTE 1)	The identity of the multicast/broadcast MBS session, or/and the identity of the MBMS bearer to be updated.
New Identity of the multicast/broadcast resource	O	The identity of the new multicast/broadcast MBS session created during update.
User plane address	O	Additional user plane IP address(es) and port for VAL to deliver the DL packet
Session description information	O (NOTE 2)	Indicates Multicast/broadcast related configuration information as defined in 3GPP TS 26.346 [28] (e.g. radio frequency and MBMS Service Area Identities) or/and 3GPP TS 23.247 [39] (e.g. MBS FSA ID(s), Area Session ID, service requirements)
NOTE 1: This IE may not be required if the session 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 shall not present.		

14.3.2.44 Multicast/broadcast resource delete request

Table 14.3.2.44-1 describes the information flow for the multicast/broadcast resource delete request from VAL server to NRM server.

Table 14.3.2.44-1: Multicast/broadcast resource delete request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
Identity of the multicast/broadcast resource	M	Identity of the multicast/broadcast resource, i.e., the MBS session ID for 5G MBS, TMGI for 4G MBMS, or both

14.3.2.45 Multicast/broadcast resource delete response

Table 14.3.2.45-1 describes the information flow for the Multicast/broadcast resource delete response from NRM server to VAL server.

Table 14.3.2.45-1: Multicast/broadcast resource delete response

Information element	Status	Description
Result	M	The result indicates success or failure of the multicast/broadcast resource delete request operation.
Identity of the multicast/broadcast resource	M	The identity of the multicast/broadcast MBS session, or/and the identity of the MBMS bearer.

14.3.2.46 Multicast resource activate request

Table 14.3.2.46-1 describes the information flow for the multicast resource activate request from VAL server to NRM server.

Table 14.3.2.46-1: Multicast resource activate request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
MBS session ID	M	Identity of multicast MBS session

14.3.2.47 Multicast resource activate response

Table 14.3.2.47-1 describes the information flow for the multicast resource activate response from NRM server to VAL server.

Table 14.3.2.47-1: Multicast resource activate response

Information element	Status	Description
Result	M	The result indicates success or failure of the multicast resource activate operation.
MBS session ID	M	Identity of multicast MBS session

14.3.2.48 Multicast resource deactivate request

Table 14.3.2.48-1 describes the information flow for the multicast resource deactivate request from VAL server to NRM server.

Table 14.3.2.48-1: Multicast resource deactivate request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
MBS session ID	M	Identity of multicast MBS session

14.3.2.49 Multicast resource deactivate response

Table 14.3.2.49-1 describes the information flow for the multicast resource deactivate response from NRM server to VAL server.

Table 14.3.2.49-1: Multicast resource deactivate response

Information element	Status	Description
Result	M	The result indicates success or failure of the multicast resource deactivate operation.
MBS session ID	M	Identity of multicast MBS session

14.3.2.50 MapVALGroupToSessionStream

Table 14.3.2.50-1 defines the MapVALGroupToSessionStream to be sent from the NRM server to NRM clients to provide specific required information to receive the media related to a group related VAL data communication within an MBS session.

Table 14.3.2.50-1: MapVALGroupToSessionStream

Information element	Status	Description
VAL group ID	M	This element identifies the VAL group related to a group related VAL data communication to be delivered over the MBS session.
VAL data stream identifier	M	This element identifies the VAL data stream of the SDP used for the group related VAL data communication within the MBS session.
MBS session ID	O	The MBS session identifier if the MapVALGroupToSessionStream message is not sent on the same session as the VAL data

14.3.2.51 UE session join notification

Table 14.3.2.51-1 defines the UE session join notification to be sent from the NRM client to NRM server after successfully joining a certain multicast MBS session procedure as defined in 3GPP TS 23.247 [39].

Table 14.3.2.51-1: UE session join notification

Information element	Status	Description
MBS session ID(s)	M	The identity of the multicast MBS session(s) being joined. It is either TMGI or source specific IP multicast address.
VAL user ID or VAL UE ID	M	The identity of the VAL user or VAL UE who sends this notification.
MBS multicast joining status	M	UE's multicast MBS session status per MBS session ID, e.g., successfully joined.

14.3.2.52 MBS listening status report

Table 14.3.2.52-1 describes the information flow of MBS listening status report from the NRM client to the NRM server. The MBS listening status report is applicable to both broadcast and multicast MBS sessions.

Table 14.3.2.52-1: MBS 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 MBS listening status.
MBS session ID(s)	M	The identity of the MBS session(s) being monitored.
MBS listening status	M	The listening status per MBS session ID.
MBS reception quality level (NOTE)	O	The reception quality level
Unicast listening status	O	The unicast listening status associated with the unicast delivery.
NOTE: The set of quality levels helps service continuity in broadcast and multicast scenarios. A reception quality level may help to make an efficient switching decision to unicast delivery. How these levels are used is implementation specific.		

14.3.2.53 UE unified traffic pattern and monitoring management subscription request

Table 14.3.2.53-1 describes the information flow for the UE unified traffic pattern and monitoring management subscription request from the VAL server to the NRM Server.

Table 14.3.2.53-1: UE unified traffic pattern and monitoring management subscription request

Information element	Monitoring	Description
VAL UE ID	M	UEs hosting clients for which the subscription is requested
VAL service ID	M	Identity of the VAL service for which the subscription is requested.
Management subscription indications	M	At least one of the following indications is to be provided
> UE unified traffic pattern monitoring management indication	O	Indicates that management of the UE unified traffic pattern is requested
> UE unified traffic pattern update notification indication	O	Indicates that notifications for updates of the UE unified traffic pattern monitoring is requested
> Network parameter coordination indication	O	Indicates whether network parameter coordination by the NRM with 5GC is requested (see NOTE 1)
traffic pattern configuration	O	Traffic pattern configuration of the VAL service for this UE, as described in table 14.3.2.53-2.
NOTE 1: The network parameter coordination functionality is also subject to policies available at the NRM Server.		

Table 14.3.2.53-2: VAL traffic pattern configuration

Information element	Monitoring	Description
Schedule elements	O	List of schedule elements applicable to the traffic patterns of the VAL service for this UE. Each schedule element is composed from seven fields: second, minute, hour, day of month, month, day of week and year. Each element indicates times or durations when the service traffic occurs. Multiple schedule elements can be used to create complex scheduling. (see NOTE 2)
Expiration time	O	Identifies when the VAL traffic pattern parameter configuration expires. If absent, it indicates that there is no expiration time.
Stationary indication	O	Identifies whether the UE is expected to be stationary or mobile while communicating using this traffic pattern configuration

NOTE 2: The following is an example of a schedule element with the fields: second, minute, hour, day of month, month, day of week and year:

*; 0-30 ; 2; *; Jan-Sept; Tues; *.

The following mapping is provided for information, if this schedule element is derived from communication patterns as described in 3GPP TS 29.122 [54] clause 5.10

- periodicCommunicationIndicator: TRUE
- communicationDurationTime: 30 min
- periodicTime: 1 week
- scheduledCommunicationTime: Tues, 2:00-2:30
- validityTime: calculated using the Jan-Sept range and the provided expiration time.

NOTE 3: The format of this IE is to be provided in stage 3. The purpose of this description is to clarify how the same element can contain multiple periodicities, specify start/stop times, etc.

14.3.2.54 UE unified traffic pattern and monitoring management subscription response

Table 14.3.2.54-1 describes the information flow for the UE unified traffic pattern and monitoring management subscription response from the NRM server to the VAL server.

Table 14.3.2.54-1: UE unified traffic pattern and monitoring management subscription response

Information element	Monitoring	Description
Result	M	Indicates success or failure of the subscription request

14.3.2.55 UE unified traffic pattern update notification

Table 14.3.2.55-1 describes the information flow for the UE unified traffic pattern update notification from the NRM server to the VAL server.

Table 14.3.2.55-1: UE unified traffic pattern update notification

Information element	Monitoring	Description
UE ID	M	UE for which the UE unified traffic pattern update notification is provided for.
Schedule elements	O	Schedule element applicable to the unified traffic patterns of the UE. A schedule element is composed from seven fields: second, minute, hour, day of month, month, day of week and year. Each element indicates times or durations of UE availability.
Stationary indication	O	Identifies whether the UE is expected to be stationary or mobile while communicating using this UE unified traffic pattern, as determined by the NRM Server
Cause	O	This element is mandatory when the notification is provided to inform of a parameter configuration applied by the network which is incompatible with the existing Traffic Patterns. (see NOTE) The element is optional when the notification informs of UE unified traffic pattern updates, providing additional information on the reason for the UE unified traffic pattern update (e.g. monitoring events received)

Editor's Note: For notifications of incompatible configurations, it is FFS whether adding an optional element with a proposed NRM Server UE unified traffic pattern update is beneficial.

14.3.2.56 Get application connectivity context request.

Table 14.3.2.56-1 describes the information flow for application connectivity context request from the NRM server to the NRM client, the context applying to UE-to-UE application-level direct communications.

Table 14.3.2.56-1: Get Application connectivity context request.

Information element	Status	Description
Requester VALUE ID	M	The identity of the source VAL client for which the NRM client performs the request.
VAL service ID	M	Identify of the VAL service for which the information is requested.
VAL-specific connection coordination context information	O	Additional information required to identify the context data (e.g. device type, device vendor, etc)

14.3.2.57 Get application connectivity context response.

Table 14.3.2.57-1 describes the information flow for application connectivity context response from the NRM client to the NRM server, the context applying to UE-to-UE application-level direct communications.

Table 14.3.2.57-1: UE-to-UE connection coordination context response

Information element	Status	Description
Result	M	The result indicates success or failure of the UE-to-UE resource coordination response operation.
Application connectivity context (see NOTE)	O	Application connectivity context used for determining connectivity parameters. If this IE is included, at least one of the information elements in Table 14.3.2.35-2 shall be provided.
NOTE: When this information element is not included, the NRM server considers default or pre-provisioned values.		

14.3.2.58 BDT configuration request

Table 14.3.58-1 describes the information flow for the BDT configuration request from the VAL server to the NRM Server.

Table 14.3.2.58-1: BDT configuration request

Information element	Status	Description
VAL service ID	M	Identity of the VAL service for which the configuration is requested.
List of VAL UE IDs	M	List of VAL UE IDs for which the transfer policy applies or a VAL group ID.
Volume per UE	M	Expected data volume for the background data transfer.
Desired time window	M	Desired time window for the background data transfer.
Desired area information	M	Desired geographical area for the background data transfer
Request expiration time	O	Expiration time for the background data transfer request to enable NRM server to delay BDT negotiation with 3GPP core network considering BDT configuration requests from other VAL servers.
Policy Selection Guidance	O	List that includes guidance to the NRM in selecting from multiple transfer policies provided by underlying network. Possible values include: ”lowest cost”, “highest throughput given maximum cost of X”, etc. If not included, the NRM may choose from among multiple transfer policies, depending on local and ASP-provided policies.

14.3.2.59 BDT configuration response

Table 14.3.2.59-1 describes the information flow for BDT configuration response from the NRM server to the VAL server.

Table 14.3.2.59-1: BDT configuration response

Information element	Status	Description
Result	M	The result indicates success or failure of the BDT configuration operation.
BDT configuration identifier (NOTE)	O	Identifier of the BDT configuration information stored at the NRM server
BDT Reference ID (see NOTE)	O	Indicates the Background data transfer Reference ID provided by the 3GPP network
Granted time window (see NOTE)	O	Granted time window for the background data transfer.
NOTE: These IEs shall be included when Result is success.		

14.3.2.60 BDT negotiation notification

Table 14.3.2.60-1 describes the information flow for BDT negotiation notification from the NRM server to the VAL server.

Table 14.3.2.60-1: BDT negotiation notification

Information element	Status	Description
BDT configuration identifier	M	Identifier of the BDT configuration information stored at the NRM server
Granted time window (see NOTE)	O	Granted time window for the background data transfer.
BDT Reference ID	M	Indicates the Background data transfer Reference ID provided by the 3GPP network
BDT policy removal indicator (see NOTE)	O	The indicator about the BDT policy removal.
NOTE: Either of these IEs are included.		

14.3.2.61 BDT configuration get request

Table 14.3.2.61-1 describes the information flow for the BDT configuration get request from the VAL server to the NRM Server.

Table 14.3.2.61-1: BDT configuration get request

Information element	Status	Description
VAL service ID	M	Identity of the VAL service for which the BDT configuration is requested to be updated.
BDT configuration identifier	M	Identifier of the BDT configuration stored in the NRM server.

14.3.2.62 BDT configuration get response

Table 14.3.2.62-1 describes the information flow for BDT configuration get response from the NRM server to the VAL server.

Table 14.3.2.62-1: BDT configuration get response

Information element	Status	Description
Result	M	The result indicates success or failure of BDT configuration get operation.
BDT configuration identifier	M	Identifier of the BDT configuration stored in the NRM server.
BDT configuration data (see NOTE)	O	The BDT configuration data stored at the NRM server which includes information like VAL service ID, List of VAL UE IDs/VAL group ID, Volume per UE, Desired Time Window, Granted Time Window, Desired Area Information, Policy Selection Guidance, BDT Reference ID
NOTE: The BDT configuration data IE is included if the Result indicates success.		

14.3.2.63 BDT configuration update request

Table 14.3.2.63-1 describes the information flow for the BDT configuration update request from the VAL server to the NRM Server.

Table 14.3.2.63-1: BDT configuration update request

Information element	Status	Description
VAL service ID	M	Identity of the VAL service for which the BDT configuration is requested to be updated.
BDT Configuration identifier	M	Identifier of the BDT configuration stored in the NRM server.
Volume per UE (see NOTE)	O	Updated expected data volume for the background data transfer.
Desired time window (see NOTE)	O	Updated desired time window for the background data transfer.
Desired area information (see NOTE)	O	Updated desired geographical area for the background data transfer
Policy Selection Guidance (see NOTE)	O	Updated list that includes guidance to the NRM in selecting from multiple transfer policies provided by underlying network. Possible values include: ”lowest cost”, “highest throughput given maximum cost of X”, etc. If value is empty, the NRM may choose from among multiple transfer policies, depending on local and ASP-provided policies.
NOTE: At least one of the IEs shall be present		

14.3.2.64 BDT configuration update response

Table 14.3.2.64-1 describes the information flow for BDT configuration update response from the NRM server to the VAL server.

Table 14.3.2.64-1: BDT configuration update response

Information element	Status	Description
Result	M	The result indicates success or failure of BDT configuration update operation.
BDT Configuration identifier	M	Identifier of the BDT configuration stored in the NRM server.

14.3.2.65 BDT configuration delete request

Table 14.3.2.65-1 describes the information flow for the BDT configuration delete request from the VAL server to the NRM Server.

Table 14.3.2.65-1: BDT configuration delete request

Information element	Status	Description
VAL service ID	M	Identity of the VAL service for which the BDT configuration is requested to be deleted.
BDT configuration identifier	M	Identifier of the BDT configuration stored in the NRM server.

14.3.2.66 BDT configuration response

Table 14.3.2.66-1 describes the information flow for BDT configuration delete response from the NRM server to the VAL server.

Table 14.3.2.66-1: BDT configuration delete response

Information element	Status	Description
Result	M	The result indicates success or failure of BDT configuration delete operation.

14.3.2.67 Reliable transmission request

Table 14.3.2.67-1 describes the information flow for reliable transmission request from SEALDD server (or VAL server) to the NRM server.

Table 14.3.2.67-1: Reliable transmission request

Information element	Status	Description
Requester Identity	M	The identity of the SEALDD server (or VAL server) performing the request.
Application descriptors	O	A pair of applic traffic descriptors (e.g. address, port, transport layer protocol) of the SEALDD server (or VAL server), used to establish redundant transmission paths.
UE ID	O	The identity of VAL UE.
UE address	O	The address of VAL UE

14.3.2.68 Reliable transmission response

Table 14.3.2.68-1 describes the information flow for the reliable transmission response from NRM server to SEALDD server (or VAL server).

Table 14.3.2.68-1: Reliable transmission response

Information element	Status	Description
Result	M	The result indicates success or failure of the reliable transmission request operation.

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.

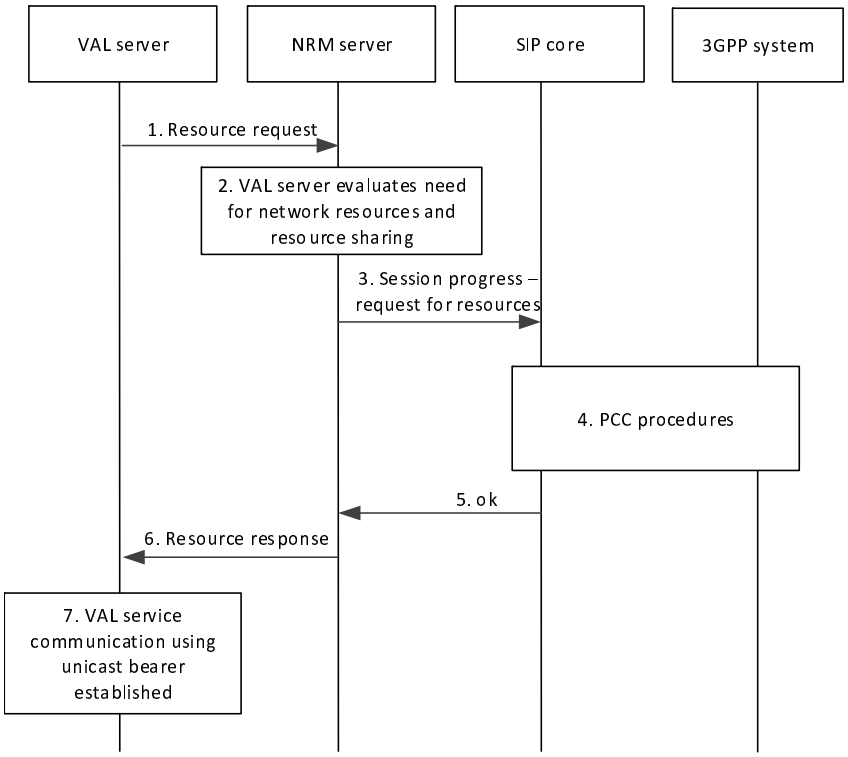

Figure 14.3.3.2.1.2-1: Resource request at VAL service communication establishment

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;

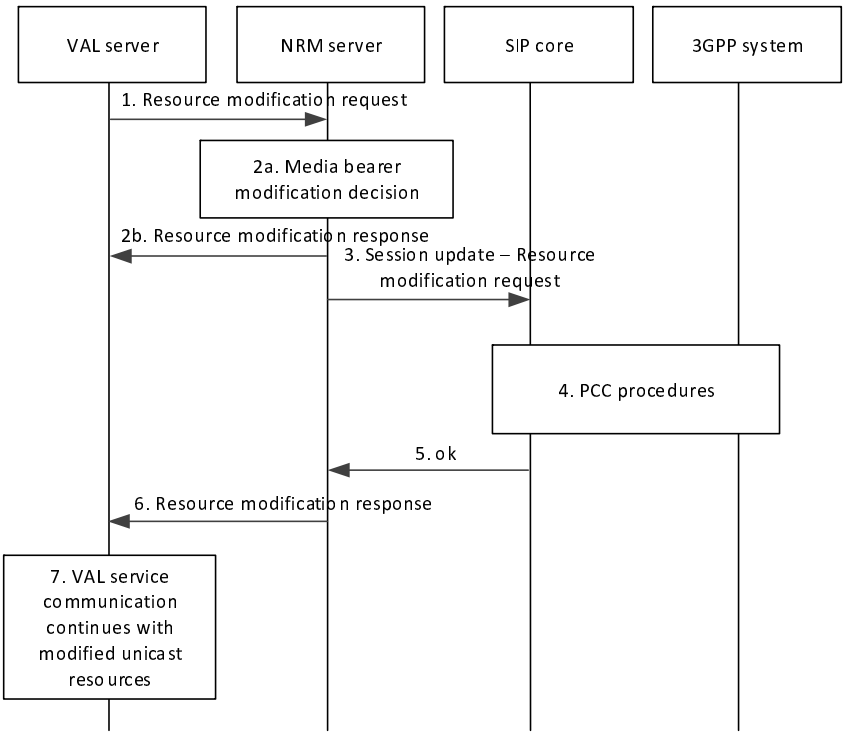

Figure 14.3.3.2.2.2-1: Bearer modification request

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.

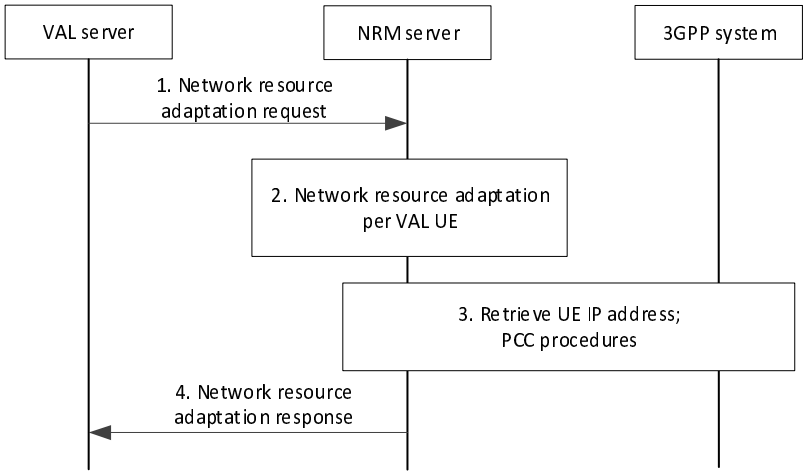

Figure 14.3.3.3.1.2-1: Network resource adaptation

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.

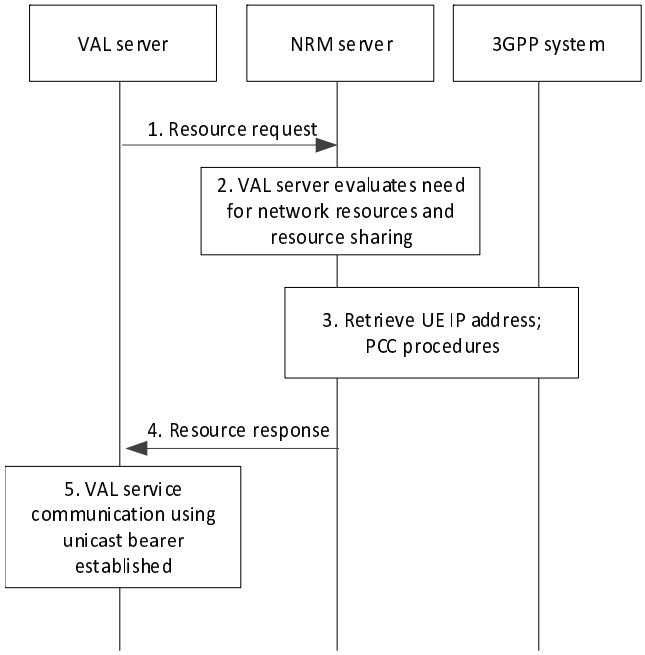

Figure 14.3.3.3.2.2-1: Resource request at VAL service communication establishment

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;

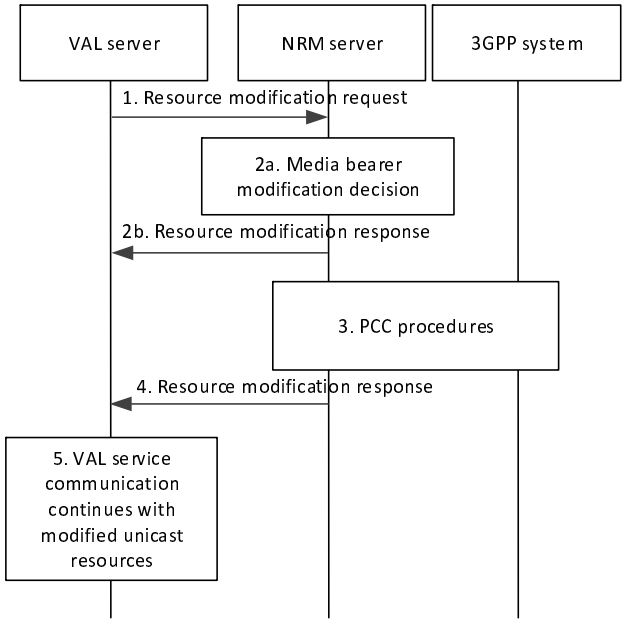

Figure 14.3.3.3.3.2-1: Bearer modification request

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

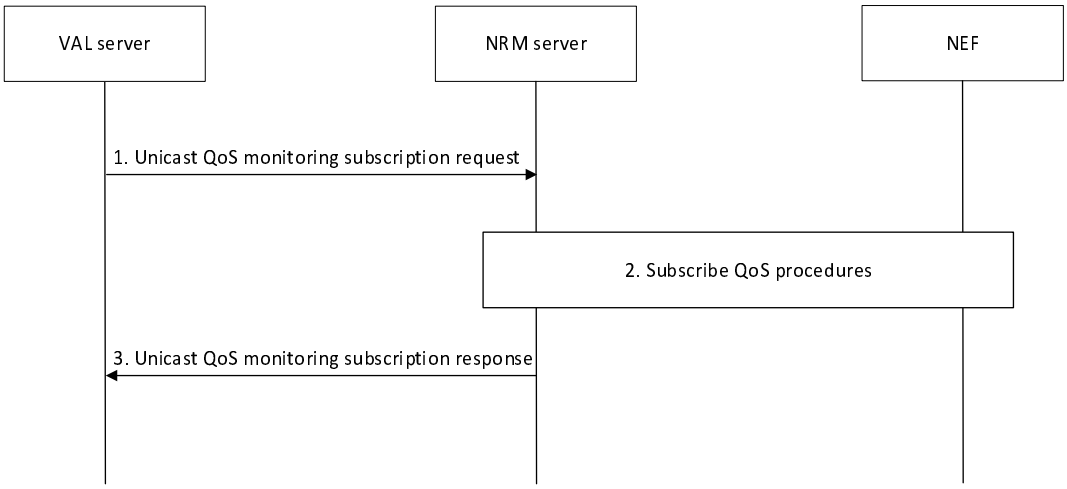

Figure 14.3.3.4.1.2-1: Unicast QoS monitoring subscription

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

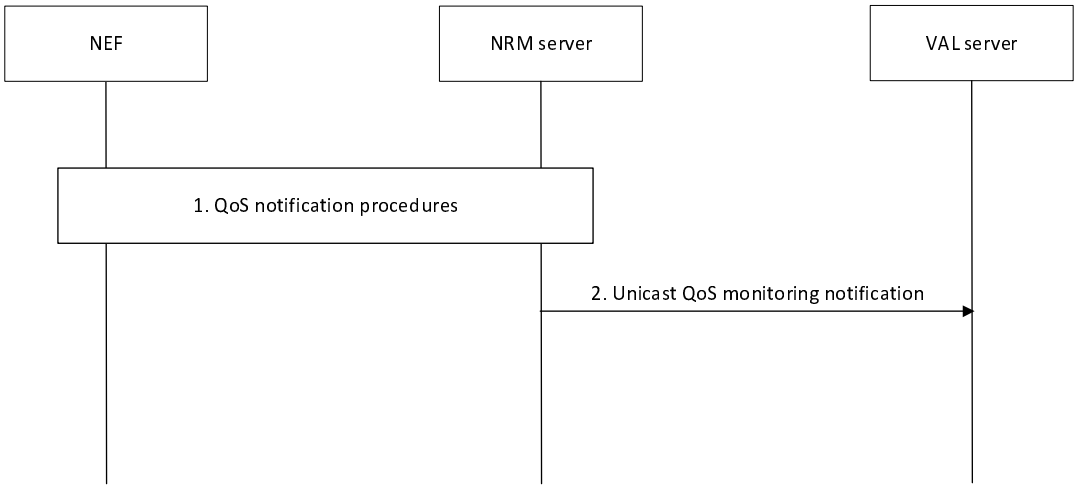

Figure 14.3.3.4.2.2-1: Unicast QoS monitoring notification procedure

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

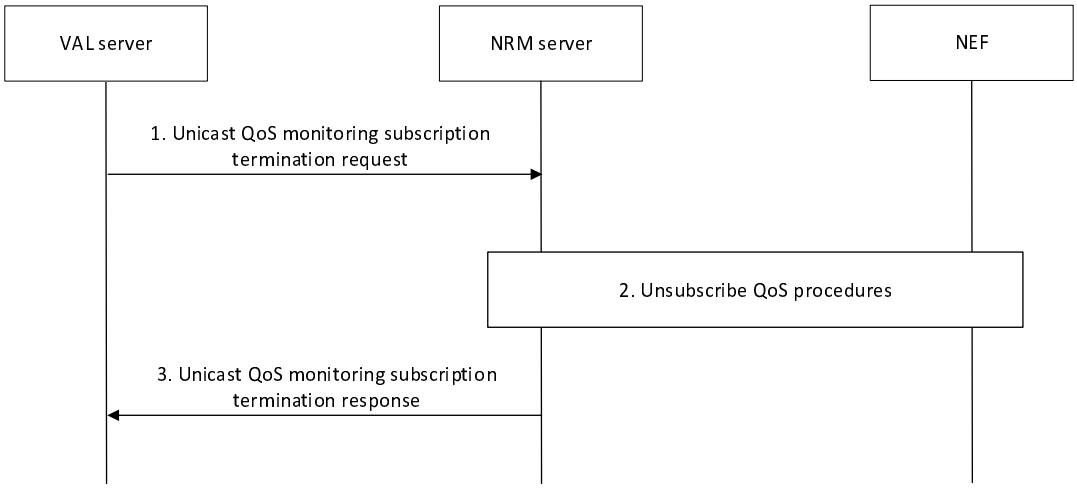

Figure 14.3.3.4.3.2-1: Unicast QoS monitoring subscription termination procedure

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.

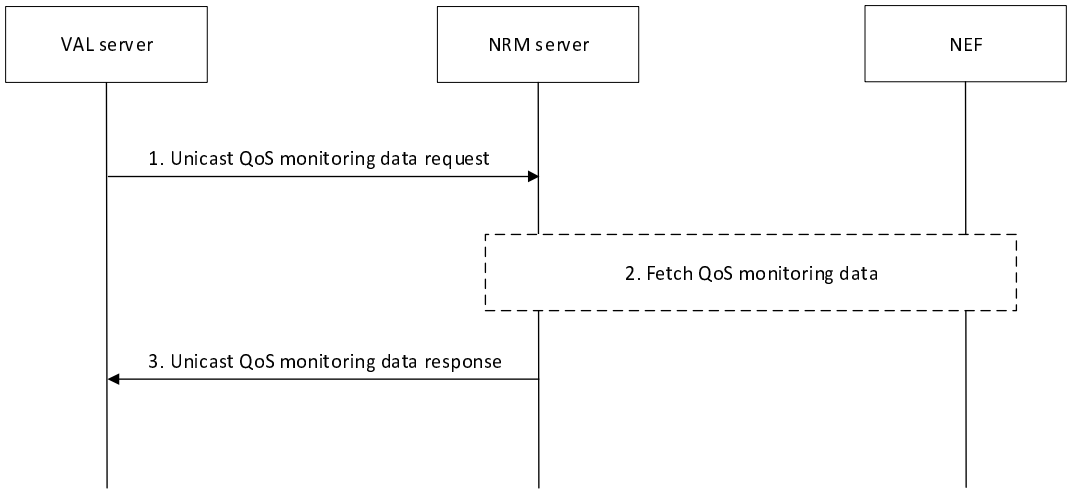

Figure 14.3.3.4.4.2-1: Retrieval of unicast QoS monitoring data

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.

14.3.3.4.5 Unicast QoS monitoring subscription update procedure

14.3.3.4.5.1 General

This subclause describes the high-level procedure to update unicast QoS monitoring subscription. This procedure updates the parameters to be monitored of an already existing unicast QoS monitoring subscription.

14.3.3.4.5.2 Procedure

Figure 14.3.3.4.5.2-1 illustrates the high level procedure for unicast QoS monitoring subscription update.

Pre-conditions:

- The VAL UE has an established connection in the 5GS
- Unicast QoS monitoring subscription has successfully been ~~invoked~~ established for the VAL UE

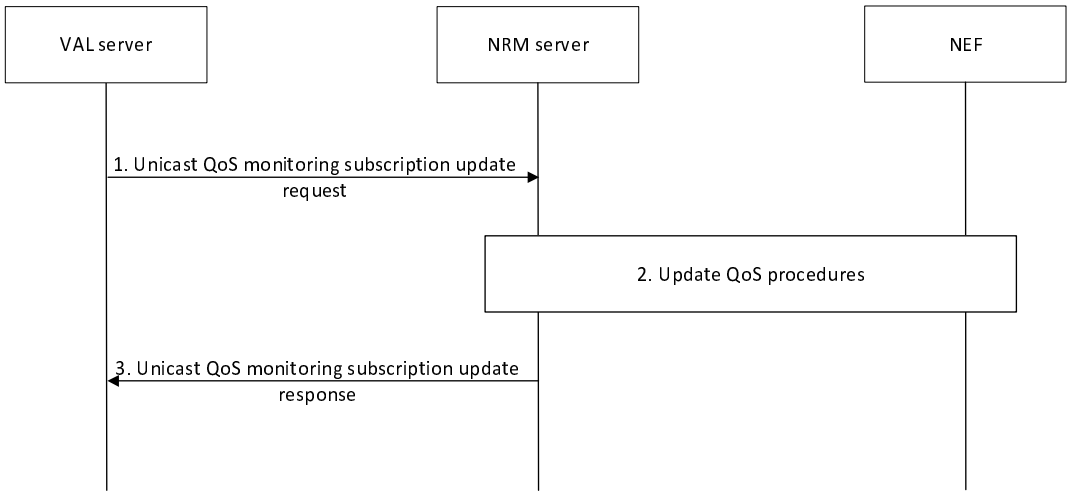

Figure 14.3.3.4.5.2-1: Unicast QoS monitoring subscription update

1. The VAL server sends a unicast QoS monitoring subscription update request to the NRM server. It shall refer to an existing subscription, identified by the list of VAL UEs, VAL UE group or VAL stream IDs included into the message.

2. The NRM server interacts with the NEF to update the relevant QoS monitoring subscription parameters and reporting frequency as specified in step 2 of clause 14.3.3.4.1.2 of this document.

3. The NRM server responds with a unicast QoS monitoring subscription update response indicating the subscription status.

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.

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.

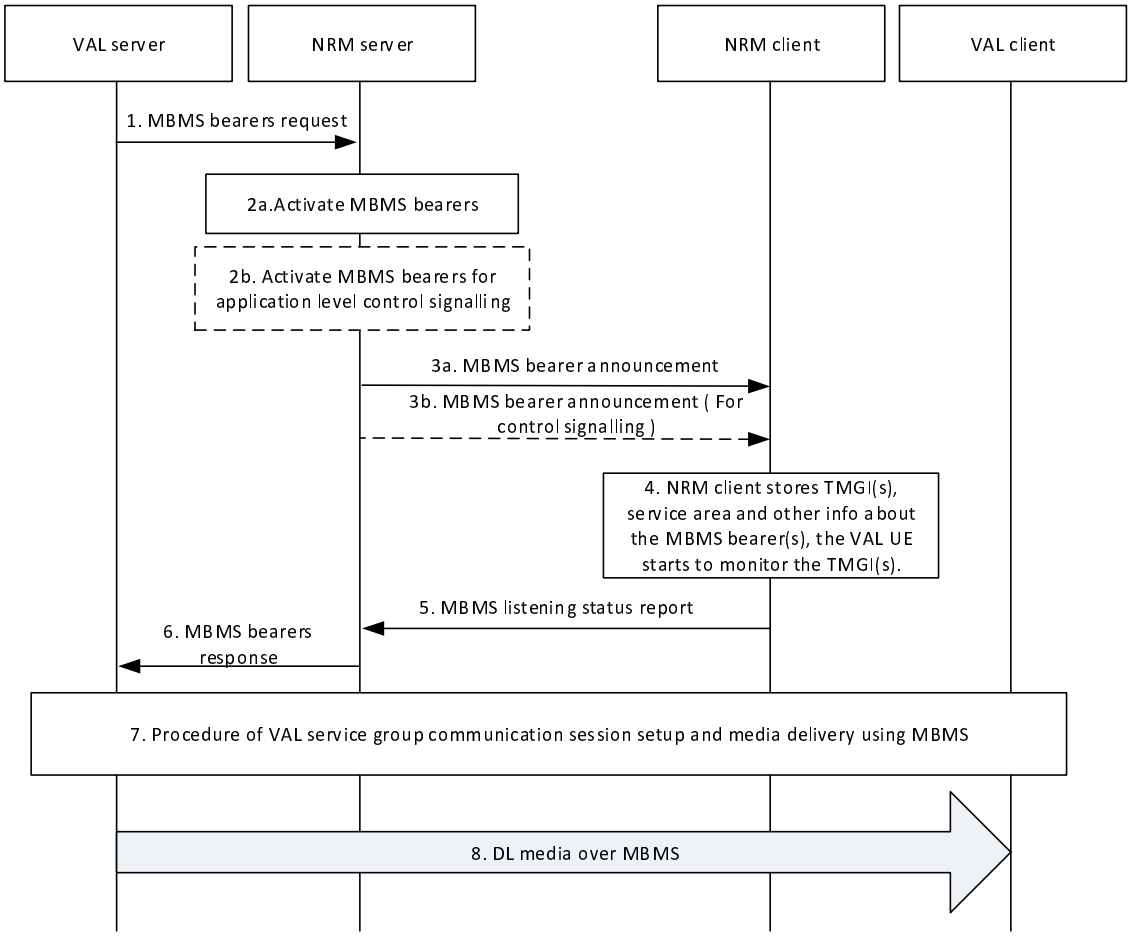

Figure 14.3.4.2.2-1: Use of pre-established MBMS bearers

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.

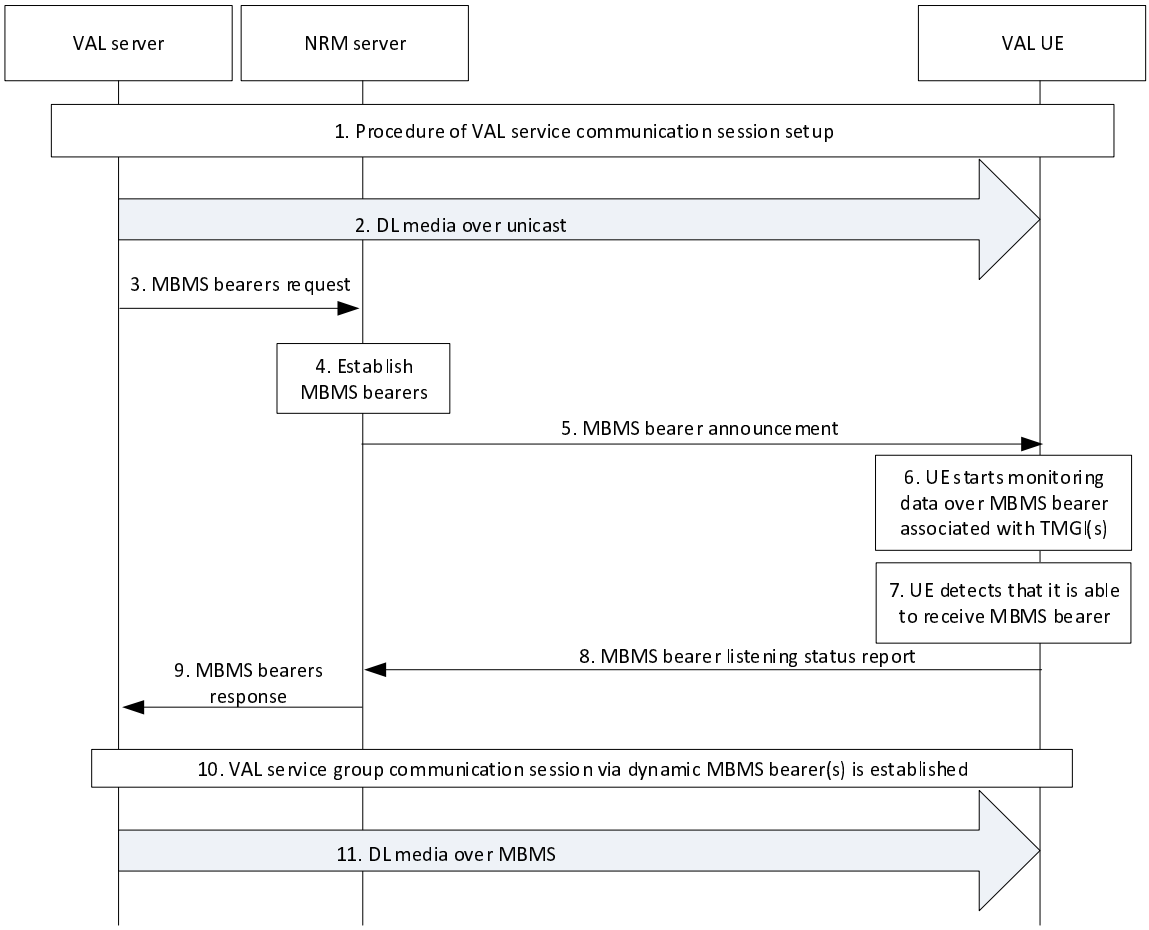

Figure 14.3.4.3.2-1: Use of dynamic MBMS bearer establishment

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.

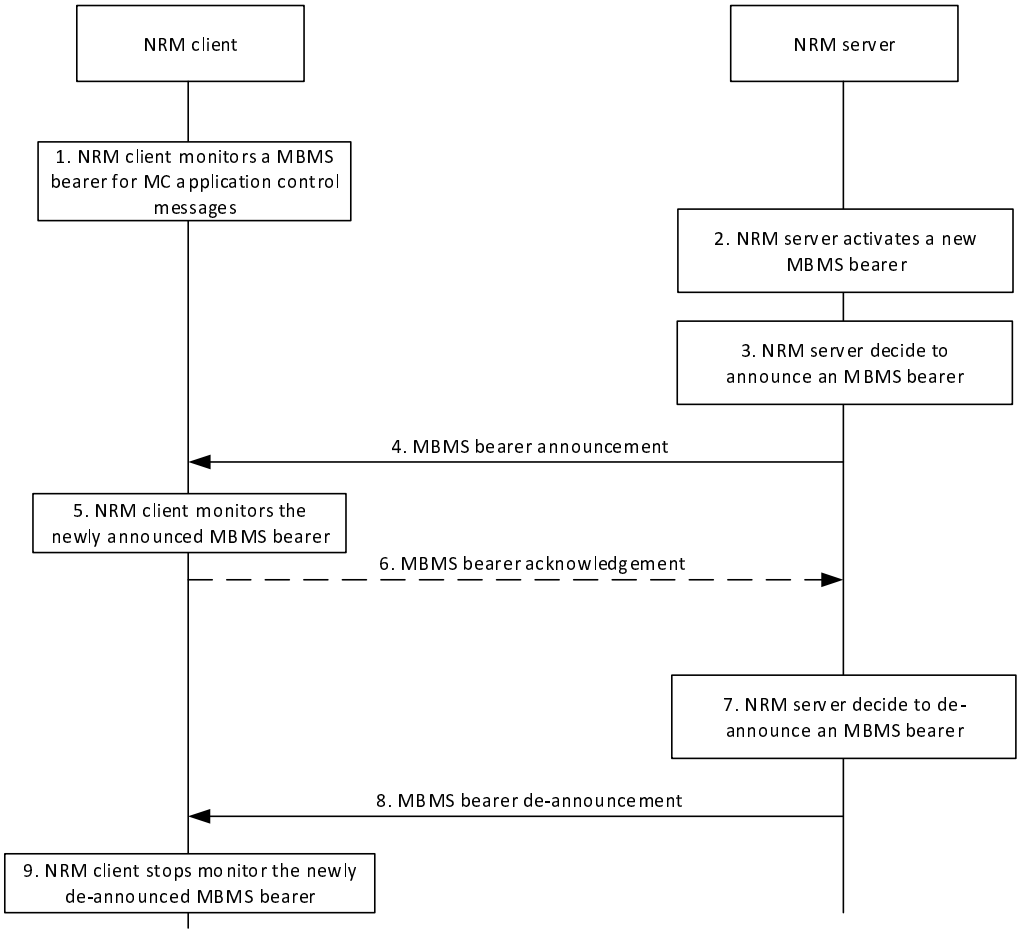

Figure 14.3.4.4.2-1: MBMS bearer announcement over an MBMS bearer used for application control messages

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

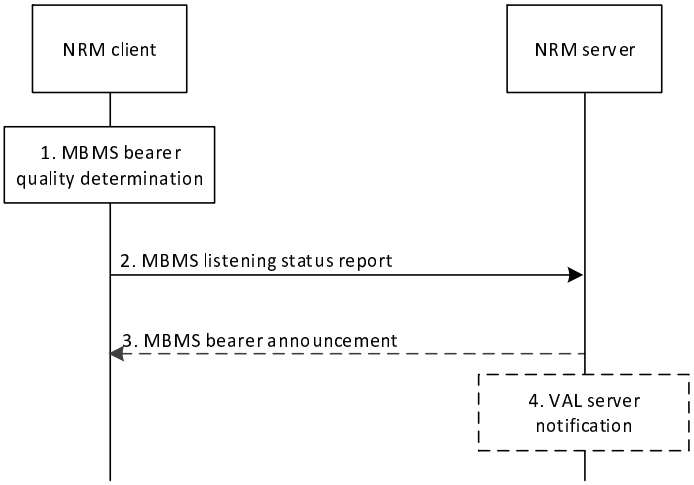

Figure 14.3.4.5.2-1: MBMS bearer quality detection

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.

NOTE 1: The set of MBMS reception quality levels and the mapping of the determined MBMS bearer quality to those levels are upto implementation.

NOTE 2: 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 3: 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 4: 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.

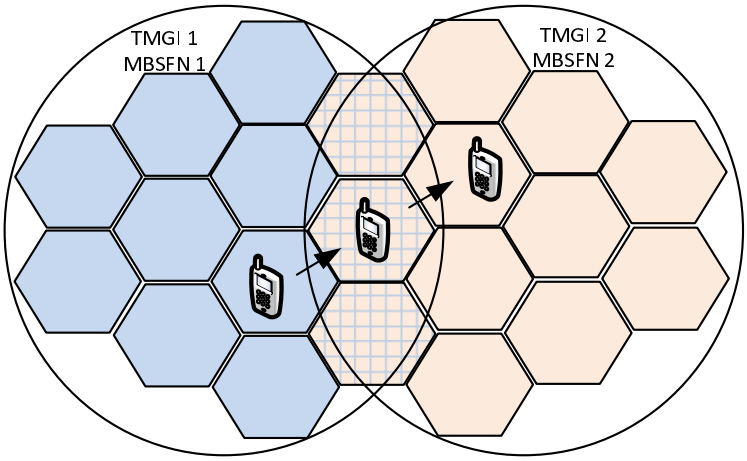

Figure 14.3.4.6.2-1: Two MBMS bearer using overlapping MBSFN areas

Figure 14.3.4.6.2-2 illustrates the procedure:

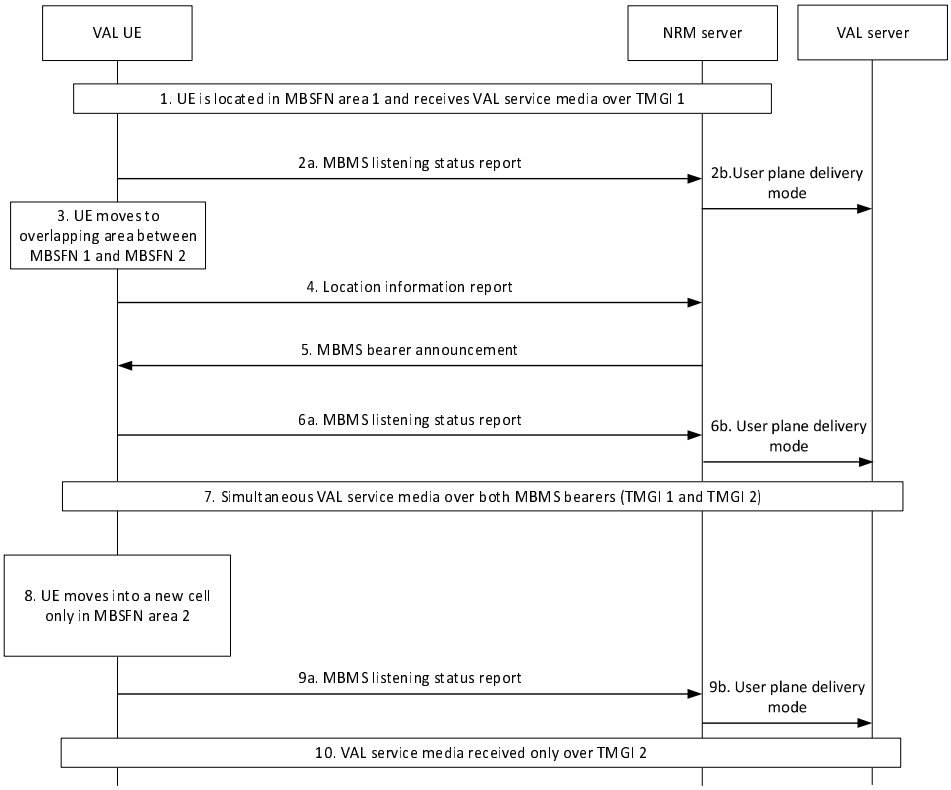

Figure 14.3.4.6.2-2: Service continuity when moving from one MBSFN to another

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.

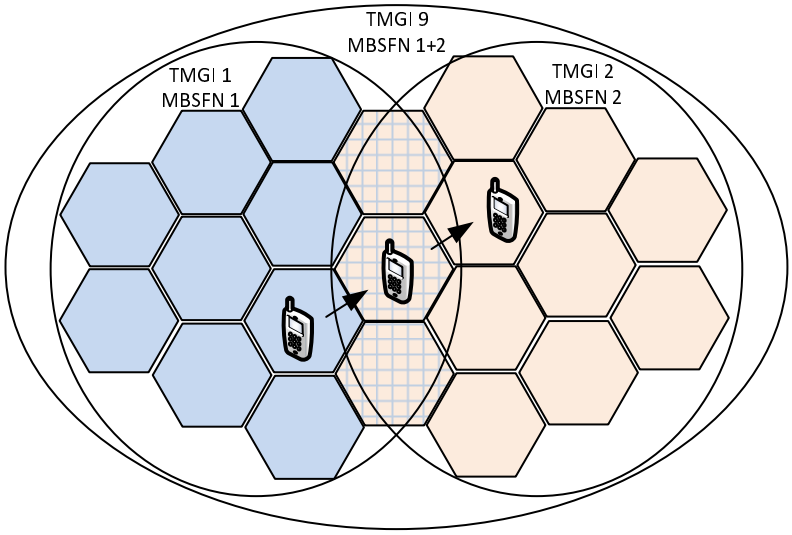

Figure 14.3.4.6.2-3: Two MBMS bearer using overlapping MBSFN areas with a separate application signalling bearer

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

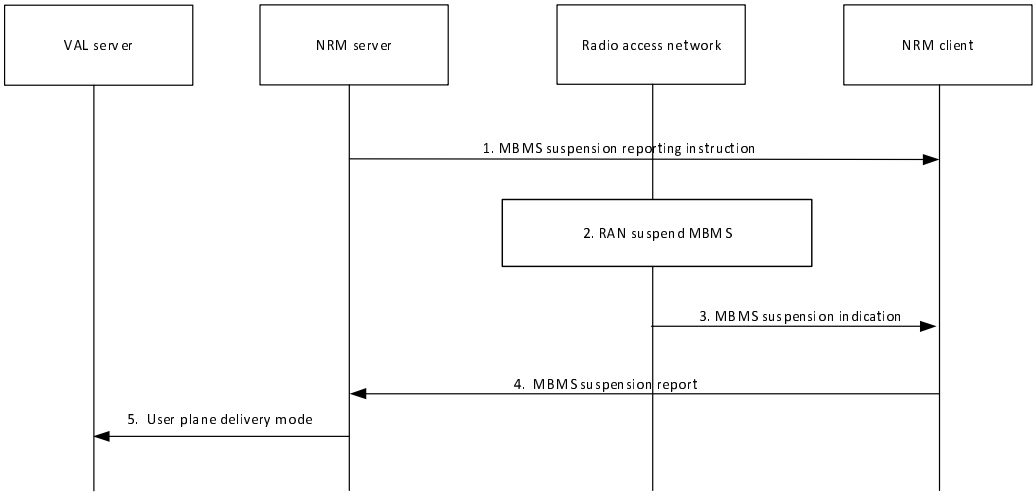

Figure 14.3.4.7.2-1: MBMS suspension notification

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.

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.

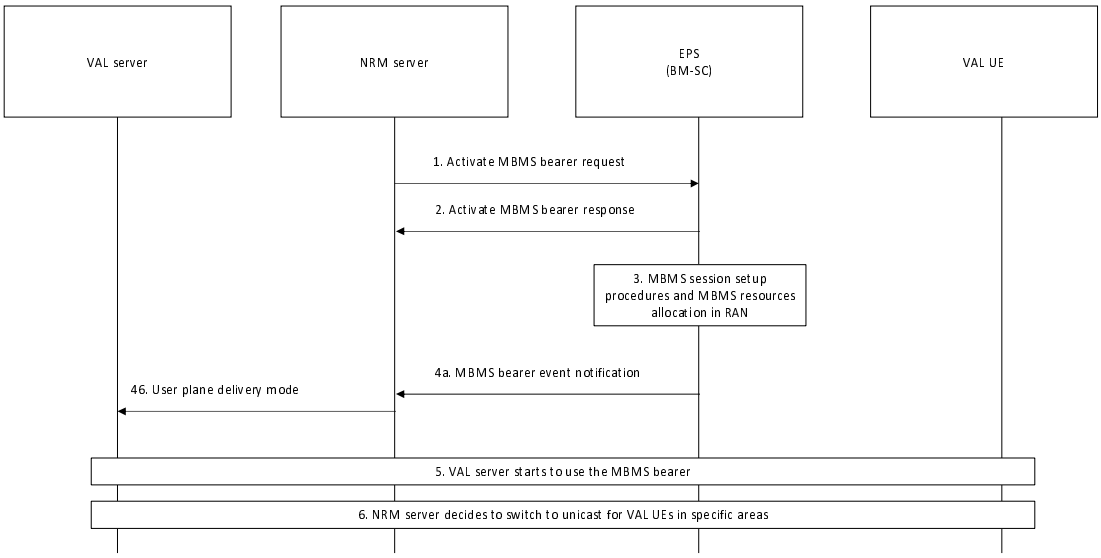

Figure 14.3.4.8.2-1: MBMS bearer event notification

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. The NRM server may decide, based on the received events (e.g., any cells fail to allocate MBMS resources to a specific MBMS bearer), to switch to unicast transmission for relevant VAL UEs.

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.

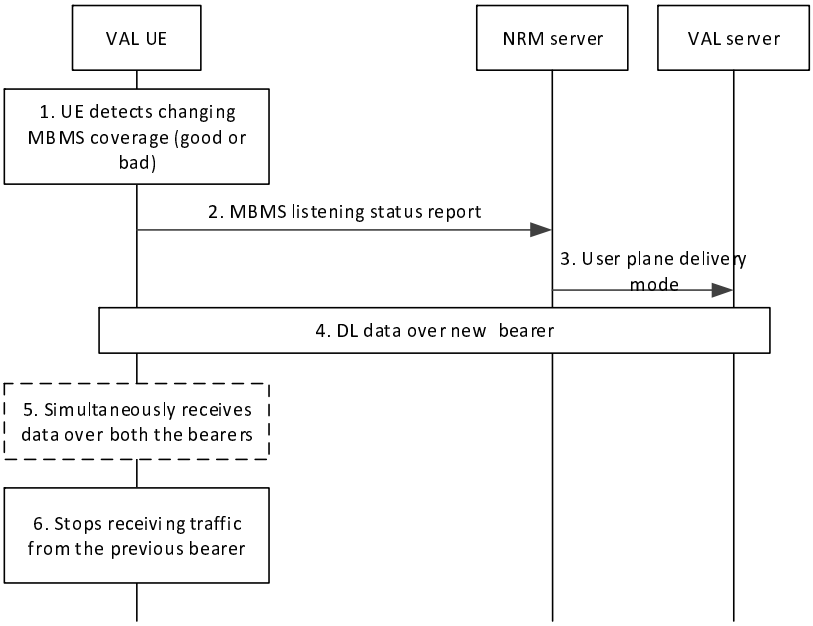

Figure 14.3.4.9.2-1: Switching between MBMS delivery and unicast delivery

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.

14.3.4A Multicast resource management for 5GS

14.3.4A.1 General

This subclause defines information flows and procedures for 5G MBS usage that applies to VAL services. 5G MBS session can be used by any VAL service for any VAL service group.

The main purpose of using 5G Multicast-Broadcast Service (MBS) by verticals is to provide efficient downlink delivery of user traffic in VAL service group communications or in a certain area.

Multicast and broadcast communication services in 5G for vertical applicationsrely on the creation and establishment of MBS sessions to deliver user data in downlink. Shared and individual delivery from the VAL server to multiple VAL users is supported either as point-to-point or point-to-multipoint over the radio. The MBS session which consist of one

or multiple QoS flows for different service requirements are either broadcast or multicast type. For the broadcast MBS session or local MBS session, the MBS service area is configured with the MBS session.

NOTE 1: Support of MBS and specific session types is an implementation choice.

Within this arrangement, the VAL server decides whether to create broadcast or multicast MBS sessions to be associated with certain VAL service groups or area. The 5GC adaptively decides whether to deliver the MBS traffic from the MB-UPF in the form of shared delivery or individual delivery, where the latter is applicable to multicast MBS sessions. The NG-RAN decides to utilize point-to-point or point-to-multipoint delivery methods applicable for shared delivery only. MBS provides reliability enhancements and minimizes loss of information, e.g., due to mobility and handover.

MBS group scheduling mechanism enables simultaneous reception of MBS and unicast user traffic by the VAL UEs. The UEs can receive broadcast MBS sessions irrespective of their RRC state (i.e., connected, inactive or idle) and multicast sessions only in RRC-CONNECTED state.

The following capabilities (non-exhaustive list) provided by MBS could be used by NRM server:

- MBS session creation;
- MBS session update;
- MBS session release;
- MBS session ID allocation;
- Dynamic PCC control for MBS session.

The first phase to utilize MBS sessions for VAL media transmission is to reserve the network resource by creating a MBS sessions. The MBS session creation is initiated by the VAL server towards the NRM server, and the NRM server further interacts with the 5GS to complete the whole process. The UE's capabilities and service related information e.g., UE's MBS capabilities, location, MBS listening status report, UE session join notification sent by group members are considered when deciding to create or use MBS sessions. During the interaction with NRM server, the necessary information related to the requested session is determined, e.g., MBS session mode (either a broadcast or a multicast session) and the required service profile. This interaction between the NRM server and the 5GS depends on the configuration option under consideration, i.e., whether the NRM server is in trusted domain (limited operations), and whether the session creation is done with or without a dynamic PCC rule.

NOTE 1: It is implementation specific whether the VAL server decides to use multicast or broadcast MBS sessions.

NOTE 2: It is implementation specific whether the VAL decides to create (one or multiple) MBS sessions for VAL media for VAL group communications associated to a certain VAL group or create (one or multiple) dynamic MBS sessions once the need has emerged, e.g., dynamic MBS sessions to be associated for an ad hoc group.

NOTE 3: It is implementation specific whether an MBS session is associated to one or multiple VAL service groups, and whether it is re-assigned to other VAL service groups.

NOTE 4: How the NRM server uses the UE's capabilities and service related information in order to create and use the MBS session is implementation specific.

The information elements describing the MBS session under consideration is then sent to the NRM clients via MBS session announcement, where the latter need to react according to the announced session mode.

If eMBMS and 5G MBS co-exist for VAL services, the NRM service server may decide to trigger the establishment of an eMBMS bearer to deliver the VAL media associated to the VAL service group communications, if the target VAL service group(s) consists of members with MBMS capable RAT. As a result, the NRM server subsequently needs to send an eMBMS bearer announcement towards the clients camping on LTE.

NOTE 5: It is implementation specific whether the NRM server triggers an eMBMS bearer or a unicast bearer to serve VAL clients camping on LTE.

14.3.4A.2 MBS session creation and MBS session announcement

14.3.4A.2.1 General

The procedures in this clause describe how MBS session creation and MBS session announcement can be used for the transmission of VAL service group communication data over either broadcast or multicast MBS sessions. The MBS session can either be created with or without dynamic PCC rule, where the latter requires less interaction done by the NRM server towards the 5GC (either directly or via NEF).

14.3.4A.2.2 Procedure for pre-created MBS session and MBS session announcement

Pre-conditions:

- The NRM server has decided to use an MBS session for VAL service group communications associated to a certain VAL servive group based on transport only mode.
- The NRM server has performed MB-SMF discovery and selection either directly or indirectly via NEF/MBSF, unless the corresponding information is locally configured.
- NRM clients 1 to n are attached to the 5GS, registered and belong to the same VAL service group X.
- The NRM server is aware whether to request the creation of the MBS service server with or without dynamic PCC rule.

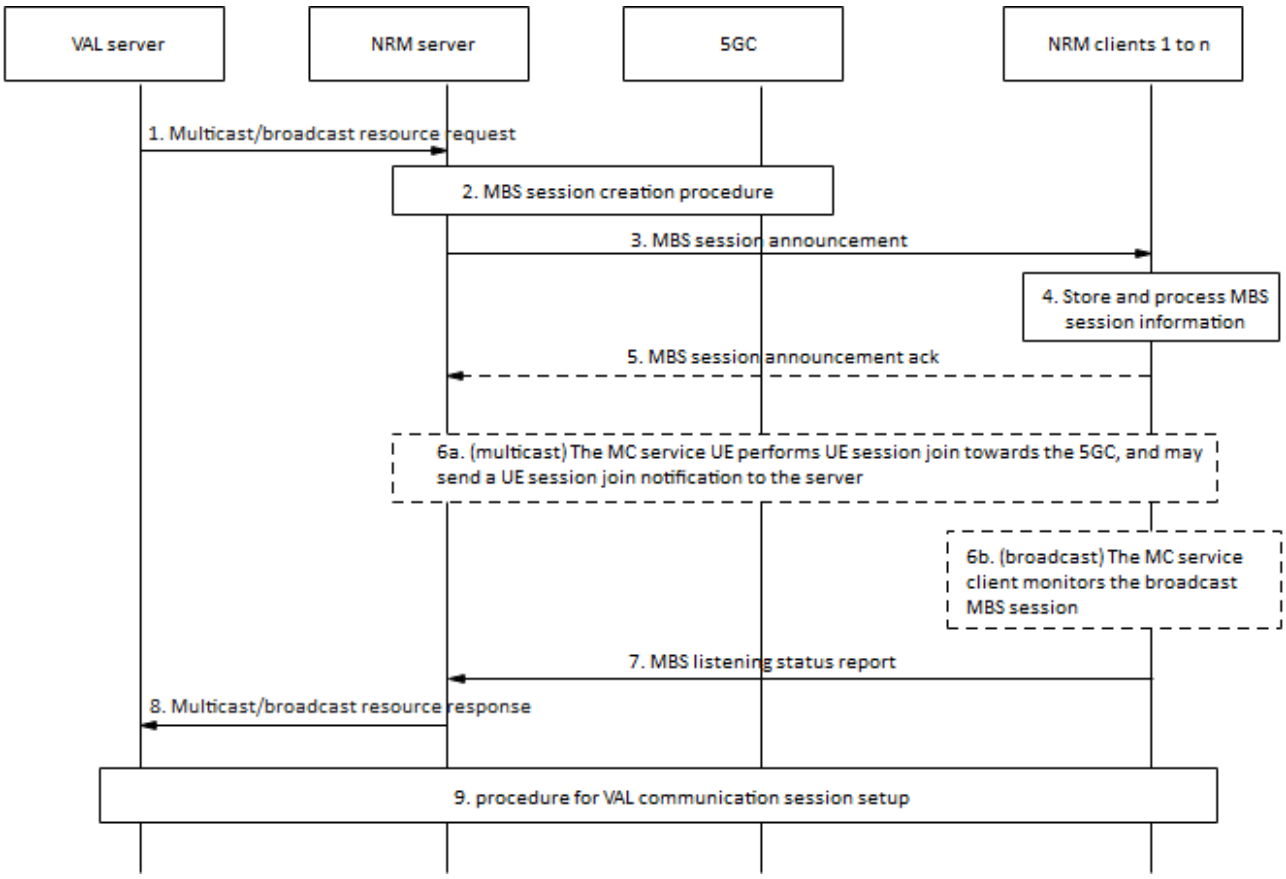

Figure 14.3.4A.1.2-1: Use of pre-created MBS session.

1. The VAL server sends a multicast/broadcast resource request towards the NRM server including the VAL server identity, service description(s), multicast resource type (e.g,. multicast type or broadcast type), service announcement mode (i.e., service announcement is sent by NRM or the VAL itself), Endpoint of the VAL server.

2. The NRM server initiates an MBS session creation procedure towards the 5GC as described in 3GPP TS 23.247 [39]. The procedure starts once the NRM server initiates a TMGI allocation request (either directly to MB-SMF or indirectly via NEF). Upon the reception of the TMGI allocation response, the NRM server sends an MBS session creation request, including further information related to the MBS session, e.g., MBS session ID, MBS session mode and the QoS requirements if dynamic PCC rule is not considered. However, if dynamic PCC rule is considered, the NRM server defines these requirements at a later step, namely it sends an MBS authorization/policy create request towards PCF (either directly or to the NEF) indicating the QoS requirements.

   In the case of an untrusted NRM server, when the requested MBS service area crosses several MB-SMF service areas, the NEF/MBSF rejects the TMGI allocation request, and it guides the NRM server by dividing the requested MBS service area into groups and returns the groups as described in 3GPP TS 23.247 [39]. Hence, the NRM server initiates a new TMGI allocation request for each grouped MBS service area. If during MBS session creation request the 5GS discovers that the MBS service area crosses several MB-SMF service areas, the request is rejected and the NEF/MBSF guides the NRM server by dividing the requested MBS service area into groups and returns the groups as described in 3GPP TS 23.247 [39]. The NRM initiates a new MBS session creation procedure for each grouped MBS service area.

   The NRM server may utilize a unicast session if any MBS service area is not supported by any MB-SMF.

NOTE 1: In case of LTE eMBMS and 5G MBS co-existence, the NRM server may trigger the establishment of eMBMS bearers as described in clause 14.3.4 (or it may establish a unicast bearer) based on the RAT capabilities supported by the VAL service group members in the VAL service group X. If MBSF and BM-SC are co-located, TMGI used by 4G eMBMS can be the same as the MBS session ID.

NOTE 2: For the case of multi carrier support for broadcast MBS sessions, the NRM server may indicate the frequencies within a broadcast MBS service area by providing the MBS frequency selection area ID(s) (MBS FSA ID(s)) to the MB-SMF or indirectly via NEF.

3. The NRM server provides the NRM clients of the VAL service group X with the information related to the created MBS session via the MBS session announcement. The MBS session announcement includes information such as the MBS session ID, MBS session mode (broadcast or multicast service type) and SDP information related to the MBS session under consideration.

NOTE 3: The NRM server may send an MBS session announcement at an earlier step during the MBS session creation procedure towards the NRM clients once the VAL service group associated to the MBS session is known.

   Optionally, the NRM server includes the information elements related to the established eMBMS bearer, as indicated in table 7.3.2.2-1. The NRM clients which camp on LTE will subsequently react to the information elements related to the eMBMS bearer as described in 3GPP TS 23.280 [3].

4. NRM clients store and process the received MBS session information.

5. NRM clients may provide an MBS session announcement acknowledgment to the NRM server to indicate the reception of the corresponding MBS session announcement.

6. Based on the MBS session mode (either multicast or broadcast), the following actions take place;

   6a. For multicast MBS sessions, NRM clients initiate a UE session join request towards the 5GC using the information provided via the MBS session announcement. Hence, upon the first successful UE session join request, the multicast is then established, and the radio resources are reserved, if the session is in an active state. The established session can either be in active or inactive state as indicated in 3GPP TS 23.247 [39]. The NRM clients sends a UE session join notification towards the server as indicated in the MBS session announcement. If indicated in the MBS session announcement information, NRM clients report the monitoring state (i.e. the reception quality of the MBS session) back to the NRM server; or

   6b. For broadcast MBS sessions, if the NRM client is accessing over 5G, the session is established as part of the session creation procedures as described in 3GPP TS 23.247 [39], and the network resources are reserved both in 5GC and NG-RAN. The NRM clients start monitoring the reception quality of the broadcast MBS session. If indicated in the MBS session announcement information, NRM clients report the monitoring state (i.e. the reception quality of the MBS session) back to the NRM server.

NOTE 4: It is implementation specific whether the MBS session reception quality level is determined per MBS session, per media stream or per MBS QoS flow level via e.g., measurements of radio level signals, such as the reference signals from the NG-RAN node(s), or packet loss.

7. The NRM clients provide a listening status notification related to the announced session (multicast or broadcast session) in the form of an MBS listening status report.

8. The NRM server provides a multicast/broadcast resource response to the VAL server.

9. An VAL service group communication setup takes place and uses the pre-created MBS session for this group communication packet DL delivery.

14.3.4A.2.3 Procedure for dynamic MBS sessions

In this scenario, the VAL service group communication is already taken place and a unicast PDU session is utilized for DL transmission. When the NRM server decides to use an MBS session for the transmission under consideration, the NRM server interacts with 5GC to reserve the necessary network resources.

NOTE 1: The NRM server logic for determining when to create a dynamic MBS session is implementation specific.

The procedure in figure 14.3.4A.2.3-1 shows one NRM client receiving the DL media. There might also be NRM clients in the same VAL service group communication session that receive the communication on a PDU session.

Pre-conditions:

- NRM client is attached to the 5GS, registered and affiliated to a certain VAL service group X.
- The NRM server is aware whether to request the creation of the MBS session with or without dynamic PCC rule.
- The NRM server has performed MB-SMF discovery and selection either directly or indirectly via NEF/MBSF, unless the corresponding information is locally configured.
- No MBS session exists, or the existing multicast MBS session fails to satisfy the QoS requirements.

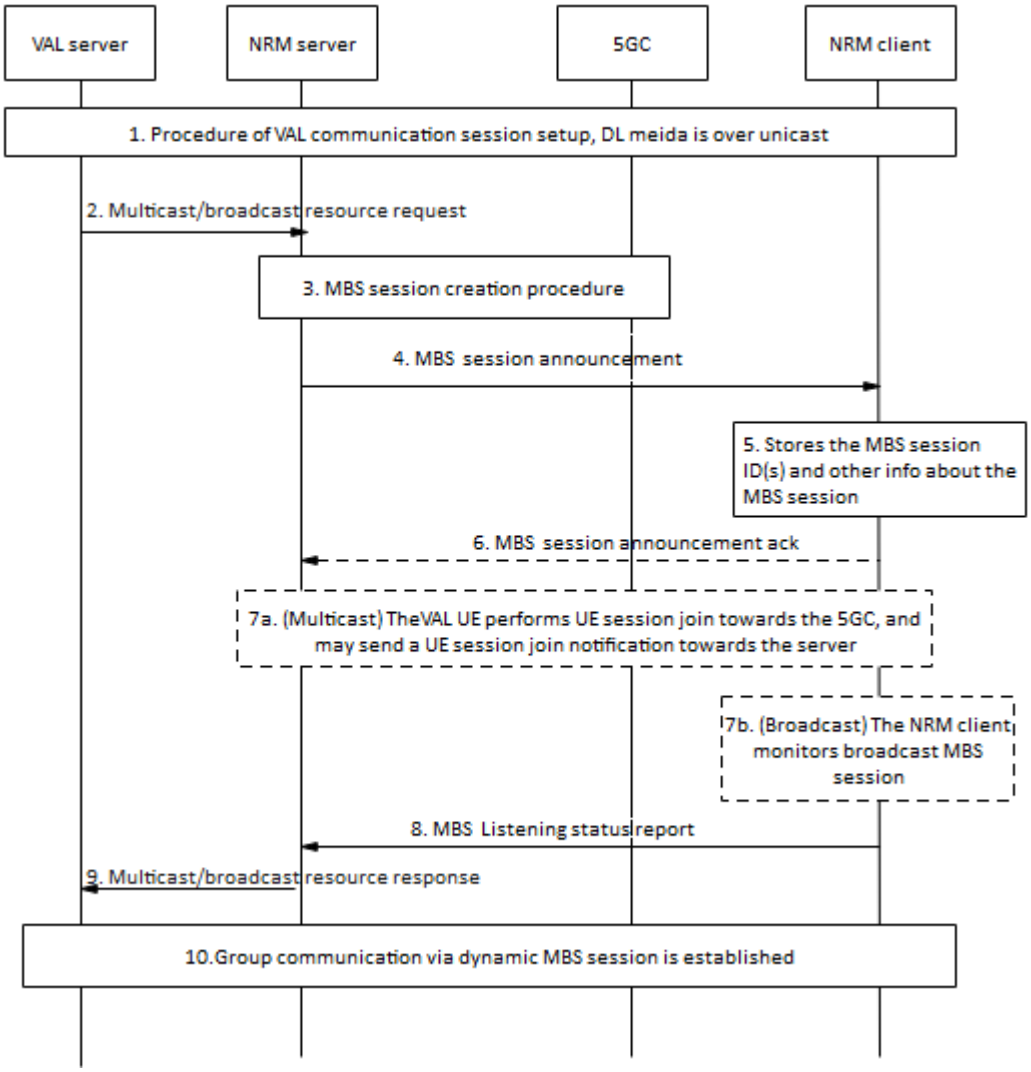

Figure 14.3.4A.2.3-1: Use of dynamic MBS session.

1. An VAL service group communication session is established and the DL media packet is delivered to the VAL client via unicast.

2. The VAL server sends a multicast/broadcast resource request towards the NRM server including the VAL server identity, service description(s), multicast resource type (e.g,. multicast type or broadcast type), service announcement mode (i.e., service announcement is sent by NRM or the VAL itself), Endpoint of the VAL server.

3. The NRM server decides to create an MBS session. The MBS session creation procedure takes place as described in clause 14.3.4A.2.2.

NOTE 2: In case of LTE eMBMS and 5G MBS co-existence, the NRM server may trigger the establishment of eMBMS bearers as described in 3GPP TS 23.280 [3] (or it may establish a unicast bearer) based on the RAT capabilities supported by the affiliated members in the VAL service group X. If MBSF and BM-SC are co-located, TMGI used by 4G eMBMS can be the same as the MBS session ID.

NOTE 3: For the case of multi carrier support for broadcast MBS sessions, the NRM server may indicate the frequencies within a broadcast MBS service area by providing the MBS frequency selection area ID(s) (MBS FSA ID(s)) to the MB-SMF or indirectly via NEF.

4. The NRM server provides the NRM client with the information related to the created MBS session via an MBS session announcement. As described in table 7.3.2.2-1, the session announcement includes information such as the MBS session ID, MBS session mode (broadcast or multicast service type), and SDP information related to the MBS session.

Optionally, the NRM server includes the information elements related to the established eMBMS bearer once the NRM server has determined the need, as indicated in table 7.3.2.2-1. The NRM clients which camp on LTE will subsequently react to the information elements related to the eMBMS bearer as described in 3GPP TS 23.280 [3].

5. The NRM client stores the MBS session ID and other associated information.

6. The NRM client may send an MBS session announcement ack back to the NRM server.

7. Based on the MBS session mode (either multicast or broadcast), the following actions take place:

   7a. For multicast MBS sessions, NRM client initiates a UE session join request towards the 5GC using the information provided via the MBS session announcement. Hence, upon the first successful UE session join request, the multicast is then established, and the radio resources are reserved, if the session is in active state. The established session can either be in active or inactive state as indicated in 3GPP TS 23.247 [39]. The NRM client sends a UE session join notification towards the server as indicated in the MBS session announcement. If indicated in the MBS session announcement information, NRM clients report the monitoring state (i.e. the reception quality of the MBS session) back to the NRM server; or

   7b. For broadcast MBS sessions, if the NRM client is accessing over 5G, the session is established as part of the session creation procedures as described in 3GPP TS 23.247 [39], and the network resources are reserved both in 5GC and NG-RAN. The NRM clients start monitoring the reception quality of the broadcast MBS session. If indicated in the MBS session announcement information, NRM clients report the monitoring state (i.e. the reception quality of the MBS session) back to the NRM server.

NOTE 4: It is implementation specific whether the MBS session reception quality level is determined per MBS session, per media stream or per MBS QoS flow level via e.g., measurements of radio level signaling such as the reference signals from the NG-RAN node(s), packet loss.

8. The NRM clients provide a listening status notification related to the announced session (multicast or broadcast session) in the form of an MBS listening status report.

9. The NRM server provides a multicast/broadcast resource response to the VAL server.

10. An VAL service group communication via dynamic MBS session is established. The VAL server sends the downlink packet for the VAL service group communication session over the MBS session.

14.3.4A.3 MBS resources update

14.3.4A.3.1 General

The VAL server can create one or several MBS sessions via the NRM server, based on certain service requirements, a certain service area, or the activity status of multicast MBS sessions. However, during the life cycle of the MBS sessions, the VAL server may need to trigger the update of the sessions via the NRM server to meet emerging needs, including the service requirements, service area related parameters.

14.3.4A.3.2 Procedure for updating MBS resources without dynamic PCC rule

The procedure shown in figure 14.3.4A.3.2-1 presents an MBS session update procedure triggered by the VAL server via the NRM server (either directly interacting with the MB-SMF, or indirectly with NEF/MBSF). Within the update request, either the service requirements, MBS service area, activity status of multicast MBS session, or all three are done, as indicated in 3GPP TS 23.247 [39].

Pre-conditions:

- The NRM clients 1 to n are attached to the 5GS, registered and belong to the same active VAL service group.

- The NRM server has obtained the required information related to the MB-SMF, either locally configured or during initial session configuration.

- The MBS session is created with certain service requirements and optionally with a certain broadcast/multicast service area. The MBS session is announced to be associated with the VAL service group for group communication purposes.

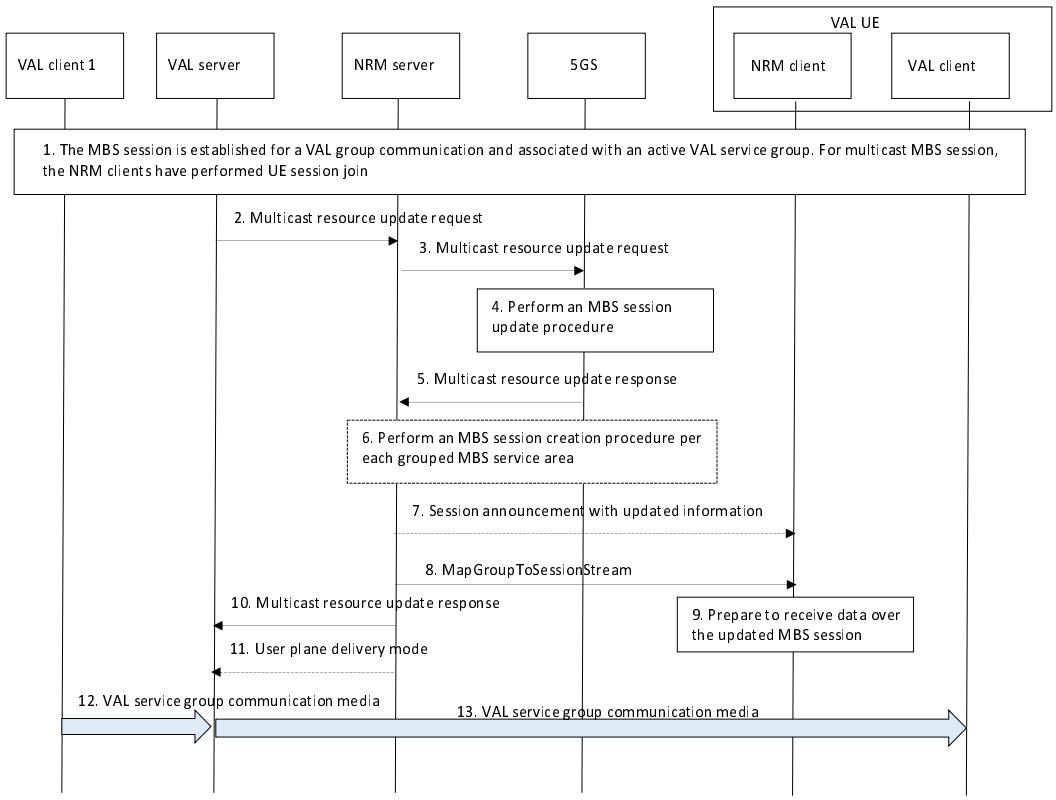

Figure 14.3.4A.3.2-1: MBS session update without dynamic PCC

1. An MBS session is established as described in in 3GPP TS 23.247 [39] (either a multicast or a broadcast session), and associated with a certain active VAL service group for group communication purposes. In the case of a multicast MBS session, the NRM clients have already joined the session.

2. The VAL server invokes the multicast resource update request to the NRM server once the need has emerged to modify some aspects for the given MBS session under consideration. The updated parameters are included, e.g., service requirements, MBS service area or both. In case of multicast MBS sessions, the VAL server may as well include the status (active or inactive) of the multicast MBS session to be set.

3. The NRM server sends an MBS session update request towards the 5GC, either directly or via NEF, as described in 3GPP TS 23.247 [39], either directly or indirectly via NEF.

4. Based on the needed requirements, the corresponding MBS session is accordingly modified at the 5GS as described in 3GPP TS 23.247 [39]. The update may lead to QoS Flow(s) addition, modification, or removal.

5. The NRM server receives an MBS session update response from the 5GS either directly or via NEF once the requested modifications are performed, and the indicated MBS session is updated accordingly.

6. In case of untrusted NRM server, if the requested MBS service area crosses several MB-SMF service areas, the requested MBS service area to be updated is partially accepted by the 5GC as described in 3GPP TS 23.247 [39]. The reduced MBS service area is grouped and provided by the NEF/MBSF in the response. Hence, the NRM server sends a new MBS session creation request as described in clause 14.3.4A.1.2. for each grouped MBS service area.

7. The NRM server may initiate a session announcement towards the NRM clients associated with the ongoing session in order to announce the updated information, if required, e.g., the updated service area or SDP information.

8. The NRM server sends an MapGroupToSessionStream over the configured MBS session providing the required information to receive the media related to the established VAL service group communication.

9. The NRM clients process the received information over the MapGroupToSessionStream in order to receive the associated VAL media over the specific MBS session stream.

10. The NRM server returns the multicast resource update response to the VAL server.
11. If the MBS session creation is failed towards the grouped MBS service areas in step 6, then the NRM server indicates to the VAL server to use unicast delivery for that grouped MBS service areas via by sending the user plane delivery mode message.
12. VAL client 1 sends media to the VAL server over unicast to be distributed for the established group communication.
13. The VAL server distributes the VAL media to the VAL clients 2 to n over the indicated streams.

14.3.4A.3.3 Procedure for updating MBS resources with dynamic PCC rule

The procedure shown in figure 14.3.4A.3.3-1 presents an MBS session update procedure triggered by the NRM server to the 5GC, either directly or via NEF/MBSF. Based on the required updates to be done, the NRM server needs to interact with the MB-SMF to update the MBS service area and multicast activity status, with the PCF to update the required QoS requirements, or sequentially both to update all the above, as indicated in 3GPP TS 23.247 [39].

Pre-conditions:

- The NRM clients 1 to n are attached to the 5GS, registered and belong to the same active VAL service group.
- The NRM server has obtained the required information related to the MB-SMF, either locally configured or during initial session configuration.
- The MBS session is created with certain service requirements and optionally with a certain broadcast/multicast service area. The MBS session is announced to be associated with the VAL service group for group communication purposes.

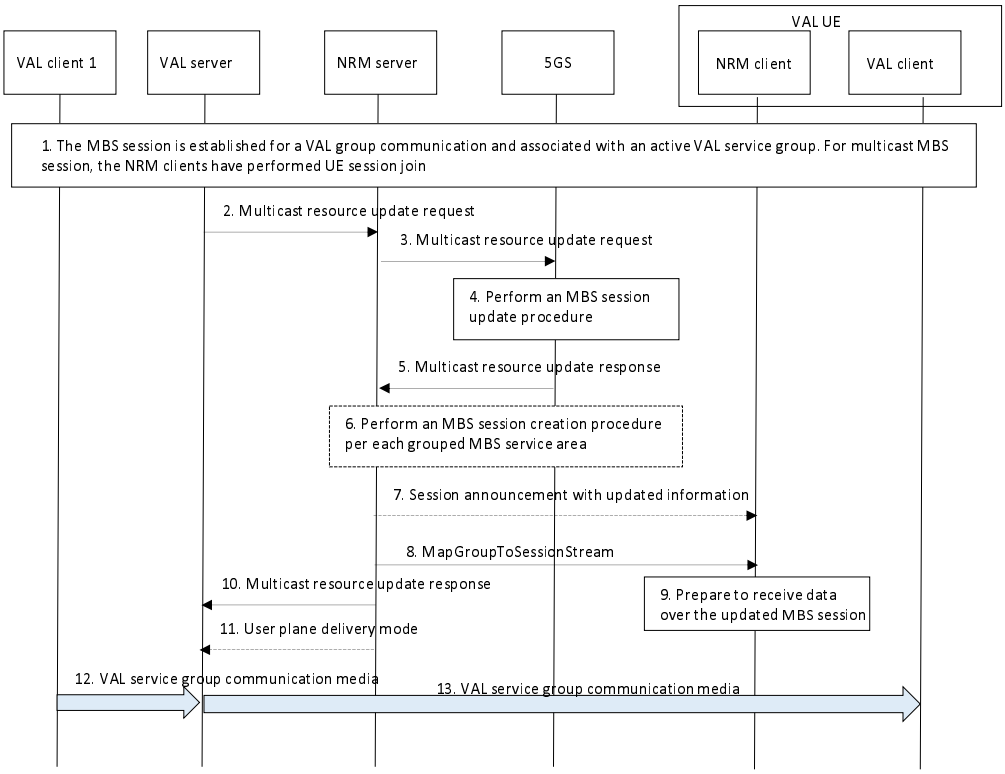

Figure 14.3.4A.3.3-1: MBS session update with dynamic PCC

1. An MBS session is established as described in 3GPP TS 23.247 [39] (either a multicast or a broadcast session), and associated with a certain active VAL service group for group communication purposes. In the case of a multicast MBS session, the NRM clients have already joined the session.

2. The VAL server invoke the multicast resource update request to the NRM server once the need has emerged to modify some aspects for the given MBS session under consideration. The updated parameters are included, e.g., service requirements, service area or both.

3. The NRM server sends an MBS session update request towards the 5GC as described in 3GPP TS 23.247 [39], either directly or indirectly via NEF.

NOTE 1: The updated service area information is required for local MBS and for broadcast MBS services.

4. Based on the update requirements the MBS session is updated with PCC procedure as described in 3GPP TS 23.247 [39].

5. The NRM server receives an MBS session update response from the 5GC either directly or via NEF once the requested modifications are performed, and the indicated MBS session is updated accordingly.

6. In case of untrusted NRM server, if the requested MBS service area crosses several MB-SMF service areas, the requested MBS service area to be updated is partially accepted by the 5GC, as described in 3GPP TS 23.247 [39]. The reduced MBS service area is grouped and provided by the NEF/MBSF in the response. Hence, the NRM server sends a new MBS session creation request as described in clause 14.3.4A.1.2. for each grouped MBS service area.

7. The NRM server may initiate a session announcement towards the NRM clients associated with the ongoing session in order to announce the updated information if required, e.g., the updated service area or SDP information.

NOTE 2: The updated service area information is required for local MBS and for broadcast MBS services.

8. The NRM server sends an MapGroupToSessionStream over the MBS session providing the required information to receive the media related to the established VAL service group communication.

9. The NRM server returns the multicast resource update response to the VAL server.

10. The NRM clients process the received information over the MapGroupToSessionStream in order to receive the associated VAL media over the specific MBS session stream.

11. If the MBS session creation is failed towards the grouped MBS service areas in step 6, then the NRM server indicates to the VAL server to use unicast delivery for that grouped MBS service areas via by sending the user plane delivery mode message.

12. VAL client 1 sends media to the VAL server over unicast to be distributed for the established group communication.

13. The VAL server distributes the VAL media to the VAL clients 2 to n over the indicated streams.

14.3.4A.4 MBS resource deletion

14.3.4A.4.1 General

The VAL server can decide to release a certain MBS session once it is no longer further utilized for the associated VAL service group communication, e.g., the VAL service group is no longer active, the VAL media transmission is over and no further VAL media to be delivered, group communication is terminated. The MBS session deletion procedure leads to releasing the network resources associated to that MBS session.

NOTE: It is up to implementation of VALserver to decide whether to release the MBS session or re-use it for subsequent group operations.

To delete the MBS session, the VAL server invokes the multicast/broadcast resource release service of NRM server which further triggers the NRM server to send an MBS session deletion request to the 5GS providing the corresponding MBS session ID. The MBS session deletion request is sent to the MB-SMF (directly or via NEF/MBSF) when PCC is

not used. However, if dynamic PCC rule is utilized, a policy authorization deletion request is initially sent to the PCF. Further details of the MBS session deletion are provided in 3GPP TS 23.247 [39].

NRM server further informs the NRM client with the MBS session de-announcement, so that the VAL UE stops monitoring the broadcast MBS session or leaves the multicast MBS session. This procedure is applied for both broadcast MBS session and multicast MBS session.

14.3.4A.4.2 Procedure

The procedure in figure 14.3.4A.4.2-1 describes the MBS session deletion aspects for group communication.

Pre-conditions:

- NRM clients 1 to n are attached to the 5GS, registered and affiliated to the same active VAL service group.
- An MBS session is configured to address the corresponding VAL service group with certain service requirements and optionally with a certain broadcast/multicast service area. The session is announced and established for group communication purposes for the VAL service group.

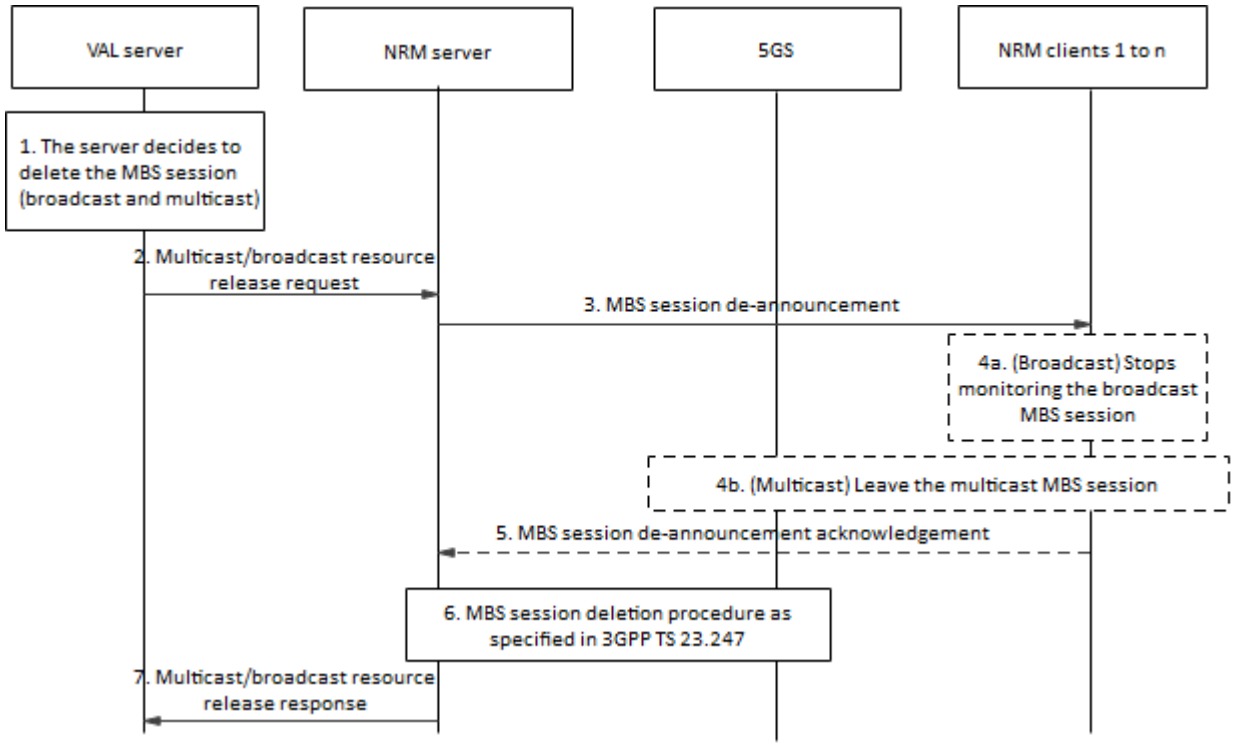

Figure 14.3.4A.4.2-1: MBS session deletion procedure.

1. The VAL server decides to delete the MBS session for the associated VAL group communication, either multicast or broadcast session.
2. The VAL server invokes the multicast/broadcast resource release service of the NRM server by sending the multicast/broadcast resource release request.
3. Upon receiving the multicast/broadcast resource release request, the NRM server sends an MBS session de-announcement message with the MBS session ID towards the NRM client(s). Upon receiving the MBS session de-announcement message, either 4a or 4b is performed.

4a. If the MBS session identified by MBS session ID is a broadcast MBS session, the UE(s) stops monitoring the broadcast MBS session and removes the broadcast MBS session related information.

4b. If the MBS session identified by MBS session ID is a multicast MBS session, the joined UE(s) initiate an MBS session leave procedure to leave the indicated MBS session in order to release the respective network resources, as defined in 3GPP TS 23.247 [39].

5. Subsequently, the NRM clients may send an MBS session de-announcement acknowledgement message to the NRM server indicating the status of MBS session.

6. The NRM server initiates the MBS session deletion procedure with the 5GC (either directly or through NEF/MBSF) in order to stop using the configured MBS session and release the corresponding network resources. The NRM server indicates within the MBS session release request the corresponding MBS session ID. The MBS session deletion procedure can either be with or without a dynamic PCC rule, as indicated in 3GPP TS 23.247 [39].

7. The NRM server returns the multicast/broadcast resource release response to the VAL server indicating the result.

14.3.4A.5 Request to activate / de-activate multicast MBS sessions

14.3.4A.5.1 General

In case of multicast MBS sessions, the members affiliated to a certain VAL service group need to initiate a UE session join request towards the 5GC in order to receive the VAL media sent via the associated MBS session. The UE session join request enables the reservation of NG-RAN resources for the members of the VAL group. However, it is not necessary that the VAL media is delivered over the whole time the multicast MBS session is associated to the group under consideration. Therefore, the VAL server is able to efficiently utilize and control the reservation of radio resources based on the availability of VAL data to be delivered via the activation and de-activation procedure with NRM server. This presents more flexibility and efficient use of resources different from LTE.

The most suitable scenario to activate/de-activate a certain multicast MBS session is based on whether there is a VAL group communication, taking place over that associated session to the VAL service group. In this manner, the VAL server can activate the associated multicast session once a VAL group communication takes place, then deactivate it once the VAL group communication is over. Whether the multicast session is activated (i.e., in an active state), or de-activated (in an inactive state), the VAL group is associated to the multicast session and its members are within a UE session join.

The activation or de-activation request is initiated by the VAL server towards the NRM server which further interacts either directly with the MB-SMF or indirectly with NEF/MBSF.

NOTE: The activation of de-activation procedure may also be triggered by MB-SMF based on receiving notification from MB-UPF based on the availability of VAL data to be transmitted.

14.3.4A.5.2 Multicast MBS session activation procedure

The procedure shown in figure 14.3.4A.5.2-1 presents the multicast MBS session activation procedure initiated by the VAL server.

Pre-conditions:

- NRM clients are attached to the 5GS, registered and affiliated to the same VAL service group X.
- The NRM server has directly performed (or via NEF/MBSF) an MB-SMF discovery and selection, unless the corresponding information is locally configured.
- The multicast MBS session for NRM group communications associated to VAL service group X.
- The MBS session is created and announced to address VAL group communication related to the associated VAL service group X with certain service requirements and optionally with a certain service area.

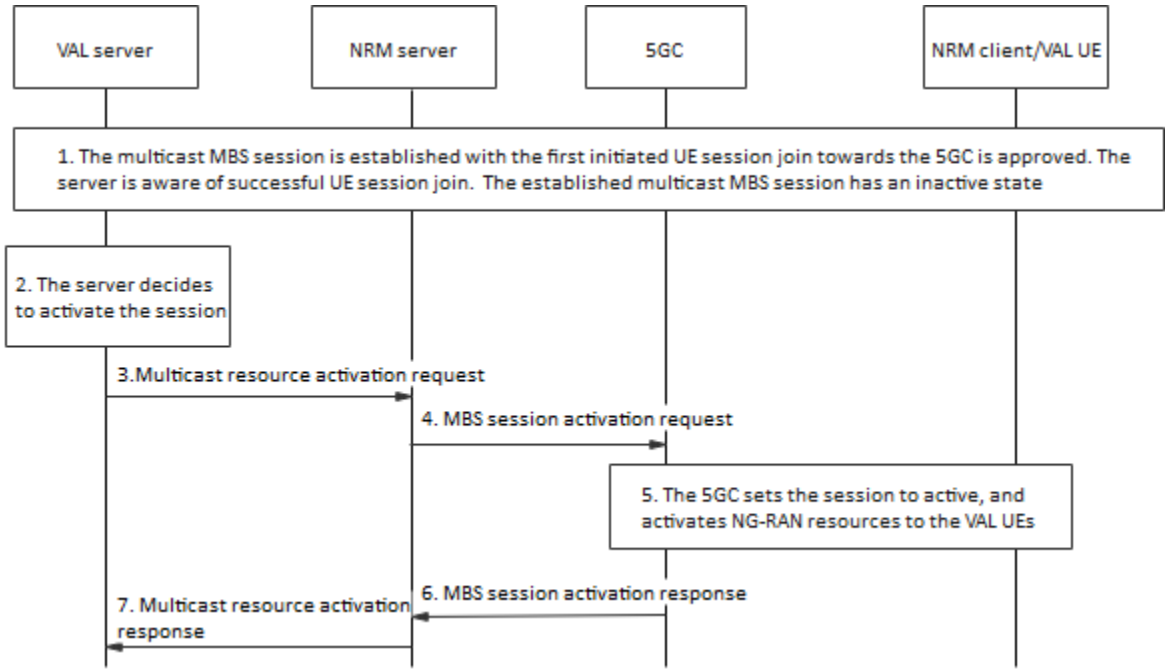

Figure 14.3.4A.5.2-1: Multicast MBS session activation procedure.

1. The multicast MBS session is established as the first UE session join request, which is initiated by the first VAL UE towards 5GC, is granted. At this stage, the multicast MBS session is established with an inactive state.
2. The VAL server decides to activate the multicast MBS session as VAL data is needed to be transmitted over the session to the VAL service group X, as a VAL group communication is to take place over the associated MBS session.
3. The VAL server invokes the multicast resource activation request provided by NRM server, the MBS session ID is included.
4. Upon receiving the request in step 3, the NRM server sends an MBS session activation request towards the 5GC, either directly to the MB-SMF or via NEF/MBSF, indicating the TMGI to be activated.
5. The 5GC changes the session status to "active" and finds the list of joined VAL UEs associated with the session and activates the NG- RAN resources for VAL data delivery.
6. The 5GC may send an MBS session activation response to the NRM server indicating that the requested multicast MBS session has been activated.
7. The NRM server returns the multicast resource activation response to the VAL server.

14.3.4A.5.3 Multicast MBS session de-activation procedure

The procedure shown in figure 14.3.4A.5.3-1 presents the multicast MBS session activation procedure initiated by the VAL server.

Pre-conditions:

- NRM clients are attached to the 5GS, registered and affiliated to the same VAL service group X.
- The NRM server has directly performed (or via NEF/MBSF) an MB-SMF discovery and selection, unless the corresponding information is locally configured.
- A multicast MBS session is created and announced to address the corresponding VAL service group with certain service requirements and optionally with a certain multicast service area.

- The VAL UE have already joined the multicast MBS session and are able to receive the VAL data over the associated MBS session.

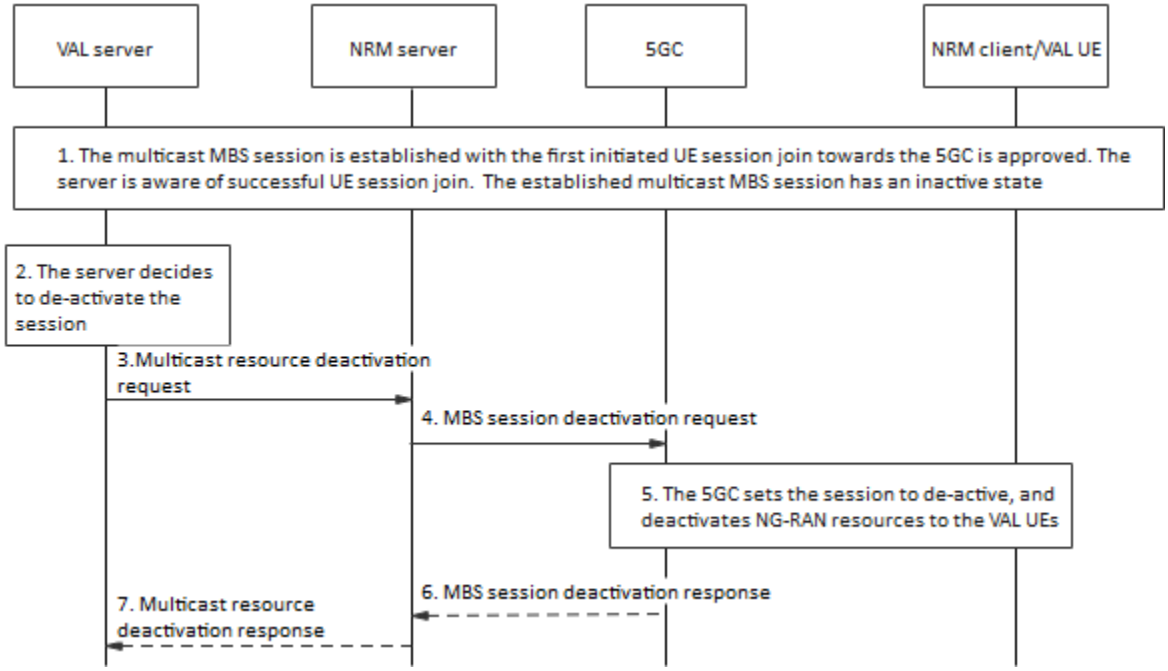

Figure 14.3.4A.5.3-1: Multicast MBS session deactivation procedure.

1. The group communication associated with VAL service group X takes place, and the corresponding VAL data is delivered over the associated multicast MBS session, hence the MBS session has an active state.

2. The VAL server decides to deactivate the multicast MBS session, as no further VAL data to be delivered to the associated group, or the VAL group communication is over, and no further VAL media is to be delivered.

3. The VAL server invokes the multicast resource deactivation request provided by NRM server, the MBS session ID is included.

4. Upon receiving the request in step 3, the NRM server sends an MBS session deactivation request towards the 5GC, either directly to the MB-SMF or via NEF/MBSF, indicating the TMGI to be deactivated.

4. The 5GC changes the session state to "inactive" and deactivates the radio resources associated with the joined VAL UEs.

5. The 5GC may send an MBS deactivation response to the server indicating that the requested multicast MBS session has been inactivated.

7. The NRM server may return the multicast resource deactivation response to the VAL server.

14.3.4A.6 VAL service group media transmissions over 5G MBS sessions

14.3.4A.6.1 General

The VAL server can decide to configure an MBS session per VAL service group to transmit the media related to the corresponding VAL group communications. Such group communications can comprise different service requirements. For that, multicast and broadcast MBS sessions need to be configured with multiple MBS QoS flows to address different service requirements, e.g., different required QoS, provided by the NRM server. For instance, application-level control messages or media associated to a group communication can comprise different QoS requirements. Also, different type of group communications can comprise different QoS requirements, e.g., emergency group communication should be handled with a higher priority than normal group communication.

The configuration of multiple MBS QoS flows to address different service requirements is associated to the assignment of different streams (e.g., different ports) within an MBS session.

The established multicast MBS session can either be in active or inactive state, where the former indicates the activation of radio resources hence transmitting the VAL media to the associated VAL service group, and the latter indicates their deactivation as no VAL media is being transmitted. The VAL server may initiate the activation of multicast MBS sessions once the VAL service group is established and active, as well as once the VAL media is available for transmission. For this purpose, the VAL server sends a multicast MBS session activation request towards the NRM indicating the MBS session ID to be activated, and the NRM server further interacts with the 5GS to complete the MBS session activation.

Similar to the use of eMBMS, the NRM server shall provide the associated information between a specific group communication and the stream to be used within an MBS session to the UE. This information could be sent in advance in an MBS session announcement or could be provided on demand in an additional signalling message for the MBS session, e.g., MapGroupToSessionStream (similar to the MapGroupToBearer in eMBMS).

14.3.4A.6.2 Procedure

The procedure in figure 14.3.4A.6.2-1 describes how media related to a specific group communication can be distributed over a configured MBS session which consist of multiple QoS flows, i.e. addressing different service requirements. The procedure is applicable for both the pre-created MBS session case as described in 14.3.4A.2.2 and the dynamic MBS session case as described in 14.3.4A.2.3. For simplicity, the figure 14.3.4A.6.2-1 shows that the MBS session is pre-created prior to the group communication establishment.

Pre-conditions:

- VAL UE 1 to n are attached to the 5GS, registered and belong to the same VAL service group X.
- The VAL server has decided to use an MBS session for VAL service group communications associated to VAL service group X.

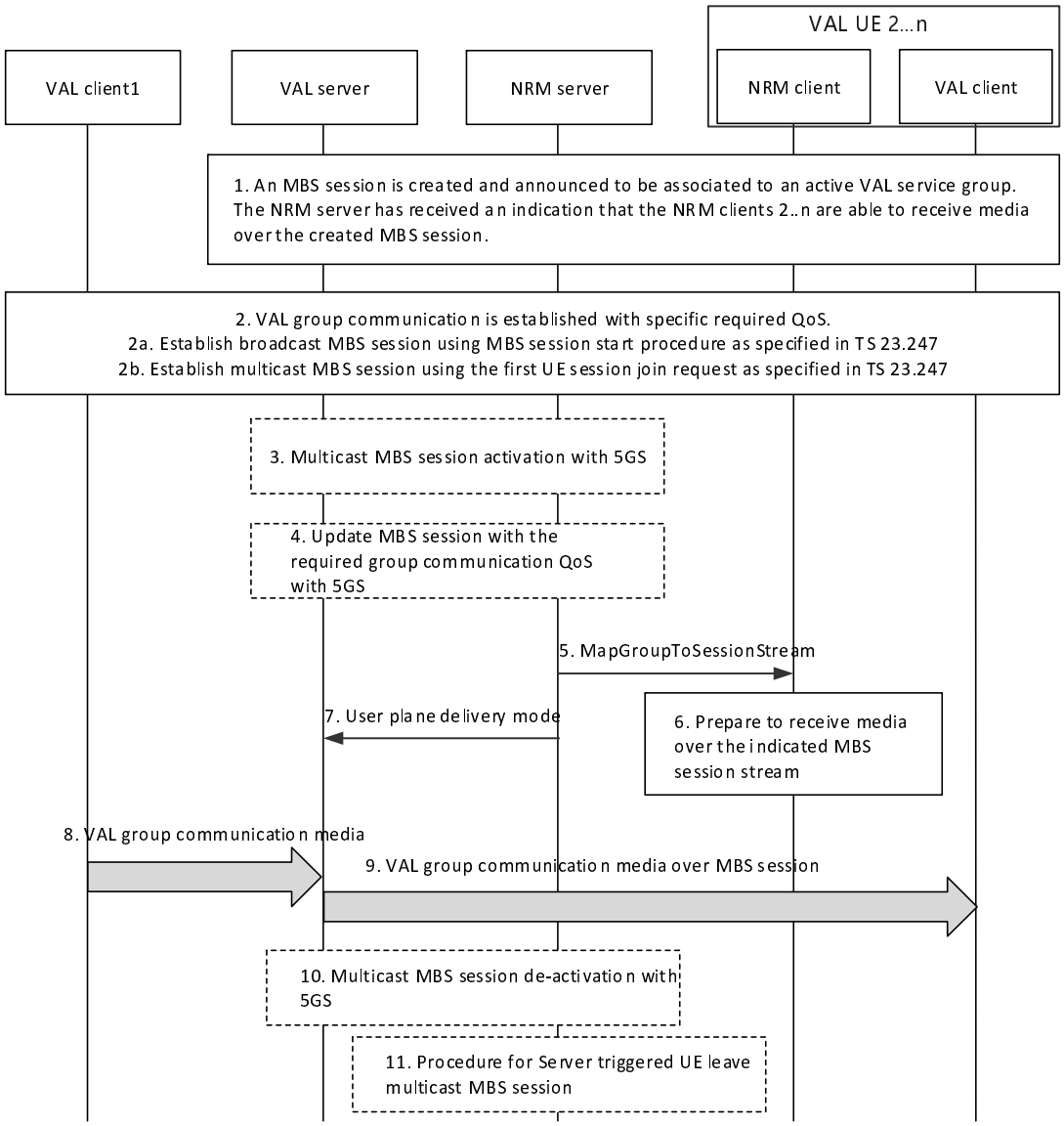

Figure 14.3.4A.6.2-1: VAL service group media transmission over MBS sessions

1. The VAL server creates a multicast or a broadcast MBS session targeting group communications associated to VAL service group X via the NRM server, as being specified in clause 14.3.4A.2. Therefore, the VAL server can provide default service requirements to be addressed by the MBS session.

   The MBS session is announced by NRM server and received by NRM client 2 to n. The NRM server has identified that VAL UE 2 to n can receive media over the MBS sessions, e.g. based on a notification from NRM clients indicating the successful join of the multicast MBS session or a monitoring report of the broadcast MBS session (similar to the listening status report used for MBMS).

2. A new VAL group communication is established for the VAL service group X consisting of a specific required service requirements, e.g. a VAL service emergency group communication. The group communication setup can be done over unicast.

2a. For broadcast MBS sessions, the session is established as described in 3GPP TS 23.247 [39].

2b. For multicast MBS session, the session is established upon the acceptance of the first UE session join request initiated from the VAL UE towards the 5GS, as described in 3GPP TS 23.247 [39]. The multicast session can then have either an active or an inactive state.

3. The VAL server may initiate the multicast MBS activation towards the NRM as described in clause 14.3.4A.5 in order to activate the multicast MBS session in case the session has an inactive state.

4. Considering that the established group communication requires a specific QoS, e.g. an VALemergency group communication which requires higher priority (i.e. better ARP), the VAL server initiates an MBS session update to the NRM to provide the new required service requirements, if not done during the MBS session creation in step 1, as described in clause 14.3.4A.2. The MBS session should then be updated and an additional QoS flow may be configured.

5. The NRM server sends a MapGroupToSessionStream to NRM clients 2 to n over the configured MBS session providing the required stream information to receive the media related to the specific established VAL group communication within the MBS session.

6. NRM clients process the MapGroupToSessionStream information to receive the related media over the specific MBS session stream.

7. The NRM server sends the user plane delivery mode message to the VAL server to instruct the VAL server to switch to MBS delivery.

8. VAL client 1 sends media to the VAL server over unicast to be distributed for the established group communication.

9. The VAL server distributes the media to VAL clients 2 to n over the indicated stream within the established MBS session.

NOTE: The VAL server can stop the unicast delivery (if ongoing) towards the VAL clients considering the UE session join notification or the MBS listening status report.

10. The VAL server may initiate the multicast MBS session deactivation towards the NRM as described in clause 14.3.4A.5, in order to deactivate the multicast MBS session.

11. The NRM server may further trigger the UE to leave multicast MBS session.

14.3.4A.7 Aplication level control signalling over 5G MBS sessions

14.3.4A.7.1 Description

The VAL server may use an 5G MBS session for application level control signalling. An 5G MBS session for application level control signalling is typically used for the purposes beyond the benefit for using 5G for resource efficiency, e.g. for improved MC service performance (KPIs), handling of high load scenarios.

Similar to the usage of eMBMS, both broadcast and multicast 5MBS session for application level control signalling may be used to transmit the following messages, for example:

- MBS session announcement for media sessions
- Group application paging
- Group dynamic data (e.g. status of the group)

5G MBS session for application level control signalling is created in a service area that is larger than the estimated service for media MBS session. The service area for the media sessions is mainly based on counting of group members in each defined service area. The MBS session for application level control signalling is also created with a QoS that is better than MBS media session since the packet loss requirements are much stricter.

The NRM client shall not send responses to group-addressed application level control signalling unless instructed or configured to respond.

14.3.4A.7.2 Procedure

The procedure in figure 14.3.4A.7.2-1 shows only one of the receiving VAL UE using a 5G MBS session.

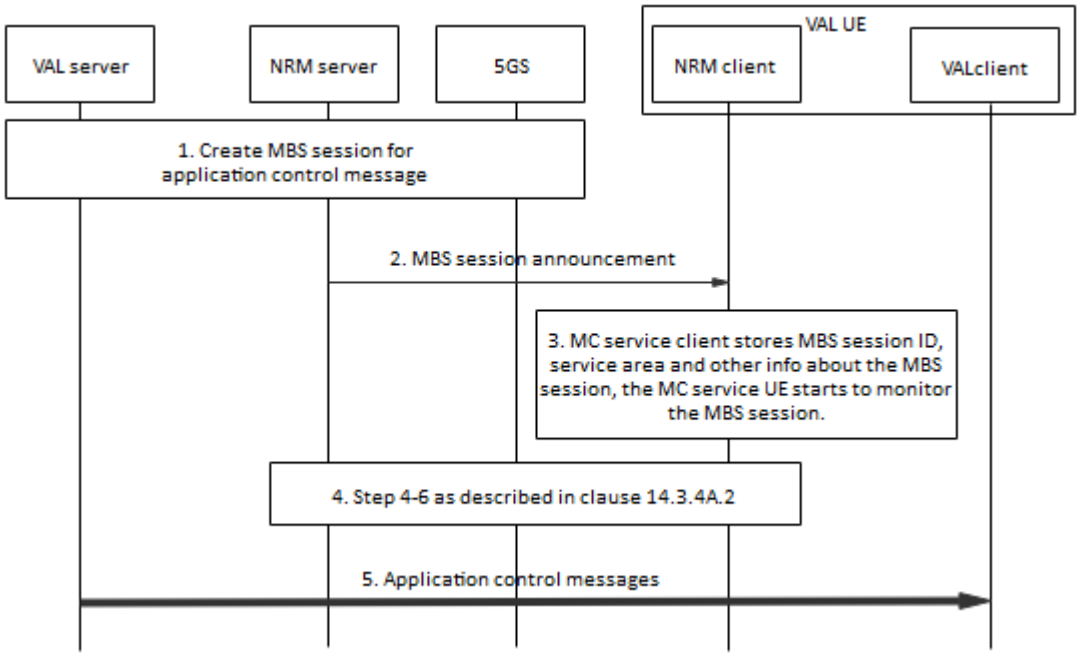

Figure 14.3.4A.7.2-1: Use of 5G MBS for application-level control signalling

1. The VAL server determines to create MBS session for application-level control signalling, the VAL server initiated the 5G MBS session establishment via the NRM is done according to clause 14.3.4A.2.
2. The NRM server passes the 5G MBS session info for the service description associated with the 5G MBS session to the NRM client. The NRM client obtains the MBS session ID, from the service description.

NOTE: For 5G MBS and 4G MBMS co-existence, the MBMS bearers activation and MBS session announcement are performed as specified in the procedure for pre-created MBS session and session announcement.

3. The NRM client stores the information associated with the MBS session ID. The NRM client uses the MBS session ID and other 5G MBS session related information to enable monitoring of the 5G MBS session by the VAL UE.
4. Steps 4 to 6 defined in clause 14.3.4A.2 are performed.
5. The VAL server transmits MC application control messages over the MBS session.

14.3.4A.8 Service continuity between 5G MBS delivery and unicast delivery

14.3.4A.8.1 General

This clause addresses the issue of VAL data delivery over MBS session, specifically, to maintain the service continuity when switching between 5G MBS delivery and unicast delivery.

14.3.4A.8.2 Service continuity for broadcast MBS session

14.3.4A.8.2.1 General

This solution provides the procedure which allows the NRM client to report the broadcast reception quality to the NRM server which is used to make the decision whether to use the unicast delivery to the VAL UE(s) which are suffering bad broadcast reception quality due to e.g., move out of the broadcast service area.

An NRM client monitors the broadcast MBS session to receive VAL data. Based on the received quality (e.g., radio level quality, RTP packet loss), the NRM client needs to inform the NRM server that the NRM client is able to receive the VAL data on the broadcast MBS session with sufficient quality or not.

This estimation of the broadcast reception quality may be dependent on, for example, the modulation and coding scheme (MCS) and measurements from the reference signals from the NG-RAN node(s), RTP packet loss, BLER of the received VAL data.

14.3.4A.8.2.2 Procedures

14.3.4A.8.2.2.1 Service continuity from broadcast to unicast

The procedure in figure 14.3.4A.8.2.2.1-1 illustrates the VAL UE which is receiving VAL data via broadcast MBS session is switched to unicast delivery because the VAL UE suffers from bad broadcast reception quality due to e.g., moving out of the broadcast service area. It shows only one of the receiving VAL UEs receiving the broadcast MBS session.

Pre-conditions:

1. The VAL group communication is ongoing and the VAL data (e.g., DL media, application layer control signalling) is transmitted via broadcast MBS session.
2. The NRM client is receiving the VAL data (e.g., DL media, application layer control signalling) via the broadcast MBS session.
3. The NRM client(s) already have the associated information (e.g., SDP) to receive the unicast delivery during the group communication establishment phase.
4. An VAL group communication session is ongoing and the DL VAL data is transmitted over broadcast MBS session.

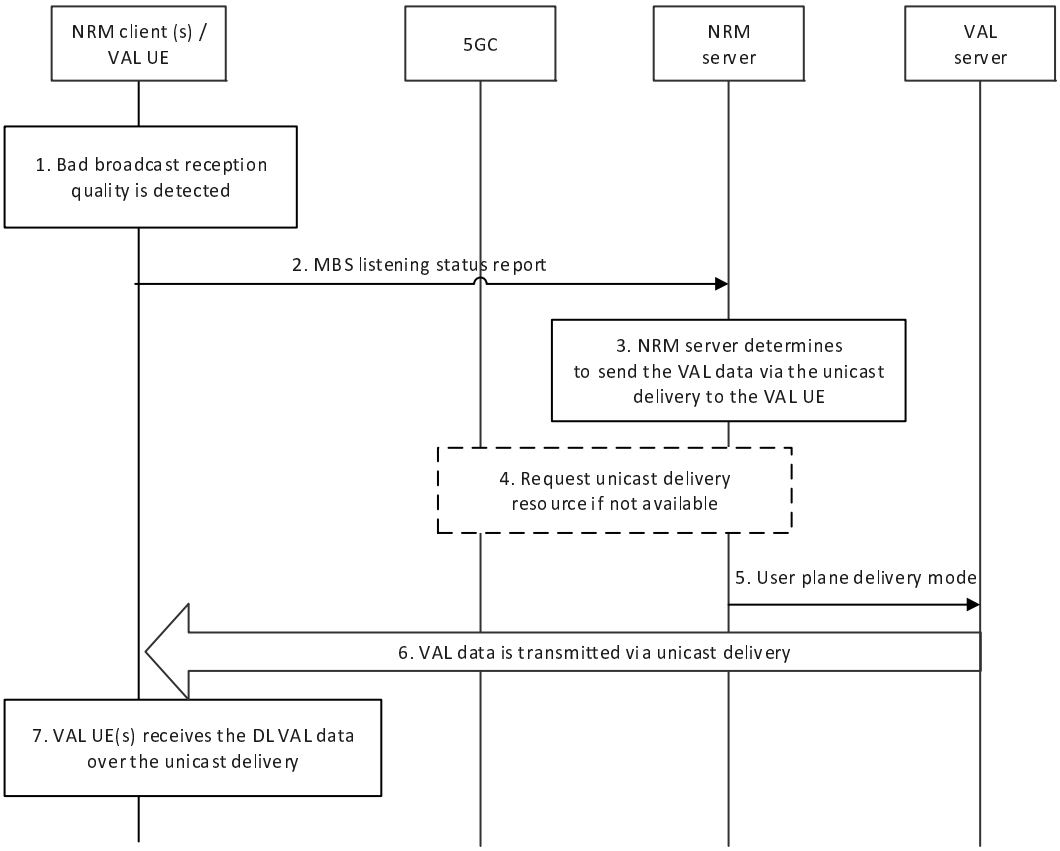

Figure 14.3.4A.8.2.2.1-1: Service continuity from broadcast to unicast

1. The NRM client detects that it suffers bad broadcast reception due to e.g., moving out of the broadcast service area of the announced MBS session ID. The NRM client may determine the broadcast reception quality by using the BLER of the received media. When no media is received, the quality estimation can consider the reference signals and the modulation and coding scheme (MCS).

2. The NRM client sends MBS listening status report which indicates the broadcast reception quality associated with the MBS session ID is not sufficient to receive media. The NRM client may also map the determined broadcast reception quality to a broadcast reception quality level. The broadcast reception quality level indicates at which specific broadcast reception quality level the VAL data has been received.

NOTE 1: It is implementation that the broadcast reception quality level can be determined per MBS session, per media stream or per MBS QoS flow level via e.g., measurements of radio level signalling such as the reference signals from the NG-RAN node(s), packet loss.

NOTE 2: The set of MBS reception quality levels and the mapping of the determined broadcast reception quality to those levels are implementation.

NOTE 3: The frequency of VAL UE sending listening reports can be limited to prevent signalling congestion. E.g., the VAL UE can stop monitoring the broadcast reception quality and send the MBS listening status report only once when it moves outside of the broadcast service area.

3. The NRM server based on the report from the participant, determines that the UE is not able to receive the media or the QoS requirements is not satisfied. The NRM server determines the VAL media (e.g., DL media, application layer control signalling) needs to be delivered via the unicast delivery to the reported NRM client.

4. If the unicast QoS flow is not satisfied, the NRM server interacts with the 5GC to update the QoS requirements.

5. The NRM server informs the VAL server to send the VAL data via the unicast delivery towards the reported NRM client by sending a user plane delivery mode message.

6. The NRM server sends the VAL media via the unicast delivery towards the NRM client which suffers bad broadcast reception quality.

7. The NRM client then receives the DL VAL data via both broadcast MBS session and unicast delivery.

14.3.4A.8.2.2.2 Service continuity from unicast to broadcast

The procedure in figure 14.3.4A.8.2.2.2-1 illustrates the VAL UE receiving VAL data via unicast delivery being switched to broadcast MBS session as the UE enters the broadcast service area where the NG-RAN is broadcasting the VAL media of the ongoing group communication. The VAL UE now is able to receive the VAL data via the broadcast MBS session. Only one of the receiving VAL UEs receiving the broadcast MBS session is shown.

Pre-conditions:

1. The VAL group communication is ongoing and the VAL data (e.g., DL media, application layer control signalling) is transmitted via broadcast MBS session in the broadcast service areas.

2. The VAL UE is receiving the VAL data (e.g., DL media, application layer control signalling) via the unicast delivery.

3. The NRM client has already received the broadcast MBS session announcement, MapVALGroupToSessionStream information and enters the broadcast service area.

4. A VAL group communication session is ongoing and the broadcast MBS session is used by the VAL server to deliver the VAL data of the group communication. The VAL UE is receiving the VAL data via the unicast delivery.

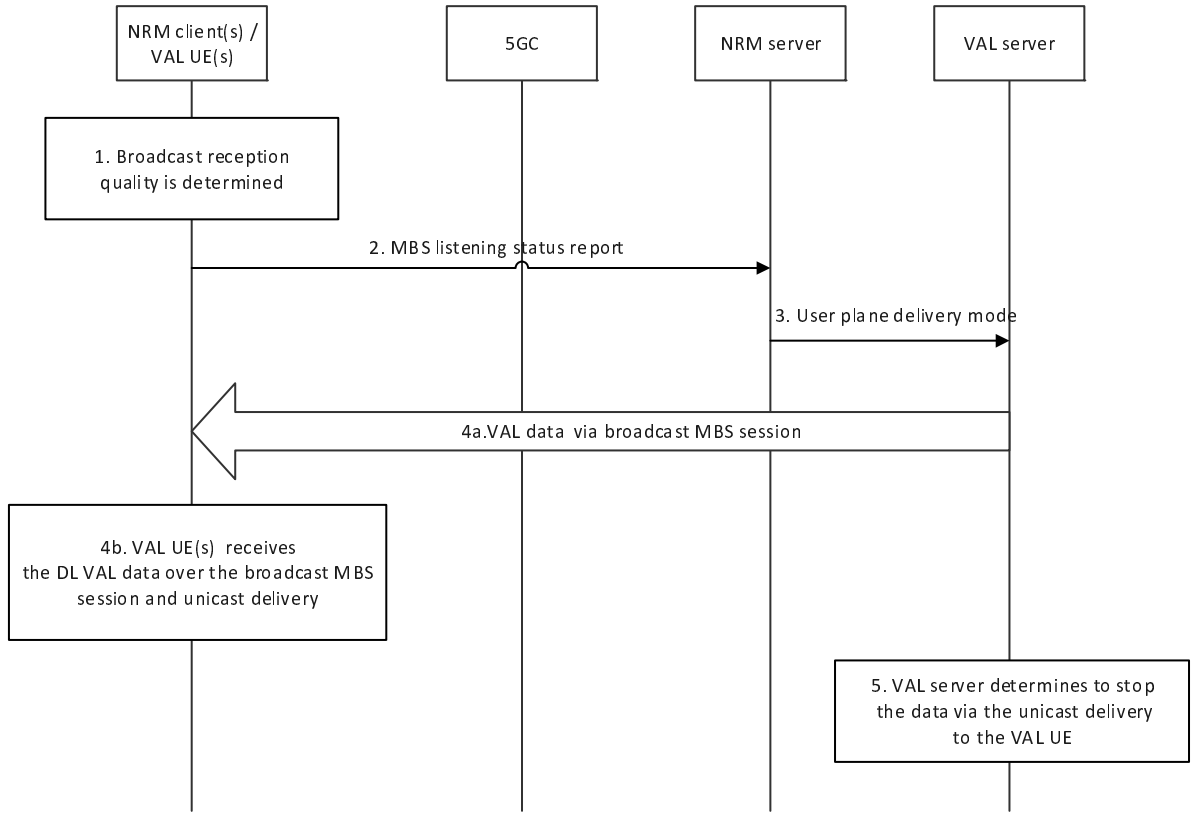

Figure 14.3.4A.8.2.2.2-1: Service continuity from unicast to broadcast

1. The NRM client detects that it is able to receive the broadcast media due to e.g., moving into the broadcast service area of the announced MBS session ID. The NRM client may determine the broadcast reception quality by using the BLER of the received media. When no media is received, the quality estimation can consider the reference signals and the modulation and coding scheme (MCS).

2. The NRM client sends MBS listening status report which indicates the broadcast reception quality associated with the MBS session ID is sufficient to receive VAL data. The NRM client may also map the determined broadcast reception quality to a broadcast reception quality level. The broadcast reception quality level indicates at which specific broadcast reception quality level the VAL data has been received.

NOTE 1: The set of MBS reception quality levels and the mapping of the determined broadcast reception quality to those levels are up to implementation.

NOTE 2: It is up to implementation that the broadcast reception quality level can be determined per MBS session, per media stream or per MBS QoS flow level via e.g., measurements of radio level signals, such as the reference signals from the NG-RAN node(s), or packet loss.

3. The NRM server determines the VAL UE is able to receive the VAL data via the the broadcast MBS session, and the NRM server sends a user plane delivery mode to the VAL server indicating to stop the unicast delivery.

4. Based on the MapVALGroupToSessionStream received before, the NRM client receives the DL VAL data via both the broadcast MBS session and the unicast delivery.

NOTE 3: If any information about the broadcast MBS session stream has changed, the NRM server provides the MapVALGroupToSessionStream again.

5. The VAL server, based on the user plane delivery mode message, determines to stop sending the VAL data (e.g., DL media, application layer control signalling) via the unicast delivery to the reporting NRM client. After then, the NRM client receives the VAL data only via the broadcast MBS session.

14.3.4A.8.3 Service continuity for multicast MBS session

14.3.4A.8.3.1 General

The NRM server may also switch between multicast and unicast by utilizing application layer mechanisms similar to switching between broadcast and unicast as specified in clause 14.3.4A.8.2. If indicated in the MBS session announcement information, the NRM client reports the monitoring state (i.e., the reception quality of the MBS session) back to the NRM server.

NOTE: Once the VAL UE has successfully joined the multicast MBS session and started to receive the VAL data via the multicast MBS session, then the network mechanism specified in 3GPP TS 23.247 [39] will deliver the media from the NRM server via the 5GC Individual MBS traffic delivery method or the 5GC Shared MBS traffic delivery method towards the VAL UE(s). The usage of 5GC Individual MBS traffic delivery method or the 5GC Shared MBS traffic delivery method is transparent to the NRM server and VAL server.

14.3.4A.9 Service continuity between 5G MBS delivery and unicast delivery

14.3.4A.9.1 General

This clause addresses the issue of VAL data delivery over MBS session, specifically, to maintain the service continuity when switching between 5G MBS delivery and unicast delivery.

14.3.4A.9.2 Service continuity for broadcast MBS session

14.3.4A.9.2.1 General

This solution provides the procedure which allows the NRM client to report the broadcast reception quality to the NRM server which is used to make the decision whether to use the unicast delivery to the VAL UE(s) which are suffering bad broadcast reception quality due to e.g., move out of the broadcast service area.

An NRM client monitors the broadcast MBS session to receive VAL data. Based on the received quality (e.g., radio level quality, RTP packet loss), the NRM client needs to inform the NRM server that the NRM client is able to receive the VAL data on the broadcast MBS session with sufficient quality or not.

This estimation of the broadcast reception quality may be dependent on, for example, the modulation and coding scheme (MCS) and measurements from the reference signals from the NG-RAN node(s), RTP packet loss, BLER of the received VAL data.

14.3.4A.9.2.2 Procedures

14.3.4A.9.2.2.1 Service continuity from broadcast to unicast

The procedure in figure 14.3.4A.9.2.2.1-1 illustrates the VAL UE which is receiving VAL data via broadcast MBS session is switched to unicast delivery because the VAL UE suffers from bad broadcast reception quality due to e.g., moving out of the broadcast service area. It shows only one of the receiving VAL UEs receiving the broadcast MBS session.

Pre-conditions:

1. The VAL group communication is ongoing and the VAL data (e.g., DL media, application layer control signalling) is transmitted via broadcast MBS session.
2. The NRM client is receiving the VAL data (e.g., DL media, application layer control signalling) via the broadcast MBS session.
3. The NRM client(s) already have the associated information (e.g., SDP) to receive the unicast delivery during the group communication establishment phase.
4. An VAL group communication session is ongoing and the DL VAL data is transmitted over broadcast MBS session.

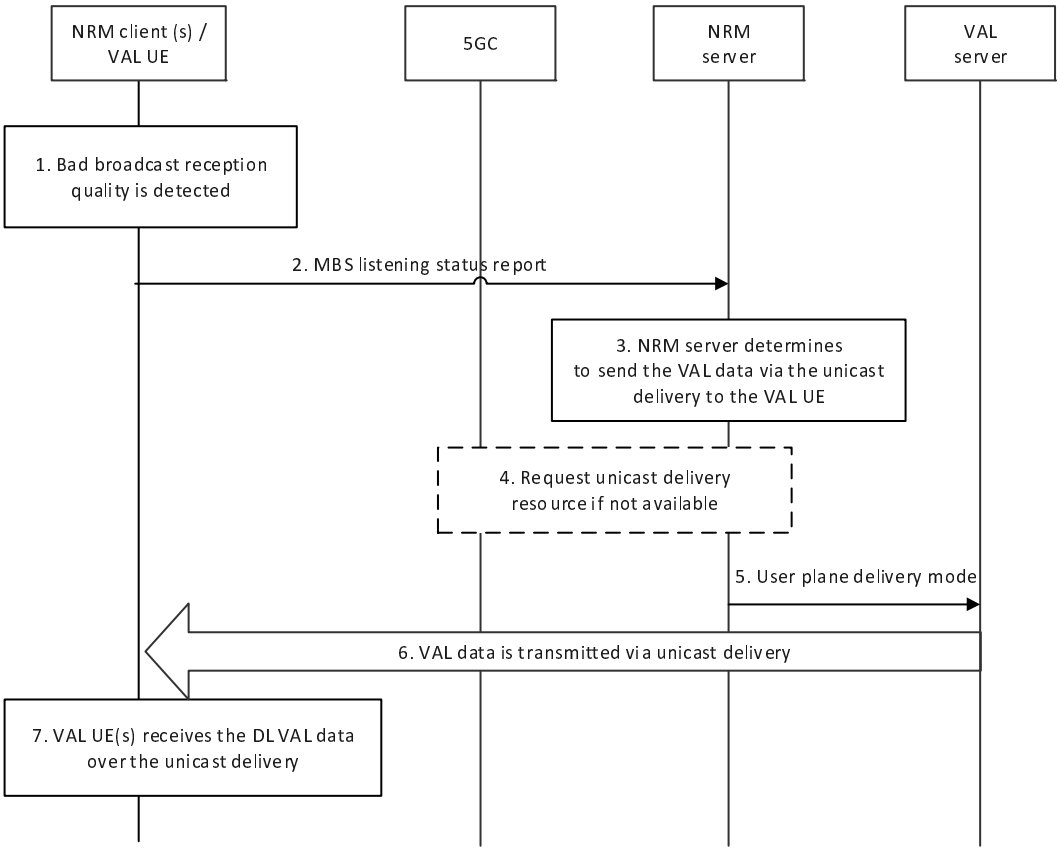

Figure 14.3.4A.9.2.2.1-1: Service continuity from broadcast to unicast

1. The NRM client detects that it suffers bad broadcast reception due to e.g., moving out of the broadcast service area of the announced MBS session ID. The NRM client may determine the broadcast reception quality by using the BLER of the received media. When no media is received, the quality estimation can consider the reference signals and the modulation and coding scheme (MCS).

2. The NRM client sends MBS listening status report which indicates the broadcast reception quality associated with the MBS session ID is not sufficient to receive media. The NRM client may also map the determined broadcast reception quality to a broadcast reception quality level. The broadcast reception quality level indicates at which specific broadcast reception quality level the VAL data has been received.

NOTE 1: It is implementation that the broadcast reception quality level can be determined per MBS session, per media stream or per MBS QoS flow level via e.g., measurements of radio level signalling such as the reference signals from the NG-RAN node(s), packet loss.

NOTE 2: The set of MBS reception quality levels and the mapping of the determined broadcast reception quality to those levels are implementation.

NOTE 3: The frequency of VAL UE sending listening reports can be limited to prevent signalling congestion. E.g., the VAL UE can stop monitoring the broadcast reception quality and send the MBS listening status report only once when it moves outside of the broadcast service area.

3. The NRM server based on the report from the participant, determines that the UE is not able to receive the media or the QoS requirements is not satisfied. The NRM server determines the VAL media (e.g., DL media, application layer control signalling) needs to be delivered via the unicast delivery to the reported NRM client.

4. If the unicast QoS flow is not satisfied, the NRM server interacts with the 5GC to update the QoS requirements.

5. The NRM server informs the VAL server to send the VAL data via the unicast delivery towards the reported NRM client by sending a user plane delivery mode message.

6. The NRM server sends the VAL media via the unicast delivery towards the NRM client which suffers bad broadcast reception quality.

7. The NRM client then receives the DL VAL data via both broadcast MBS session and unicast delivery.

14.3.4A.9.2.2.2 Service continuity from unicast to broadcast

The procedure in figure 14.3.4A.8.2.2.2-1 illustrates the VAL UE receiving VAL data via unicast delivery being switched to broadcast MBS session as the UE enters the broadcast service area where the NG-RAN is broadcasting the VAL media of the ongoing group communication. The VAL UE now is able to receive the VAL data via the broadcast MBS session. Only one of the receiving VAL UEs receiving the broadcast MBS session is shown.

Pre-conditions:

1. The VAL group communication is ongoing and the VAL data (e.g., DL media, application layer control signalling) is transmitted via broadcast MBS session in the broadcast service areas.
2. The VAL UE is receiving the VAL data (e.g., DL media, application layer control signalling) via the unicast delivery.
3. The NRM client has already received the broadcast MBS session announcement, MapVALGroupToSessionStream information and enters the broadcast service area.
4. A VAL group communication session is ongoing and the broadcast MBS session is used by the VAL server to deliver the VAL data of the group communication. The VAL UE is receiving the VAL data via the unicast delivery.

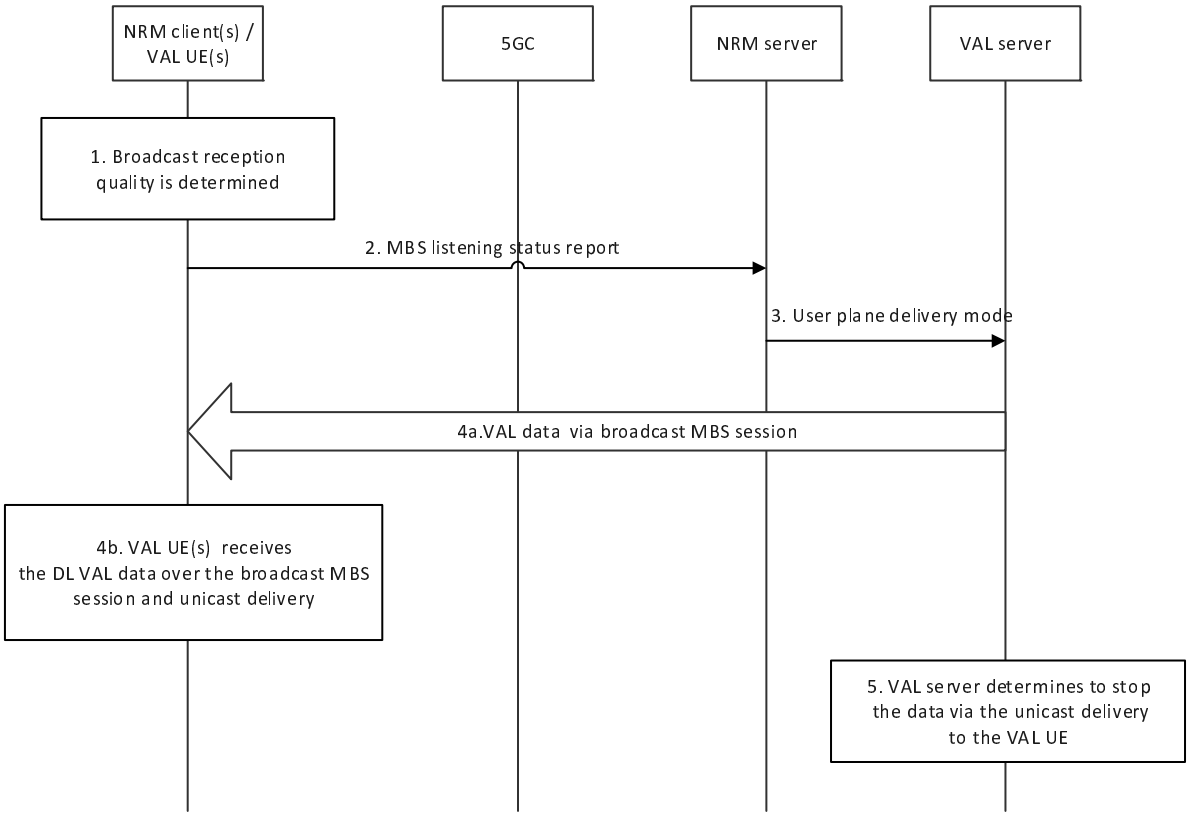

Figure 14.3.4A.9.2.2.2-1: Service continuity from unicast to broadcast

1. The NRM client detects that it is able to receive the broadcast media due to e.g., moving into the broadcast service area of the announced MBS session ID. The NRM client may determine the broadcast reception quality by using the BLER of the received media. When no media is received, the quality estimation can consider the reference signals and the modulation and coding scheme (MCS).
2. The NRM client sends MBS listening status report which indicates the broadcast reception quality associated with the MBS session ID is sufficient to receive VAL data. The NRM client may also map the determined broadcast reception quality to a broadcast reception quality level. The broadcast reception quality level indicates at which specific broadcast reception quality level the VAL data has been received.

NOTE 1: The set of MBS reception quality levels and the mapping of the determined broadcast reception quality to those levels are up to implementation.

NOTE 2: It is up to implementation that the broadcast reception quality level can be determined per MBS session, per media stream or per MBS QoS flow level via e.g., measurements of radio level signals, such as the reference signals from the NG-RAN node(s), or packet loss.

3. The NRM server determines the VAL UE is able to receive the VAL data via the the broadcast MBS session, and the NRM server sends a user plane delivery mode to the VAL server indicating to stop the unicast delivery.

4. Based on the MapVALGroupToSessionStream received before, the NRM client receives the DL VAL data via both the broadcast MBS session and the unicast delivery.

NOTE 3: If any information about the broadcast MBS session stream has changed, the NRM server provides the MapVALGroupToSessionStream again.

5. The VAL server, based on the user plane delivery mode message, determines to stop sending the VAL data (e.g., DL media, application layer control signalling) via the unicast delivery to the reporting NRM client. After then, the NRM client receives the VAL data only via the broadcast MBS session.

14.3.4A.9.3 Service continuity for multicast MBS session

14.3.4A.9.3.1 General

The NRM server may also switch between multicast and unicast by utilizing application layer mechanisms similar to switching between broadcast and unicast as specified in clause 14.3.4A.9.2. If indicated in the MBS session announcement information, the NRM client reports the monitoring state (i.e., the reception quality of the MBS session) back to the NRM server.

NOTE: Once the VAL UE has successfully joined the multicast MBS session and started to receive the VAL data via the multicast MBS session, then the network mechanism specified in 3GPP TS 23.247 [39] will deliver the media from the NRM server via the 5GC Individual MBS traffic delivery method or the 5GC Shared MBS traffic delivery method towards the VAL UE(s). The usage of 5GC Individual MBS traffic delivery method or the 5GC Shared MBS traffic delivery method is transparent to the NRM server and VAL server.

14.3.4A.10 VAL service inter-system switching between 5G and LTE

14.3.4A.10.1 General

The VAL server delivers the VAL data to the VAL UE(s) without being aware of the mobility of the VAL UE with the assistance and guidance of the NRM server. When working in transport only mode, the NRM server guides the NRM clients throughout the VAL data transmission for switching between the LTE and 5G systems. For this purpose, the location management client may send location related information to the location management server, similar to the one defined in clause 9, which is triggered due to its location change – in this case due to Radio Access Technology (RAT) change, to inform the NRM server hence the latter provides guidance related to how to receive the VAL data after the location update.

The procedures cover both the deployment scenarios with/without MBSF/MBSTF. The procedures specify four inter-system switching related scenarios as follows:

1. Inter-system switching from 5G MBS session to LTE eMBMS bearer, as in 14.3.4A.10.2

2. Inter-system switching from 5G MBS session to LTE unicast bearer, as in 14.3.4A.10.3

3. Inter-system switching from LTE eMBMS to 5G MBS session, as in 14.3.4A.10.4

4. Inter-system switching from LTE eMBMS to 5G unicast PDU session, as in 14.3.4A.10.5

In all the inter-system switching related scenario described in 14.3.4A.10.2, 14.3.4A.10.3, 14.3.4A.10.4 and 14.3.4A.10.5, the functional entity that resides in 5GS may be NEF, or MBSF, or MB-SMF for session creation and together with PCF or PCC related interaction.

NOTE: There will be a service interruption when the VAL server performs path switch between 5G and LTE bearers or sessions.

14.3.4A.10.2 Inter-system switching from 5G MBS session to LTE eMBMS bearer

The procedure provided in figure 14.3.4A.10.2-1 describes how the NRM server handles inter-system switching when the VAL UE switches from 5G to LTE network, where the NRM server is able to provide the VAL data to the clients over eMBMS bearer(s).

Pre-conditions:

- NRM clients are attached to the 5GS, registered.
- The VAL service can be provided via both 5GS and EPS.
- The NRM client(s) is within the eMBMS service area.
- It is assumed that the NRM client(s) has not received the eMBMS bearer announcement while camping in 5GS.

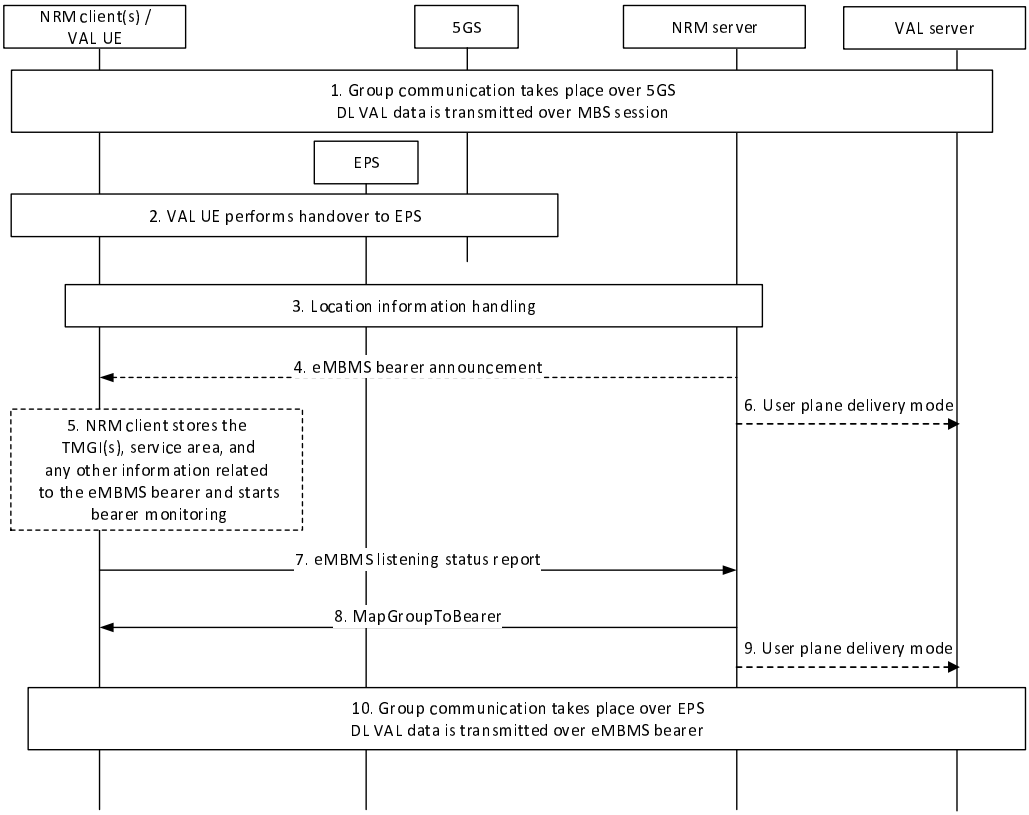

Figure 14.3.4A.10.2-1: Inter-system switching from 5G MBS session to LTE eMBMS bearer.

1. An VAL group communication takes place, and the VAL data is delivered over 5G MBS session (either broadcast or multicast session mode), which is associated to the VAL group X.
2. The VAL UE performs handover to EPS.
3. Location information indicating the RAT change from the VAL UE is provided to the NRM server. VAL UE`s location information is provided via the location management client, triggered by RAT change, to the location management server, where the latter provides the location information to the NRM server. Also, location information handling can be based on notifications provided from the network to the NRM server related to 5GS supporting EPS interworking, as specified in 3GPP TS 23.501 [10], 3GPP TS 23.502 [11], and 3GPP TS 23.503 [12]. For that, the NRM server can subscribe to receive notifications of specific events from the network. For instance, the NRM server can subscribe to PCF related notifications (via N5 or Rx) for specific events, e.g., access network information notification and change of access type. Also, when SCEF+NEF is deployed, the NRM server can subscribe to SCEF+NEF related notifications for specific events, e.g., core network (CN) type change.

4. The NRM server analyses the RAT change and decides how to deliver the DL VAL data. If the NRM server decides to serve the client via eMBMS bearer, it may send an eMBMS bearer announcement. This step is optional as the bearer announcement related information could be sent in advance (implementation specific).
5. If not already available, the NRM client stores the announced TMGI(s), service area, and any relevant information to the eMBMS, which is delivered via the bearer announcement. As a result, the NRM client starts monitoring the bearer.
6. The NRM server may inform the VAL server to stop sending DL VAL data via the MBS by sending the user plane delivery mode message, e.g., when the last UE leaves the MBS session or move out of the MBS service area.
7. The NRM client sends an eMBMS listening status report to inform the server of its ability of receiving DL VAK data over the specified bearer.
8. The NRM server sends the necessary information related to receiving the DL VAL data in the form of the MapGroupToBearer.
9. The NRM server may inform the VAL server to start sending DL VAL data via the eMBMS by sending the user plane delivery mode message, e.g., the first UE(s) enters the eMBMS service area.
10. The VAL group communication takes place over EPS, and the VAL data is transmitted over an eMBMS bearer.

14.3.4A.10.3 Inter-system switching from 5G MBS session to LTE unicast bearer

The procedure provided in figure 14.3.4A.10.3-1 describes how the NRM server handles inter-system switching when the VAL UE switches from 5G to LTE network, where the VAL server is unable to provide the VAL services to the VAL UE over eMBMS bearer.

Pre-conditions:

- NRM clients are attached to the 5GS, registered and affiliated to the same VAL group X.
- The VAL services can be provided via both 5GS and EPS.

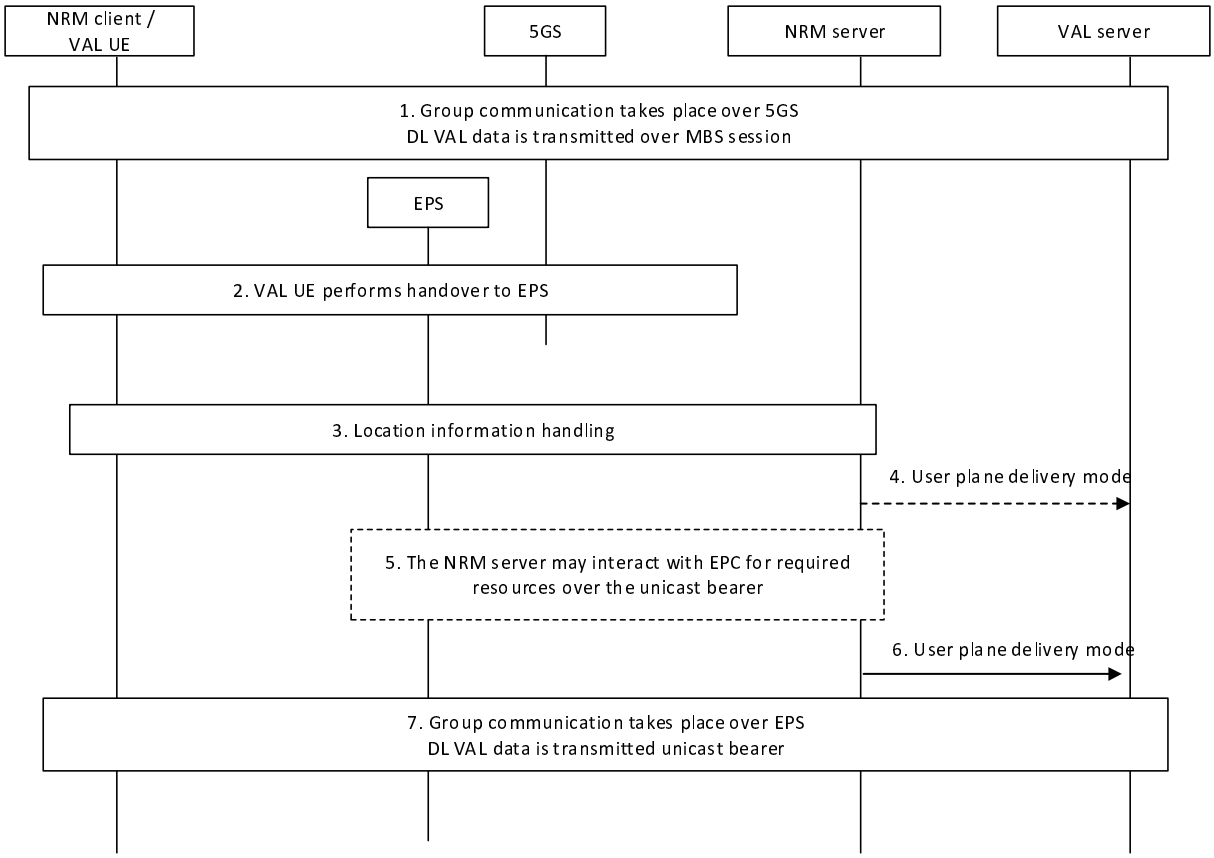

Figure 14.3.4A.10.3-1: Inter-system switching from 5G MBS session to LTE unicast bearer.

1. An VAL group communication takes place, and the VAL data is delivered over 5G MBS session (either broadcast or multicast session mode), which is associated to the VAL group X.

2. The VAL UE performs handover to EPS.

3. Location information indicating the RAT change from the VAL UE is provided to the NRM server. VAL UE`s location information is provided via the location management client, triggered by RAT change, to the location management server, where the latter provides the location information to the NRM server.

   Also, location information handling can be based on notifications provided from the network to the NRM server related to 5GS supporting EPS interworking, as specified in 3GPP TS 23.501 [10], 3GPP TS 23.502 [11], and 3GPP TS 23.503 [12]. For that, the NRM server can subscribe to receive notifications of specific events from the network. For instance, the NRM server can subscribe to PCF related notifications (via N5 or Rx) for specific events, e.g. access network information notification and change of access type. Also, when SCEF+NEF is deployed, the NRM server can subscribe to SCEF+NEF related notifications for specific events, e.g. core network (CN) type change.

4. The NRM server may inform the VAL server to stop sending DL VAL data via the MBS by sending the user plane delivery mode message, e.g., when the last UE leaves the MBS session or move out of the MBS service area.

5. The NRM server may interact with the EPC for providing the required media resources over the unicast bearer, if not already allocated.

6. The NRM server informs the VAL server to send DL VAL data to the VAL UE via the LTE unicast bearer by sending the user plane delivery mode message.

7. The VAL group communication takes place over EPS, and the DL VAL data is transmitted over a LTE unicast bearer.

14.3.4A.10.4 Inter-system switching from LTE eMBMS to 5G MBS session

The procedure provided in figure 14.3.4A.10.4-1 describes how the NRM server handles inter-system switching when the VAL UE switches from LTE network to 5G, where the NRM server is able to provide the VAL services to the client over 5G MBS sessions (either broadcast or multicast).

Pre-conditions:

- NRM clients are attached to the EPC.
- The VAL services can be provided via both 5GS and EPS.
- The NRM client(s) is within the service area (if the session is limited to an area), where the MBS session is configured.
- It is assumed that the NRM client(s) has not received the 5G MBS session announcement while camping in EPS.

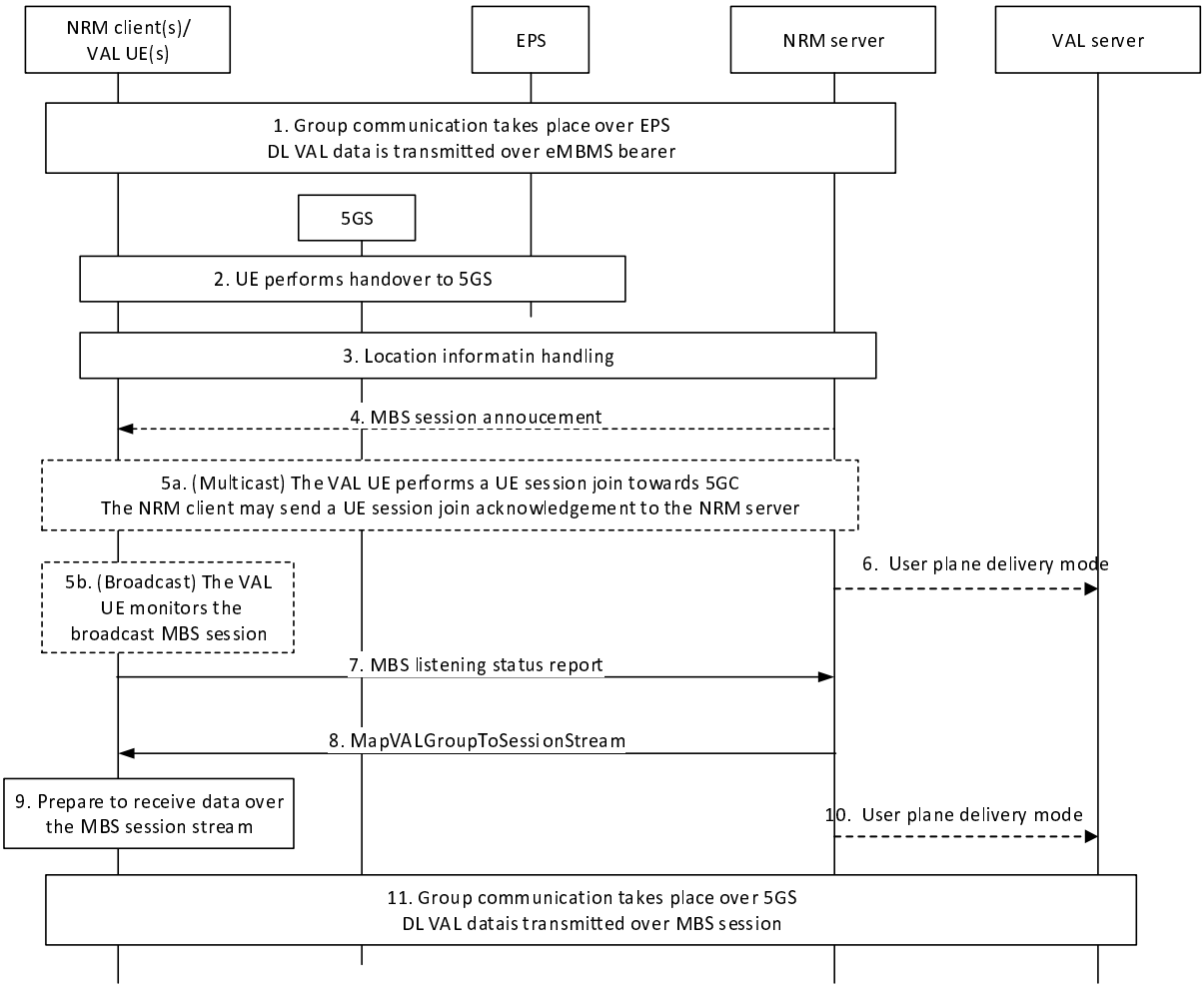

Figure 14.3.4A.10.4-1: Inter-system switching from LTE eMBMS bearer to 5G MBS sessions (either broadcast or multicast).

1. An VAL group communication takes place, and the DL VAL data is delivered over eMBMS bearer, which is associated to the VAL group X.
2. The VAL UE performs handover to 5GS.
3. Location information indicating the RAT change from the VAL UE is provided to the NRM server. VAL UE`s location information is provided via the location management client, triggered by RAT change, to the location management server, where the latter provides the location information to the NRM server.

Also, location information handling can be based on notifications provided from the network to the NRM server related to 5GS supporting EPS interworking, as specified in 3GPP TS 23.501 [10], 3GPP TS 23.502 [11], and 3GPP TS 23.503 [12]. For that, the NRM server can subscribe to receive notifications of specific events from the network. For instance, the NRM server can subscribe to PCF related notifications (via N5 or Rx) for specific events, e.g., access network information notification and change of access type. Also, when SCEF+NEF is deployed, the NRM server can subscribe to SCEF+NEF related notifications for specific events, e.g., core network (CN) type change.

4. The NRM server analyses the RAT change and decides how to deliver the DL VAL data. If the NRM server decides to serve the client via 5G MBS session, it may send an MBS session announcement indicating information among others the session mode to serve the NRM client and the corresponding MBS session ID. This step is optional as the session announcement related information could be sent in advance (implementation specific).

5. The VAL UE acts according to the MBS session mode provided to receive the DL media.

5a. In case of multicast MBS sessions, the VAL UE performs a UE session join towards the 5GC indicating the MBS session ID to join. It may as well send a UE session join acknowledgement to the NRM server.

5b. In case of broadcast MBS sessions, the VAL UE starts monitoring the broadcast MBS session. 6. The NRM server may inform the VAL server to stop sending DL VAL data via the eMBMS bearer by sending the user plane delivery mode message, e.g., when the last UE moves out of the MBMS service area.

7. The NRM client sends an MBS listening status report to the server indicating its ability to receive media over the indicated MBS session.

8. The NRM server sends a MapVALGroupToSessionStream over the MBS session providing the required stream information to receive the media related to the group communication.

9. The NRM client processes the received information related to the DL VAL data over the MBS session.

10. The NRM server may inform the VAL server to start sending DL VAL data via the 5G MBS session by sending the user plane delivery mode message, e.g., the first UE(s) enters the MBS service area or joins the multicast MBS session.

11. The VAL group communication takes place over 5GS, and the DL VAL data is delivered over the broadcast or multicast MBS session.

14.3.4A.10.5 Inter-system switching from LTE eMBMS to 5G unicast PDU session

The procedure provided in figure 14.3.4A.10.5-1 describes how the NRM server handles inter-system switching when the VAL UE switches from LTE network to 5G, where the NRM server is able to provide the VAL services to the client over 5G MBS sessions (either broadcast or multicast).

Pre-conditions:

- NRM clients are attached to the EPC and affiliated to the same VAL group X.
- The VAL services can be provided via both 5GS and EPS.

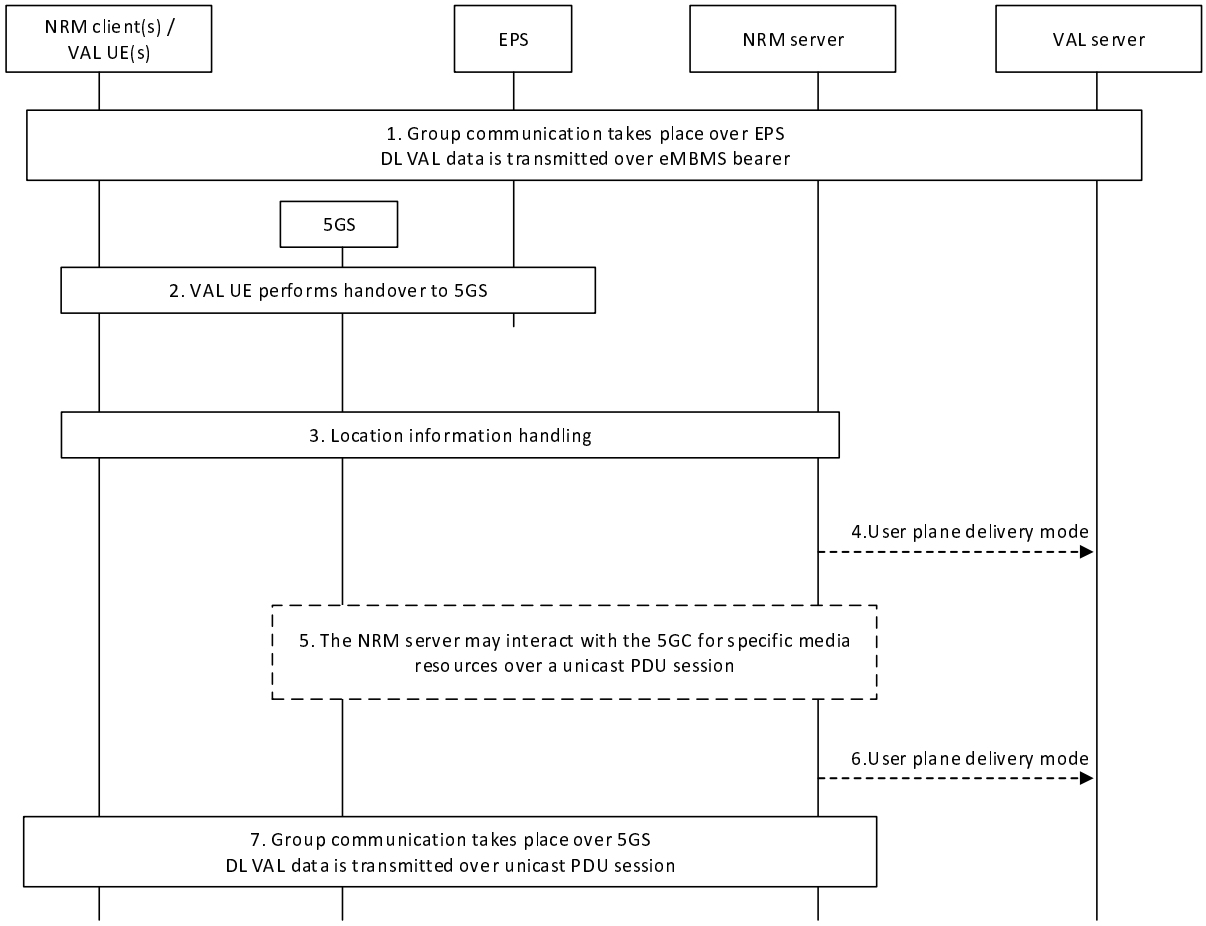

Figure 14.3.4A.10.5-1: Inter-system switching from LTE eMBMS bearer to 5G unicast PDU session.

1. An VAL group communication takes place, and the VAL data is delivered over eMBMS bearer, which is associated to the VAL group X.

2. The VAL UE performs handover to 5GS.

3. Location information indicating the RAT change from the VAL UE is provided to the NRM server. VAL UE`s location information is provided via the location management client, triggered by RAT change, to the location management server, where the latter provides the location information to the NRM server.

   Also, location information handling can be based on notifications provided from the network to the NRM server related to 5GS supporting EPS interworking, as specified in 3GPP TS 23.501 [10], 3GPP TS 23.502 [11], and 3GPP TS 23.503 [12]. For that, the NRM server can subscribe to receive notifications of specific events from the network. For instance, the NRM server can subscribe to PCF related notifications (via N5 or Rx) for specific events, e.g. access network information notification and change of access type. Also, when SCEF+NEF is deployed, the NRM server can subscribe to SCEF+NEF related notifications for specific events, e.g. core network (CN) type change.

4. The NRM server may inform the VAL server to stop sending DL VAL data via the eMBMS bearer by sending the user plane delivery mode message, e.g., when the last UE moves out of the LTE MBMS service area.

5. The NRM server may interact with the 5GC to request media resources (if not already allocated) with specific requirements over unicast PDU session, as it is able to serve the NRM client via unicast PDU session.

6. The NRM server informs the VAL server to send DL VAL data to the VAL UE via the PDU session by sending the user plane delivery mode message.

7. The VAL group communication takes place over 5GS, and the VAL data is delivered over unicast PDU session.

14.3.5 QoS/resource management for network-assisted UE-to-UE/VN group 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.
- 5G LAN-Type communication within a 5G VN group as specified in 3GPP TS 23.501 [10].

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, or for 5G LAN-type service such trigger may be initiated by the AF (e.g. on VAL UE1) that manages the corresponding 5G VN group.

The clause 14.3.5.2.1 describes the end-to-end QoS/resource management capability for network-assisted UE-to-UE communications for a single pair of UEs.

The clause 14.3.5.2.2 describes the end-to-end QoS/resource management capability for network-assisted UE-to-UE communications for a group of UEs.

14.3.5.2.1 Procedure for a single pair of UEs

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 for a single pair of UEs.

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 3GPP TS 23.502 [11]).

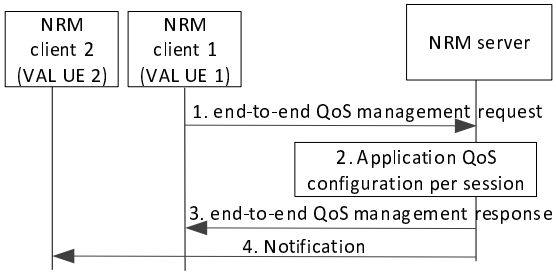

Figure 14.3.5.2.1-1 end-to-end QoS management request / response

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.

14.3.5.2.2 Procedure for a group of UEs

Figure 14.3.5.2.2 illustrates the procedure where the NRM server is initiating the end-to-end QoS/resource management capability for network-assisted UE-to-UE communications for a group of UEs.

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 a group of VAL UEs) are connected to one or more PLMNs and have ongoing PDU sessions.

Note : The NRM client2 (of VAL UE 2) can be any VAL UEs in the group of VAL UEs.

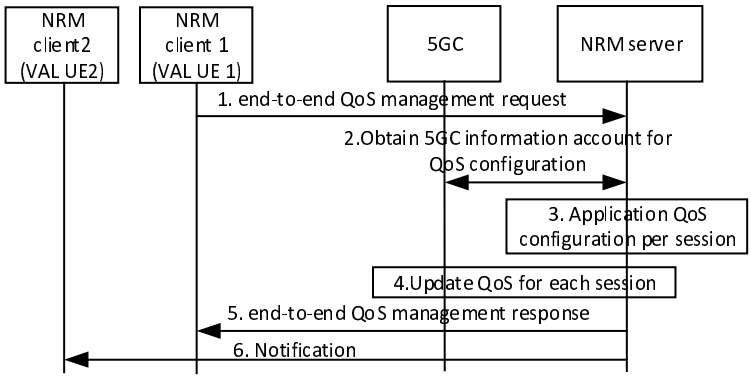

Figure 14.3.5.2.2 end-to-end QoS management request / response for a group of UEs

1. The NRM server receives from the AF on NRM client 1 (of VAL UE 1) the end-to-end QoS management request for managing the QoS on UE-to-UE traffic for a group of UEs.

2. The NRM server retrieves from 5GC or subscribe to 5GC to obtain additional VAL-UE associated information for each member in the group identified by the VAL group ID, which is account for decomposition. The VAL-UE associated information could be from the 5GC (NEF Monitoring Events as in 3GPP TS 23.502 [11], QoS sustainability analytics as in 3GPP TS 23.288 [34]) or SEAL LMS (on demand location reporting).

3. The NRM server configures the application QoS parameters by decomposing the end-to-end QoS requirements (UE-to-UE traffic for any two UEs in a group) to application QoS parameters for each individual session (uplink network session for ingress group member and downlink network session for egress group member). The NRM server needs to take the additional VAL-UE associated information into account for evaluation during such decomposition.

4. The NRM/SEAL server, acting as AF, sends to the 5GC a "Procedures for AF requested QoS for a UE or group of UEs not identified by a UE address" to set the application QoS parameters respectively for uplink network session for each ingress group member in the group and for downlink network session for egress group member.

   Additionally, the NRM/SEAL server may activate monitoring of the performance to receive QoS monitoring event notifications from 5GC by setting the (optionally with Alternative QoS Profiles) in the request, in this case the AF may receive the QoS downgrade notification for e.g. latency thus to initiate the NRM-assisted coordinated QoS provisioning for 5G LAN-Type communication in clause 14.3.5.3.x

5. The NRM server sends to the NRM client 1an end-to-end QoS management response with a positive or negative acknowledgement of the request.

6. If the NRF server receives the end-to-end QoS management request including VAL UE2 as any of the List of VAL UEs, then 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).

The clause 14.3.5.2.1 describes the end-to-end QoS/resource management capability for network-assisted UE-to-UE communications for a single pair of UEs.

The clause 14.3.5.2.2 describes the end-to-end QoS/resource management capability for network-assisted UE-to-UE communications for a group of UEs.

14.3.5.3.1 Procedure for a single pair of UEs

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 for a single pair of UEs.

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 3GPP TS 23.501 [10].

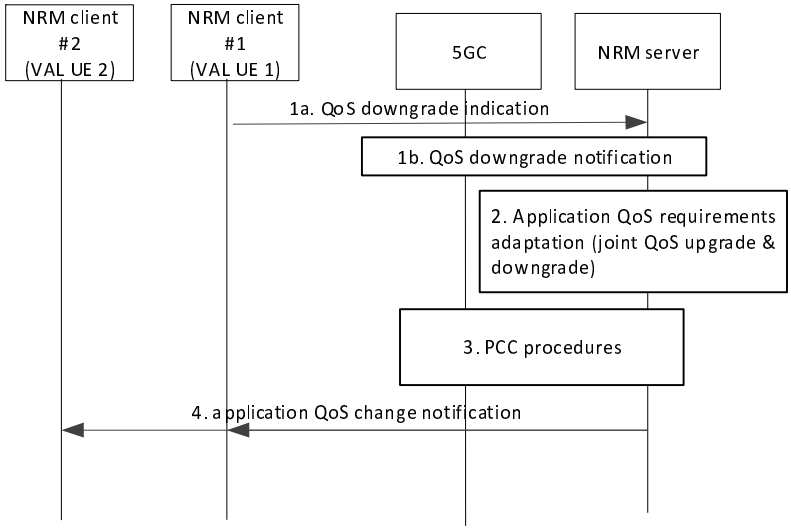

Figure 14.3.5.3.1-1: NRM-assisted coordinated QoS provisioning for C2 communication

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 [10]).

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 3GPP TS 23.502 [11], QoS sustainability analytics as in 3GPP 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 [11] 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.

14.3.5.3.2 Procedure for a group of UEs

Figure 14.3.5.3.2 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 any UEs in a group), as specified in 3GPP TS 23.501 [10].

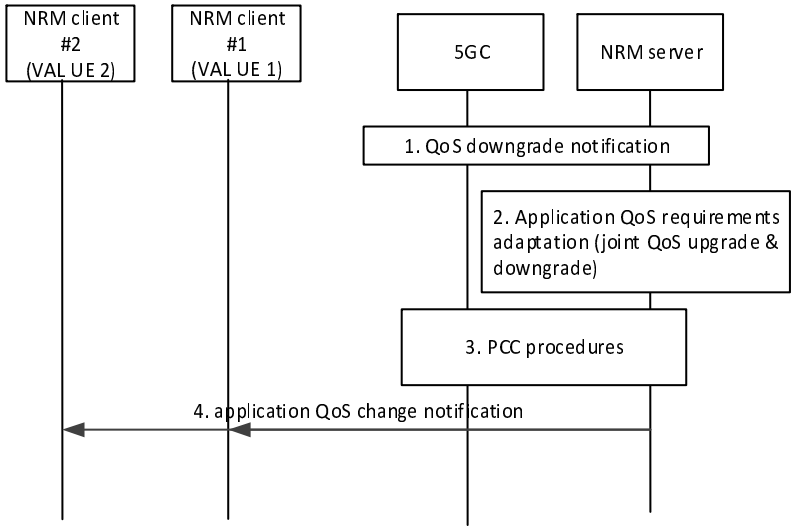

Figure 14.3.5.3.2-1: NRM-assisted coordinated QoS provisioning for 5G LAN-Type communication

1. The NRM server receives a trigger event from the 5GC (SMF/NEF), denoting a QoS downgrade notification for the network session of any group member in a group. (described in clause 5.7.2.4.1b of 3GPP TS 23.501 [10]).

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 3GPP TS 23.502 [11], QoS sustainability analytics as in 3GPP 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 only uplink/downlink network session or both uplink and downlink network sessions for each ingress group member in the group.

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 impacted network sessions or the update of the PCC rules to apply the new traffic policy (as specified in 3GPP TS 23.502 [11] in clause 4.15.6.14: AF requested QoS for a UE or group of UEs not identified by a UE address 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]);

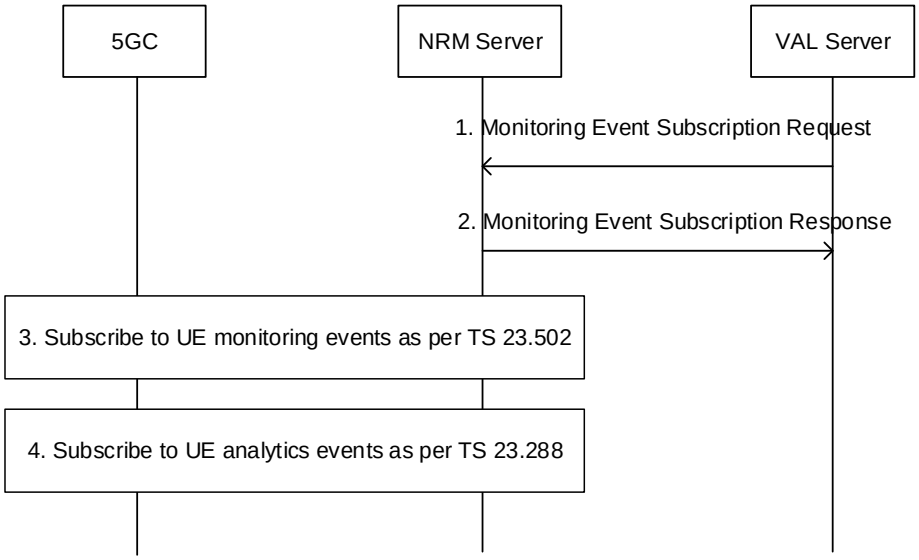

Figure 14.3.6.2.2-1: Monitoring Events Subscription Procedure

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 (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;

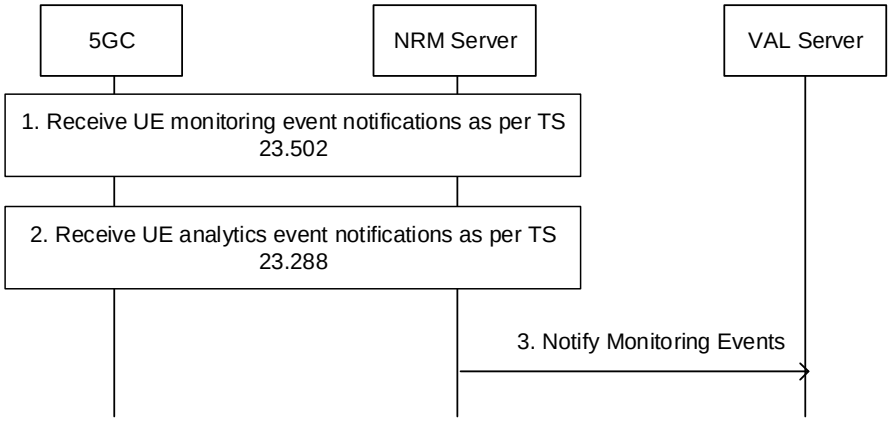

Figure 14.3.6.3.2-1: Monitoring Events Notification Procedure

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.

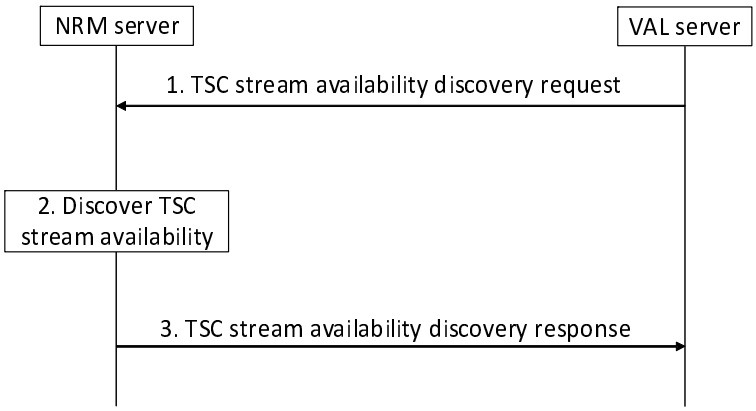

Figure 14.3.7.2-1: TSC stream availability discovery procedure

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 specified in clause 14.3.7.2.

3. The NRM server maintains mapping from the traffic class to TSC QoS.

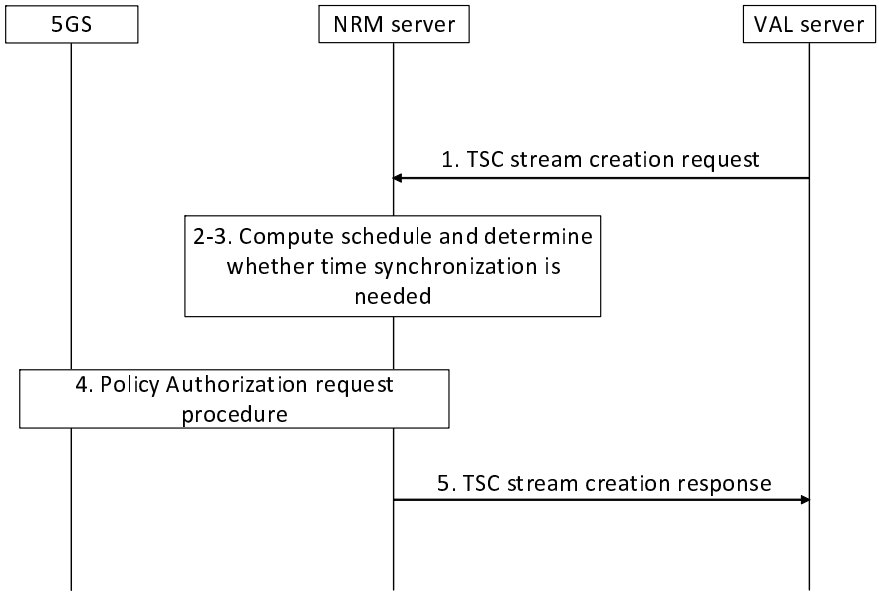

Figure 14.3.7.3-1: TSC stream creation procedure

1. The 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. The 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 [36]) 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 [36]) 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. Based on the Traffic specification (from the TSC stream creation request in step 1), the SEAL NRM server determines whether time synchronization needs to be activated for the TSC stream on the DS-TTs. If the DS-TTs are time synchronized, then the NRM does not activate the time synchronization for the corresponding DS-TT.

4. As a TSCTSF, the NRM server triggers via N84 the Npcf_PolicyAuthorization_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.

   If time synchronization is determined to be needed for the TSC stream on the DS-TTs in step 3, the NRM server uses the procedures in clause K.2.2 of 3GPP TS 23.501 [10] to activate the time synchronization via the Npcf_PolicyAuthorization_Update service operation. The procedure includes the configuration and initialization of the PTP instance in the DS-TTs, the construction of PMICs to each DS-TT/UE to activate the time synchronization service in the DS-TT and to subscribe for the port management information changes in the DS-TTs.

Editor's note: Using gate control parameters for hold and forward buffering is FFS.

5. The 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.

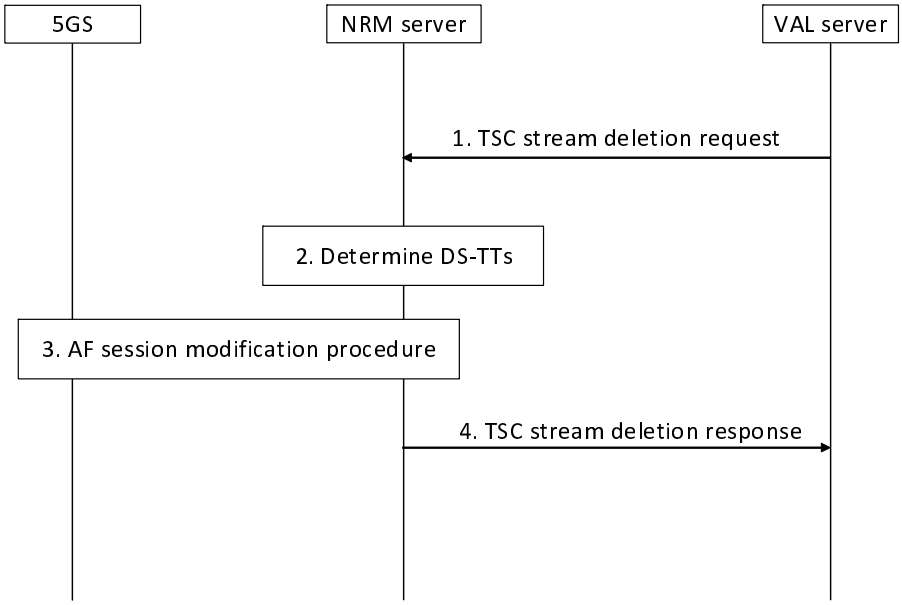

Figure 14.3.7.4-1: TSC stream deletion procedure

1. The NRM server receives a request from VAL server to delete a TSC stream for with a VAL Stream ID.
2. The NRM server identifies the MAC addresses of the DS-TTs involved in the stream based on the stored information for the VAL Stream ID. If none of the streams require to keep the time synchronization activated, the NRM server deactivates the time synchronization for the corresponding DS-TTs, otherwise keeps the time synchronization activated if the time synchronization for the DS-TTs was activated by the NRM server.
3. As a TSCTSF, the NRM server triggers via N84 the Npcf_PolicyAuthorization_Delete service operation defined in 3GPP TS 23.502 [11] for MAC addresses referred to by the VAL Stream ID. The 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. Before invoking the Npcf_PolicyAuthorization_Delete procedure, if the time synchronization service for the DS-TTs needs deactivation, the NRM server deactivates the time synchronization for the DS-TTs as described in clause K.2.2 3GPP TS 23.501 [10] via the Npcf_PolicyAuthorization_Update service operation.
4. The 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 server acting as TSN-AF.

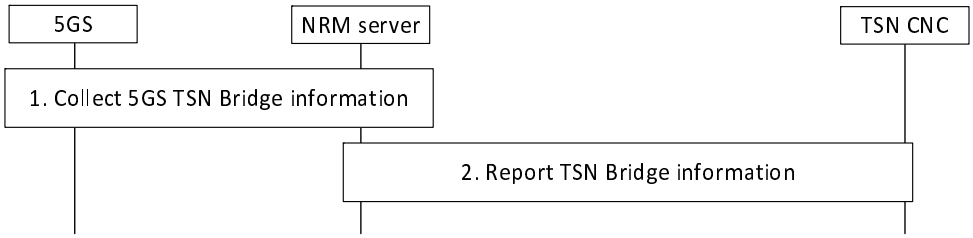

Figure 14.3.8.2-1: TSN Bridge information reporting procedure

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.

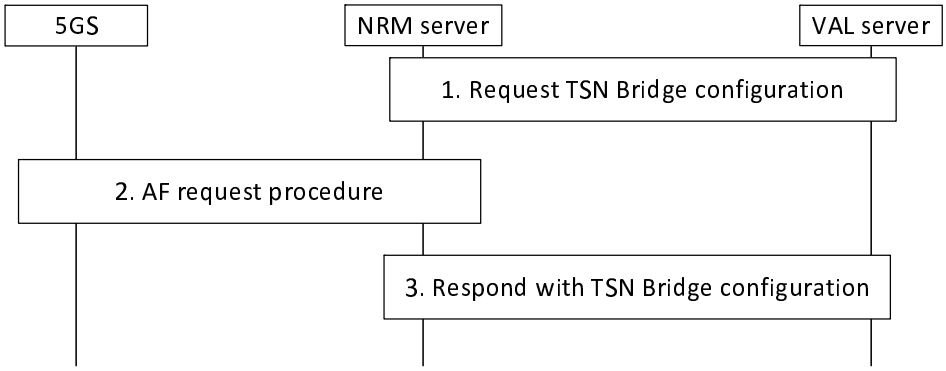

Figure 14.3.8.3-1: TSN Bridge configuration procedure

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.

14.3.9 Establishing communication with application service requirements

14.3.9.1 General

The NRM client and the NRM server (acting as an AS) are involved in the exchange and analysis of the desired service requirements (e.g. packet size, packet transmission interval, reliability, packet error rate) for the E2E communication amongst the Vertical UEs. The NRM server triggers the establishment of application-level direct service connectivity between two UEs via Uu, based on the information provided by the UEs and static configuration information available to the NRM server prior to the UE interaction. Note that service connectivity among VAL clients is established over the Uu, without device-to-device direct radio connectivity (e.g. PC5) requirement.

14.3.9.2 Procedures

14.3.9.2.1 Procedure triggered by correlated source and destination requests

The procedure for establishing Uu-based application-level direct communications between two UEs, with application service requirements is as illustrated in figure 14.3.9.2.1-1. In this procedure the source and destination VAL clients correlate their triggering of the procedure establishment before the NRM Server provides the service.

Pre-conditions:

- NRM client 1 and NRM client 2 are provided configuration information for the VAL clients served e.g. connectivity requirements, which destination UEs to connect to over Uu, etc.
- The NRM client 1 and NRM client 2 are configured with the information of the NRM server and have connectivity enabled to communicate with the NRM server. The information is provided via pre-configuration.
- The NRM server is configured with policies and information of the UEs to determine authorization of the UEs requesting connectivity via Uu.
- The VAL clients associated with NRM client 1 and NRM client 2 have triggered the establishment of connectivity.

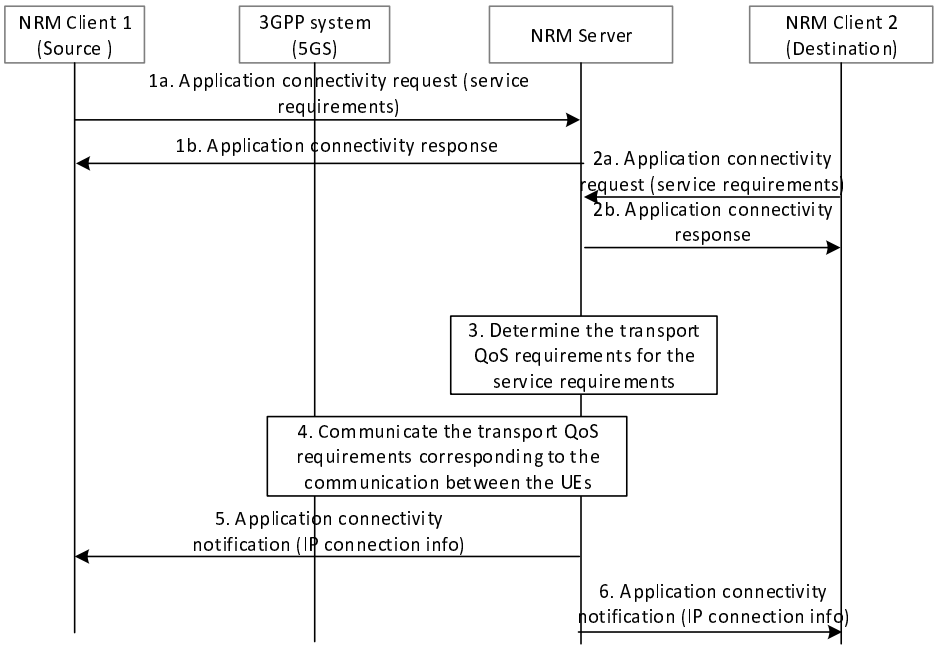

Figure 14.3.9.2.1-1: Establishing communication with application service requirements

1a. The NRM client 1 sends the application connectivity request (source identity and IP address, destination identities, service requirements) to the NRM Server. The service requirement from the source includes packet size, packet transmission interval, packet E2E latency, allowed packet loss rate/packet loss amount/packet error

rate, etc. The destination may be multiple UEs (devices). The identity of source and destination may be the application user identity or the MAC address.

1b. The NRM server determines whether the UE of NRM client 1 is authorized to connect to the destination UEs for direct service communications via Uu. If UE of NRM client 1 is authorized to connect to the destination UEs, then a response is provided to the NRM client 1 indicating acceptance of the request.

2a. The NRM client 2 sends the application connectivity request (destination identity and IP address, source identity, service requirements) to the NRM server. The service requirements from the destination includes the service requirements as described in step 1a.

2b. The NRM server determines whether the UE of NRM client 2 is authorized to connect to the destination UEs for direct service communications via Uu. If UE of NRM client 2 is authorized to connect to the destination UEs, then a response is provided to the NRM client 2 indicating acceptance of the request.

3. Based on the service requirements received in step 1 and step 2, the NRM server determines the parameters and patterns for direct service connectivity between the UEs via Uu and also the transport requirements, i.e., QoS requirements for the 3GPP system (e.g. 5GS). This step may also include retrieving the direct link status of the UEs (e.g. PDU Session Status, UE reachability). If the NRM server determines that direct service connectivity via Uu is not authorized or not possible with the given connectivity requirements, it skips step 4 and proceeds to steps 5 and 6, informing each NRM client accordingly.

   NRM server will process E2E connectivity establishment between NRM client 1 and NRM client 2 only after it receives the request from NRM client 2. There can be several NRM clients (destinations) which will perform step 2 and NRM server will process their E2E connectivity with NRM client 1 (source) as and when the requests are received by the NRM server.

4. The NRM server triggers 3GPP system to establish Uu connectivity between the UE of NRM client 1 and UE of NRM client 2 with required QoS as specified in 3GPP TS 23.501 [10].

5. The NRM server sends the application connectivity notification (connectivity/session information) to NRM client 1 indicating successful establishment of the connectivity. The connectivity/session information may contain the accepted destination identities.

6. The NRM server sends the application connectivity notification (connectivity/session information) to NRM client 2 indicating successful establishment of the connectivity.

14.3.9.2.2 Procedure triggered by source request and coordinated with destination

This procedure is used for establishing Uu-based application-level direct communications between two UEs, based on a single client initiating and providing application requirements. The procedure is as illustrated in figure 14.3.9.2.2-1. The NRM Server provides the service by coordinating with the destination client.

Pre-conditions:

- NRM client 1 and NRM client 2 are provided configuration information for the VAL clients served e.g. connectivity requirements, etc.

- Pre-processing determines that network assisted UE-to-UE communications is required. VAL application policies and destination information for NRM clients are available at the NRM server.

- The VAL client associated with NRM client 1 triggers the establishment of connectivity and provides information about (one or more) destination VAL client(s).

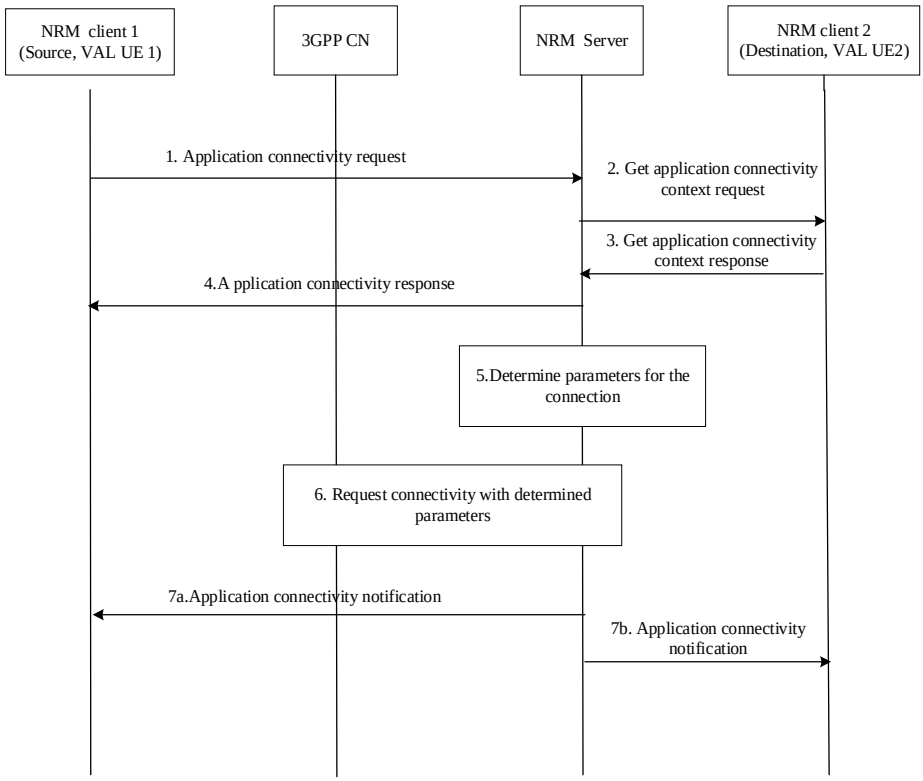

Figure 14.3.9.2.2-1: Coordination UE-to-UE communications with VAL application requirements

1. The NRM client 1 sends the application connectivity request (source identity and IP address, destination identities, application requirements) to the NRM server to establish connectivity for VAL client 1 on UE 1. The destination VAL client(s) may be hosted on one or multiple UEs (devices).

2. The NRM server determines whether VAL client 1 is authorized to connect to VAL client 2 for application-level direct UE-to-UE communications. If VAL client 1 is authorized to connect to VAL client 2, the NRM server performs the get application connectivity context request to retrieve VAL UE-to-UE connection coordination context procedure as described in clause 14.3.2.56. This step can be skipped if the NRM server is already aware of VAL client 2's context information.

   NOTE: The signaling and functionality for handling the cases when NRM client 2 will be temporarily unavailable for establishing the direct service connection are implementation dependent.

3. The NRM client 2 sends the get application connectivity context response to the NRM server, 2. Using the request information and local policies, the NRM client 2 determines whether context information is to be provided for establishing application-level direct connectivity to the counterpart UE for the VAL application indicated. If the NRM client determines that context information is to be provided, it responds to the NRM server and provides the VAL connection coordination context data for the VAL client served.

4. The NRM server sends the application connectivity response to NRM client 1.

5. The NRM server uses VAL client 1's and VAL client 2's context information, their application-level direct UE-to-UE connectivity requirements, location information, and network context as input, checks connectivity service policies, and determines the parameters and patterns for application-level direct UE-to-UE connectivity between the VAL clients. The NRM server may also determine transport requirements, e.g. QoS requirements, for the 3GPP system (e.g. 5GS).

   If network provided location information is used, location information may be obtained from the SEAL location management server. Alternatively, Location Reporting monitoring as described in 23.502[12] may be used. This step may also include a request for direct link status (e.g. PDU Session Status, UE reachability, etc. as described

in 23.502 [12]). This action may be skipped if the clients provide location information or if there are no location requirements for establishing the application-level direct UE-to-UE connectivity.

If the NRM server determines that UE-to-UE application-level direct connectivity is not authorized or not possible with the given connectivity requirements, it skips step 5 and proceeds to steps 6 and 7, informing each NRM client accordingly.

6. The NRM server may request the 3GPP system to establish or modify the 3GPP system level connectivity that enables the application-level direct UE-to-UE connection for VAL client 1 and VAL client 2 services, e.g. via modification of existing radio bearers. NRM server provides the necessary information (e.g. identifiers of VAL client 1 and VAL client 2, transport requirements) in this request message.

7. a. The NRM server notifies NRM client 1 of the established UE-to-UE connection b. The NRM server notifies the NRM client 2 of the established UE-to-UE connection.

Each NRM client notifies the corresponding VAL client of the established application-level direct UE-to-UE connection.

14.3.10 AF influence URSP procedure for reliable transmission

14.3.10.1 General

The procedures related to the AF influence URSP for reliable transmission are described in the following subclauses.

14.3.10.2 AF influence URSP procedure for reliable transmission

Pre-conditions:

1. The SEALDD server (or VAL server) has decided to use reliable transmission for a specific SEALDD client (or VAL client) and has got the UE address or UE ID.

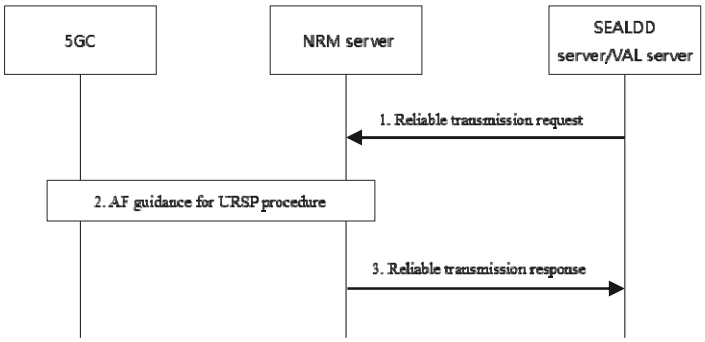

Figure 14.3.10.2-1: AF influence URSP procedure for reliable transmission

1. The NRM server receives from the SEALDD server (or VAL server) about the request for reliable transmission service with the application descriptors for the two redundant transmission paths. The SEALDD client's current UE address or UE ID is also provided to identify the affected UE.

2. After receiving the request from SEALDD server (or VAL server), the NRM server associates the available DNN and S-NSSAI information for the two application descriptors. NRM server triggers via N5/N33 with the AF guidance for URSP procedure as described in 3GPP TS 23.502 [11] clause 4.15.6.10. The AF request includes the application traffic descriptors and the associated DNN, S-NSSAI, and also includes UE address or UE ID received in step 1.

3. NRM server sends response about reliable transmission service.

14.3.11 VAL services over 5GS supporting EPS interworking

The VAL server consumes the network resource management services from the NRM server. As specified in 3GPP TS 23.501 [10], a dedicated user plane anchor point, i.e. UPF + PGW-U function, is defined for interworking between 5GS and EPS. This enables that the network can directly handle PDU sessions (in 5GS) and PDN connections (in EPS) associated to VAL service sessions of a VAL UE during inter-system mobility.

The inter-system mobility of a VAL UE will be transparent to the NRM server and VAL server. The NRM server will continue interacting with the same control plane functions, e.g. PCF, and the VAL server will continue interacting with the same user plane function, e.g. UPF + PGW-U.

NOTE: For the case that seamless session continuity is required for VAL services, EPS interworking with N26 (interface between AMF in 5GC and MME in EPC) is required for inter-system change, as described in 3GPP TS 23.501 [10].

14.3.12 UE unified traffic pattern and monitoring management

14.3.12.1 General

UE unified traffic pattern and monitoring management procedures allow NRM to offer services leveraging CN exposure APIs for network parameter values configuration and UE monitoring event management.

14.3.12.2 UE unified traffic pattern and monitoring management subscription procedure

VAL servers can indicate to the NRM server interest in receiving UE unified traffic patterns and monitoring management services by sending the UE unified traffic pattern and monitoring management subscription requests.

The subscription requests from each VAL server also include the traffic pattern configuration of the requester, which refers to application-level patterns of data traffic. The NRM server aggregates the traffic patterns obtained from the requestors (and described in Table 14.3.2.53-2) to determine the UE unified traffic patterns per UE. The UE unified traffic patterns are described via Table 14.3.2.55-1 for the UE unified traffic pattern update notification. These aggregated traffic patterns per UE (termed UE unified traffic pattern) are updated/adjusted by the NRM Server based on information obtained from UE monitoring.

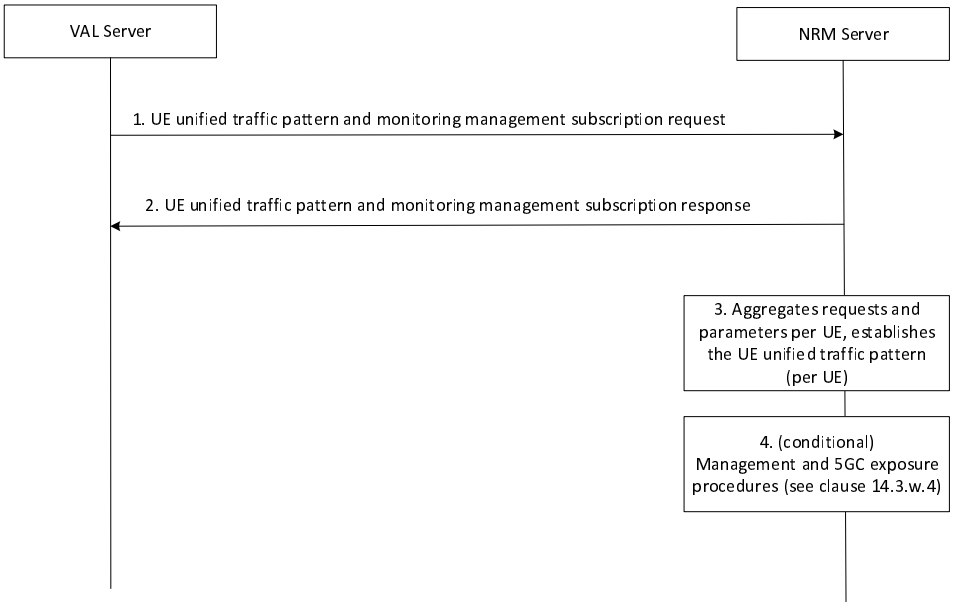

Figure 14.3.12.2-1: UE unified traffic pattern and monitoring management subscription procedure

1. In order to subscribe to the NRM Server services, the VAL server sends the UE unified traffic pattern and monitoring management subscription request, as detailed in clause 14.3.2.53. The subscription request may include traffic pattern configuration, which provides the traffic patterns of the specific VAL Server. The request may also include Management subscription indications which indicate to the NRM Server which management and 5GC exposure procedures the VAL server allows the NRM Server to perform on its behalf.

2. Upon receipt of the request, the NRM server sends a UE unified traffic pattern and monitoring management subscription response as detailed in clause 14.3.2.54.

3. The NRM Server aggregates UE unified traffic pattern and monitoring management subscription requests from different VAL servers and determines the UE unified traffic pattern per UE (using the traffic patterns of all the communicating with the UE).

4. Depending on the subscription requests received and local policies, the NRM Server executes one or more management and 5GC exposure procedure (per UE). Management and 5GC exposure procedures are detailed in clause 14.3.12.4.

   The NRM Server determines the management procedures required to be executed on behalf of the VAL Servers based on the received management subscription indications as follows:

   - If the UE unified traffic pattern monitoring management indication is provided, the NRM Server executes steps 1-3 of the UE unified traffic pattern monitoring procedure detailed in clause 14.3.12.4.2.

   - If the UE unified traffic pattern monitoring update notification indication is provided, the NRM Server executes the steps 1-4 of the UE unified traffic pattern monitoring procedure detailed in clause 14.3.12.4.2.

   - If the Network parameter coordination indication is provided, the NRM executes the network parameter coordination procedure detailed in clause 14.3.12.4.3.

NOTE: The NRM Server translates the management subscription indications received from different VAL Servers into per-UE management indications based on local policies and configurations. For example, an NRM Server may be configured to execute a management procedure for a UE if at least one VAL Server indicates it. Another NRM Server may be configured to provide all the management procedures for the UEs using the platform independent of VAL Server subscription indications.

14.3.12.3 UE unified traffic pattern update notification procedure

An NRM Server can provide updated UE unified traffic pattern information to VAL servers by sending UE unified traffic pattern update notifications as shown in figure 14.3.12.3-1. The UE unified traffic pattern management procedure detailed in clause 14.3.12.4.2. is an example of procedure which may result in UE unified traffic pattern updates at the NRM server, based on which UE unified traffic pattern update notifications are provided.

Pre-conditions:

1. The VAL server has subscribed for UE unified traffic pattern and monitoring management services, requesting to receive UE unified traffic pattern update notifications

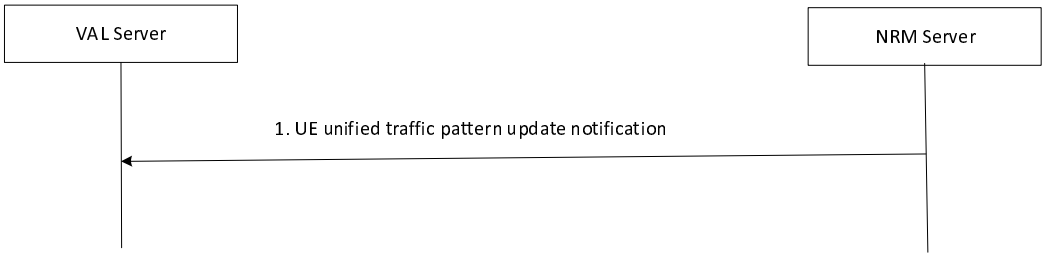

Figure 14.3.12.3-1: UE unified traffic pattern update notification procedure

1. The NRM server sends the UE unified traffic pattern update notification when either of the following occurs:

- Monitoring events lead to updates in the UE unified traffic pattern (e.g., to schedule elements in Table 14.3.2.55-1) the NRM server sends a corresponding notification to the VAL server. Other notifications may be provided, e.g., if the stationary indication changes.
- An NP Configuration Notification is received with a new set of applied network parameters and if the NRM Server determines that the new configuration is incompatible with the current UE unified traffic pattern (see also clause 14.3.12.4.2 step 3).

14.3.12.4 Management and 5GC exposure procedures

14.3.12.4.1 General

The management and 5GC exposure procedures in this clause show NRM processing and its interactions with 5GC in support of the functionality described in clause 14.3.12.2

14.3.12.4.2 UE unified traffic pattern management procedure

The UE unified traffic pattern management procedure is used to determine and manage a unified traffic pattern applicable to a specified UE. The NRM Server then uses the 5GC exposure of UE monitoring events to update the UE unified traffic pattern.

Pre-conditions:

1. The NRM Server determines to provide the service for a specific UE if either of the following conditions is true:
   a) It receives UE unified traffic pattern monitoring management indications in UE unified traffic pattern and monitoring management subscription requests; or
   b) It determines to provide Network parameter coordination services for the UE.

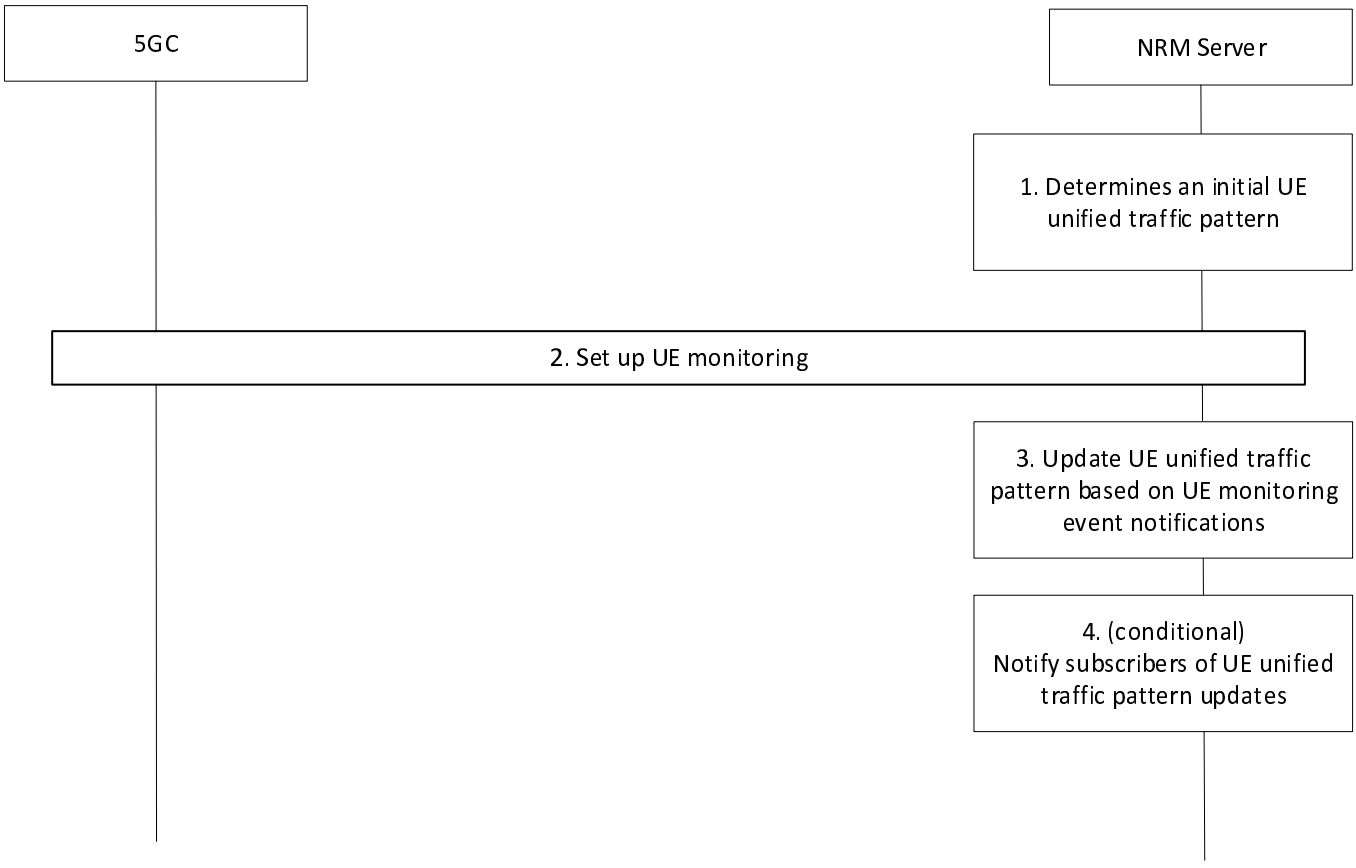

Figure 14.3.12.4.2-1: UE unified traffic pattern and monitoring management subscription procedure

1. The NRM Server determines an initial UE unified traffic pattern, e.g. by using all Traffic pattern configurations received for the UE .

2. The NRM Server determines, based on local policy that UE monitoring events are to be configured and executes the corresponding Monitoring procedure as described in 3GPP TS 29.122 [54] clause 4.4.2.

3. The NRM Server updates the UE unified traffic pattern based on the received monitoring events as follows:

   - If a Monitoring Notification report for UE_REACHABILITY is received, and *idleStatusInfo* information is provided in the report, the NRM Server changes the schedule element of the UE unified traffic pattern such that the duration of activity is set to the value of the *activeTime* parameter configured in the *idleStatusInfo*.

   - If a Monitoring Notification report for AVAILABILITY_AFTER_DDN_FAILURE is received after UEs transition to idle mode, the NRM Server updates the schedule element of the UE unified traffic pattern such that: the start of an activity window is based on the Idle Timestamp, with a periodicity equal to the TAU/RAU Timer; the duration of the activity window indicates the Active Time value.

   - If a Monitoring Notification report for COMMUNICATION_FAILURE is received The NRM updates the schedule element of the UE unified traffic pattern to indicate that no communications are currently available (e.g. by using a keyword such as "NULL"). Local policies may specify events/ thresholds further defining when the NRM may provide a UE unified traffic pattern update based on monitoring events. For example, the update may be provided only after repeated communication failures are received within a timespan, or only if high reliability communications are expected. It is recommended that UE Reachability monitoring is also enabled in conjunction with the Communication Failure monitoring. This enables the NRM to provide updated timing information once the UE becomes reachable again.

   - If a Monitoring Notification report for LOSS_OF_CONNECTIVITY is received, the NRM Server changes the schedule element of the UE unified traffic pattern to indicate that no communications are currently available

4. Conditional: The NRM Server notifies subscribers of the UE unified traffic pattern updates, as described in clause 14.3.2.55

14.3.12.4.3 Network parameter coordination procedure

The network parameter coordination procedure uses UE unified traffic pattern information to influence aspects of UE/network behaviour such as the UE's PSM and extended idle mode DR14. For this purpose, parameter values may be suggested for Maximum Latency and Maximum Response Time for a UE. 5GC may choose to accept, reject or modify the suggested configuration parameter value.

Pre-conditions:

1. The NRM Server determines to provide the service for a specific UE after receiving Network parameter coordination indications in UE unified traffic pattern and monitoring management subscription requests, subject to policy.

2. The NRM Server determines and manages UE unified traffic patterns as described in clause 14.3.12.4.2.

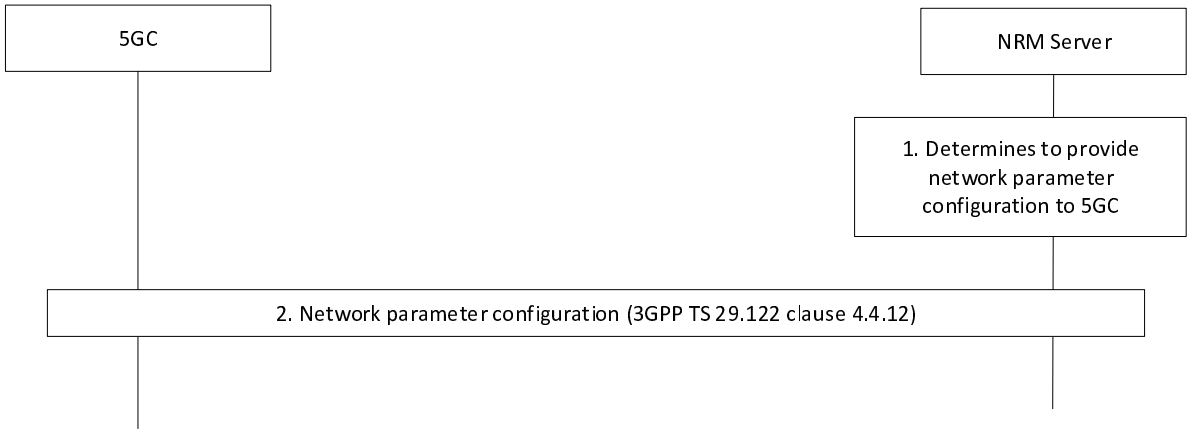

Figure 14.3.12.4.3-1: Network parameter coordination procedure

1. The NRM Server determines to provide Network parameter configuration to 5GC. This determination can be based on updates to the UE unified traffic patterns resulting from interactions with VAL Servers (e.g. Traffic pattern configuration updates), on local policies, etc.

   The NRM Server determines parameters the needed for NpConfiguration data structure as specified in 3GPP TS 29.122 [54] from the UE unified traffic patterns as follows:

   - *maximumLatency* – This value tells the network how long the UE is allowed to sleep. Setting it to 0 will disable PSM, extended idle mode DRX, and extended buffering. The NRM Server can extract the periodicity derived from the UE unified traffic pattern, which includes the schedule elements for the UEs communications with all VAL servers. The NRM Server sets *Maximum Latency* to be approximately the periodicity of the active periods derived from the schedule element of the UE unified traffic pattern.

   - *maximumResponseTime* – When the UE uses PSM, Maximum Response Time tells the network how long the UE should stay reachable after a transition to idle. When the UE uses eDRX, Maximum Response Time is used by the network to determine when to send a reachability notification before a UE's paging occasion. The NRM Server extracts a duration of activity from the schedule element of the UE unified traffic pattern and sets *Maximum Response Time* to reflect the duration of activity, indicating how long the UE should stay reachable for downlink communications.

2. The NRM Server performs the Network Parameter Configuration procedure as described in 3GPP TS 29.122 [54] clause 4.4.12.

NOTE: The values provided by NRM Server to 5GC in the Network parameter configuration procedure may or may not be accepted by the network. If they are not accepted, 5GC responds accordingly and the previous values apply, or new values are provided. The new values are used by NRM Server as described in this clause when they were provided via monitoring event notifications.

14.3.13 Background Data Transfer configuration

14.3.13.1 General

The Background Data Transfer (BDT) feature requires an initial step in which BDT policies are requested and negotiated. BDT Policy requests to the 3GPP network are based on an expected time window and UE set, with additional optional information e.g., expected data volume per UE. The UE set may be indicated as an expected number of UEs, a group ID or geographical area.

The feature allows for the NRM server involved to negotiate the BDT policies proposed by the network. It also allows the NRM server to enable notifications to be sent, should network conditions affect future BDT policies.

Based on the BDT policies obtained using the procedures detailed in this clause, a VAL server can initiate a data transfer to the client at the negotiated time and with the negotiated charging rates. The data transfer between the VAL

Server and the VAL Client is performed without NRM Server enablement. Service layer functionality for the purpose of facilitating the data transfer with the negotiated BDT policy is not in scope of this specification.

14.3.13.2 Request and Select Background Data Transfer Policy

Figure 14.3.13.2-1 depicts a general procedure for the request and configuration of traffic policies for BDT initiated by a request from a VAL Server.

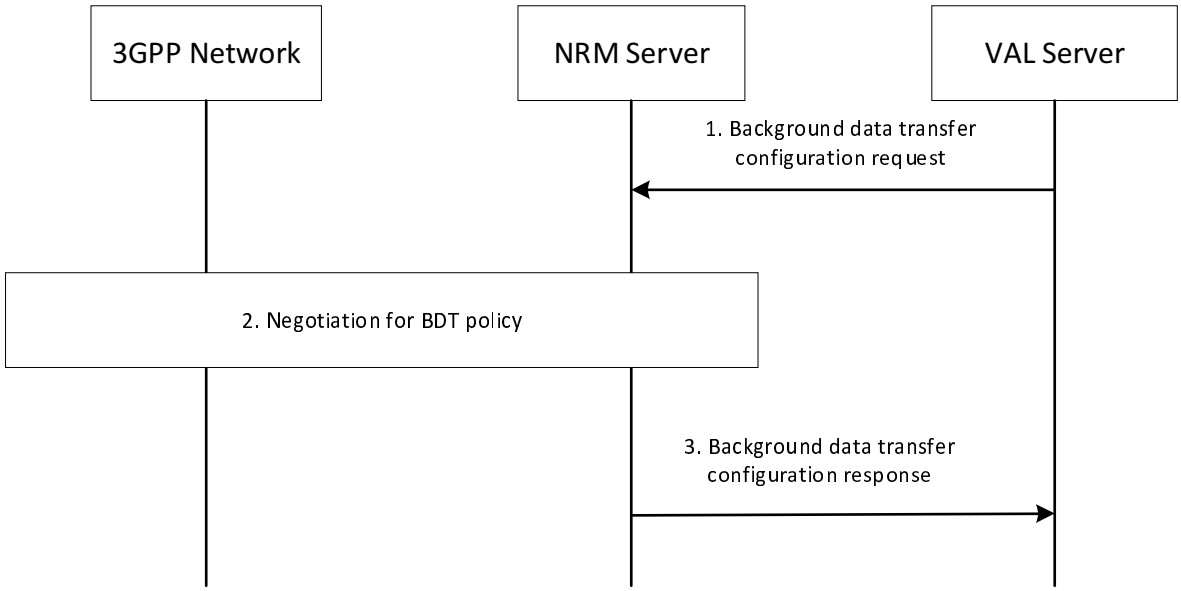

Figure 14.3.13.2-1: General Procedure for configuration of Background Data Transfer

1. A VAL Server requests the NRM Server to negotiate with the 3GPP network a background data transfer policy using the BDT_Configuration_request (see clause 14.4.2.15).

   The request includes expected data volume, expected number of UEs, expected time window for the background data transfer. The request may also include group ID, geographic information for the UEs, a request expiration time, guidance for policy selection. If guidance for policy selection is not included, the VAL Server indicates if the NRM Server may choose independently from among multiple transfer policies.

2. Based on the request expiration time and Service Provider policies, NRM Server may determine to delay interactions with the 3GPP network in order to negotiate on behalf of multiple VAL Servers.

   The NRM Server performs the procedure for negotiation of background data transfer policy as described in 3GPP TS 23.502 [11] clause 4.16.7.2. The procedure requires that expected data volume, expected number of UEs, and expected time window are provided by the NRM Server. If the NRM Server determines to negotiate on behalf of multiple VAL Servers, the parameters included reflects a superset of the individual VAL Server requests.

   NOTE 1: The NRM Server determines to negotiate on behalf of multiple VAL Servers based on implementation options and local policies. For example, if the request expiration time and expected time window are sufficiently large and, respectively, far away in time, the NRM Server may be allowed to delay the negotiations with the 3GPP network in case another request is received, targeting the same group of UEs. If another request is received with expected time windows sufficiently close and if the guidance for policy selection allows, a single policy/time window may be negotiated instead. This allows the UE group to wake up only once for multiple background data transfers.

   The 3GPP network determines one or more applicable BDT policies based on the requesting Background Data Transfer parameters. A list of BDT policies and a mandatory BDT Reference ID is provided to the NRM Server. Each BDT policy includes charging rating group reference and allocated time window and optional maximum UL and DL bandwidth as specified by 3GPP TS 23.503 [12]. The NRM Server uses ASP policies and the

transfer selection guidance (if available) to select a BDT policy. The NRM Server informs the 3GPP Network of the selected BDT policy.

NOTE 2: Based on 3GPP TS 23.503 [12] clause 6.1.2.4. it is assumed that the NRM server is configured to understand the charging rating group reference based on agreements with the operator.

NOTE 3: The NRM server utilizes the BDT warning notification from 3GPP network based on local policies.

3. The NRM Server stores the BDT configuration information with the information received from VAL server in step 1 along with the BDT Reference ID and selected BDT policy. The NRM server responds to the VAL Server, providing the BDT Reference ID and allocated time window of the selected background data transfer policy.

14.3.13.3 Reselect Background Data Transfer Policy

Figure 14.3.13.3-1 depicts a procedure for reselecting BDT policies after BDT warning.

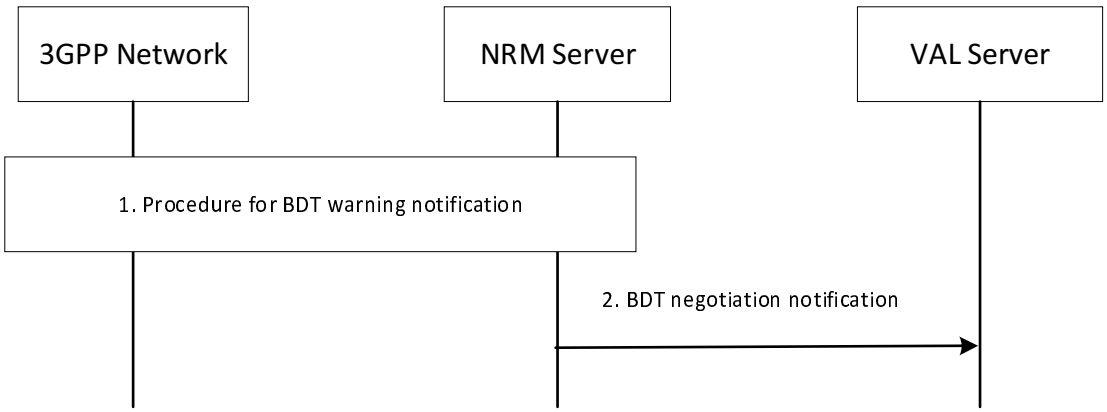

Figure 14.3.13.3-1: Reselecting BDT policies after BDT warning

1. The 3GPP Network, via NEF, sends the BDT warning (BDT Policy negotiate) notification to the NRM server as specified in step 10, clause 4.16.7.3 of 3GPP TS 23.502 [11]. The notification includes the affected BDT Reference ID and list of candidate BDT policies.

   Each of the BDT policies in the candidate BDT list includes charging rating group reference and time window, as well as optional maximum UL and DL bandwidth.

   The NRM Server checks the new BDT policies included in the candidate list of the BDT warning notification. The NRM Server determines whether the notification affects multiple VAL Servers or not. The NRM Server uses ASP policies and the transfer selection guidance (if available) provided with the initial VAL Server request to select a policy.

   The NRM Server informs the 3GPP Network of the selected transfer policy or that no new policy has been selected by using steps 11-16 of the procedure for BDT warning notification in 3GPP TS 23.502 [11] clause 4.16.7.3.

2 The NRM server updates the BDT configuration information with the newly selected BDT policy or no BDT policy is selected for the BDT Reference ID. The NRM Server sends a BDT_Negotiation_notification (see clause 14.4.2.16), to the VAL server, providing information about the newly selected BDT policy, or that no BDT policy is selected for the BDT Reference ID. If a new BDT policy is selected by the NRM server, the information provided to the VAL Server includes the BDT Reference ID and the granted time window.

14.3.13.4 BDT configuration get

Figure 14.3.13.4-1 illustrates a procedure for retrieving the BDT configuration on the NRM server by the VAL server.

Pre-conditions:

1. The VAL server has performed the BDT configuration request as specified in clause 14.3.13.2.

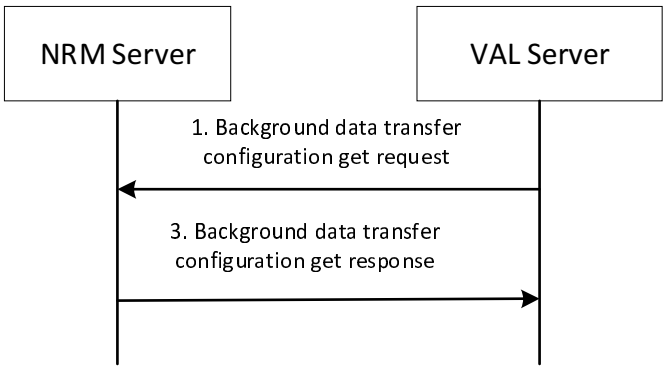

Figure 14.3.13.4-1: BDT configuration get

1. A VAL Server requests the NRM Server to retrieve its background data transfer policy configuration using the BDT_Configuration_Get_request (see clause 14.4.2.19).

   The request includes identifier for the BDT policy configuration stored at the NRM server.

2. The NRM Server provides a response to the VAL server indicating success or failure of the operation and the BDT configuration data available at the NRM server.

14.3.13.5 BDT configuration update

Figure 14.3.13.5-1 illustrates a procedure for updating the BDT configuration on the NRM server by the VAL server.

Pre-conditions:

1. The VAL server has performed the BDT configuration request as specified in clause 14.3.13.2.

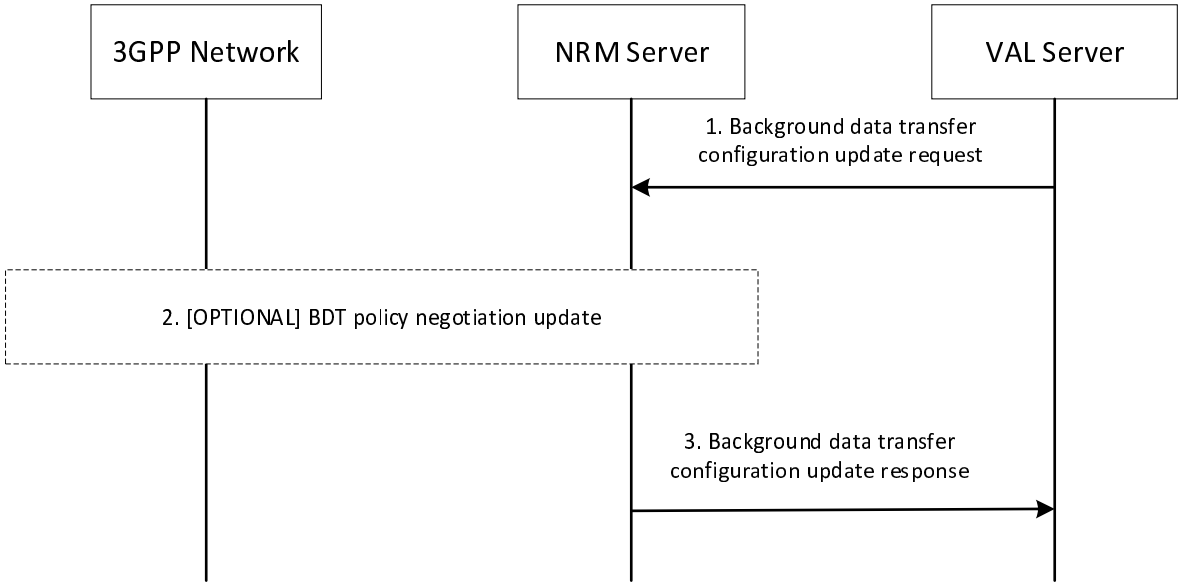

Figure 14.3.13.5-1: BDT configuration update

1. A VAL Server requests the NRM Server to update its background data transfer policy configuration using the BDT_Configuration_Update_request (see clause 14.4.2.20).

   The request includes identifier for the BDT policy configuration stored at the NRM server and one or more updated information like expected data volume, expected number of UEs, expected time window for the background data transfer, geographic information for the UEs, a request expiration time, guidance for policy selection.

2. The NRM Server may perform the BDT policy negotiation update as specified in 3GPP TS 23.502 [11] clause 4.16.7.2. The request for update of the BDT policy configuration by the VAL server may provide several updates to the requirements of the VAL server to perform BDT to the VAL UE or group of VAL UEs. This may impact the selected BDT policy.

3. The NRM Server provides a response to the VAL server indicating success or failure of the operation.

14.3.13.6 BDT configuration delete

Figure 14.3.13.6-1 illustrates a procedure for deleting the BDT configuration on the NRM server by the VAL server.

Pre-conditions:

1. The VAL server has performed the BDT configuration request as specified in clause 14.3.13.2.

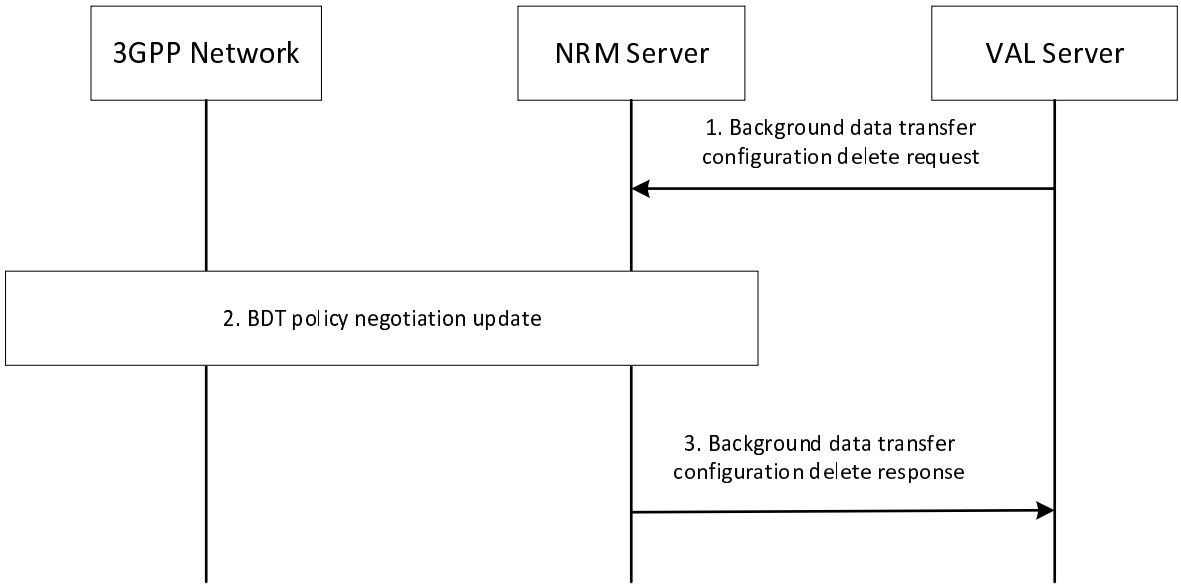

Figure 14.3.13.6-1: BDT configuration delete

1. A VAL Server requests the NRM Server to delete its background data transfer policy configuration using the BDT_Configuration_delete_request (see clause 14.4.2.21).

   The request includes identifier for the BDT policy configuration stored at the NRM server.

2. The NRM Server may perform the BDT policy negotiation update as specified in 3GPP TS 23.502 [11] clause 4.16.7.2. If NRM server is currently serving only one VAL server, then BDT policy delete is performed as specified in 3GPP TS 23.502 [11] clause 4.16.7.3. The request for deletion of the BDT policy configuration by the VAL server removes the requirement of the VAL server to perform BDT to the VAL UE or group of VAL UEs. This may impact the selected BDT policy.

3. The NRM Server provides a response to the VAL server indicating success or failure of the operation.

14.4 SEAL APIs for network resource management

14.4.1 General

Table 14.4.1-1 illustrates the SEAL APIs for network resource 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
	Reliable_Transmission	VAL server, SEALDD server	Request /Response
	BDT_Configuration_Request	VAL server	Subscribe/Notify
	BDT_Negotiation_Notification	VAL server	Subscribe/Notify
	BDT_Configuration_Get	VAL server	Request /Response
	BDT_Configuration_Update	VAL server	Request /Response
	BDT_Configuration_Delete	VAL server	Request /Response
	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
	Update_Unicast_QoS_Monitoring_Subscription	VAL server	

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.

14.4.2.10 Request_Multicast/Broadcast_Resource

API operation name: Request_Multicast/Broadcast_Resource

Description: Requesting multicast/broadcast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.40.

Outputs: See subclause 14.3.2.41.

See subclause 14.3.4A for the details of usage of this API operation.

14.4.2.11 Update_Multicast/Broadcast_Resource

API operation name: Update_Multicast/Broadcast_Resource

Description: Updating multicast/broadcast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.42.

Outputs: See subclause 14.3.2.43.

See subclause 14.3.4A for the details of usage of this API operation.

14.4.2.12 Delete_Multicast/Broadcast_Resource

API operation name: Delete_Multicast/Broadcast_Resource

Description: Deleting multicast/broadcast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.44.

Outputs: See subclause 14.3.2.45.

See subclause 14.3.4A for the details of usage of this API operation.

14.4.2.13 Activate_Multicast_Resource

API operation name: Activate_multicast_Resource

Description: Activating multicast/broadcast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.46.

Outputs: See subclause 14.3.2.47.

See subclause 14.3.4A for the details of usage of this API operation.

14.4.2.14 Deactivate_Multicast_Resource

API operation name: Deactivate_multicast_Resource

Description: Deactivating multicast/broadcast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.48.

Outputs: See subclause 14.3.2.49.

See subclause 14.3.4A for the details of usage of this API operation.

14.4.2.15 BDT_Configuration_request

API operation name: BDT_Configuration_request

Description: Requesting Background data transfer configuration.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.58

Outputs: See subclause 14.3.2.59

14.4.2.16 BDT_Negotiation_notification

API operation name: BDT_Negotiation_notification

Description: Forwards BDT negotiation notification.

Known Consumers: VAL server.

Inputs: None

Outputs: See subclause 14.3.2.59

14.4.2.17 Subscribe_Unified_Traffic_Pattern_and_Monitoring_Management operation

API operation name: Subscribe_Unified_Traffic_Pattern_and_Monitoring_Management

Description: Requesting UE unified traffic pattern and monitoring management subscription

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.53

Outputs: See subclause 14.3.2.54.

See subclause 14.3.12.2 for the details of usage of this API operation.

14.4.2.18 Notify_Unified_Traffic_Pattern_Update operation

API operation name: Notify_Unified_Traffic_Pattern_Update

Description: Notifies of update to UE unified traffic patterns

Known Consumers: VAL server.

Inputs: None

Outputs: See subclause 14.3.2.55.

See subclause 14.3.12.3 for the details of usage of this API operation.

14.4.2.19 BDT_Configuration_Get_request

API operation name: BDT_Configuration_Get_request

Description: Retrieving Background data transfer configuration.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.61

Outputs: See subclause 14.3.2.62

See subclause 14.3.13.4 for the details of usage of this API operation.

14.4.2.20 BDT_Configuration_Update_request

API operation name: BDT_Configuration_Update_request

Description: Updating Background data transfer configuration.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.63

Outputs: See subclause 14.3.2.64

See subclause 14.3.13.5 for the details of usage of this API operation.

14.4.2.21 BDT_Configuration_Delete_request

API operation name: BDT_Configuration_Delete_request

Description: Deleting Background data transfer configuration.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.65

Outputs: See subclause 14.3.2.66

See subclause 14.3.13.6 for the details of usage of this API operation.

14.4.2.22 Reliable_Transmission_request

API operation name: Reliable_Transmission_request

Description: Requesting Reliable Transmission service

Known Consumers: SEALDD server or VAL server

Inputs: See subclause 14.3.2.67.

Outputs: See subclause 14.3.2.68.

See subclause 14.3.10.2 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.

14.4.4.6 Update_Unicast_QoS_Monitoring_Subscription operation

API operation name: Update_Unicast_QoS_Monitoring_Subscription

Description: Updates the QoS monitoring subscription of a unicast resource.

Known Consumers: VAL server.

Inputs: See subclause 14.3.2.38

Outputs: See subclause 14.3.2.39

See subclause 14.3.3.4.5 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.

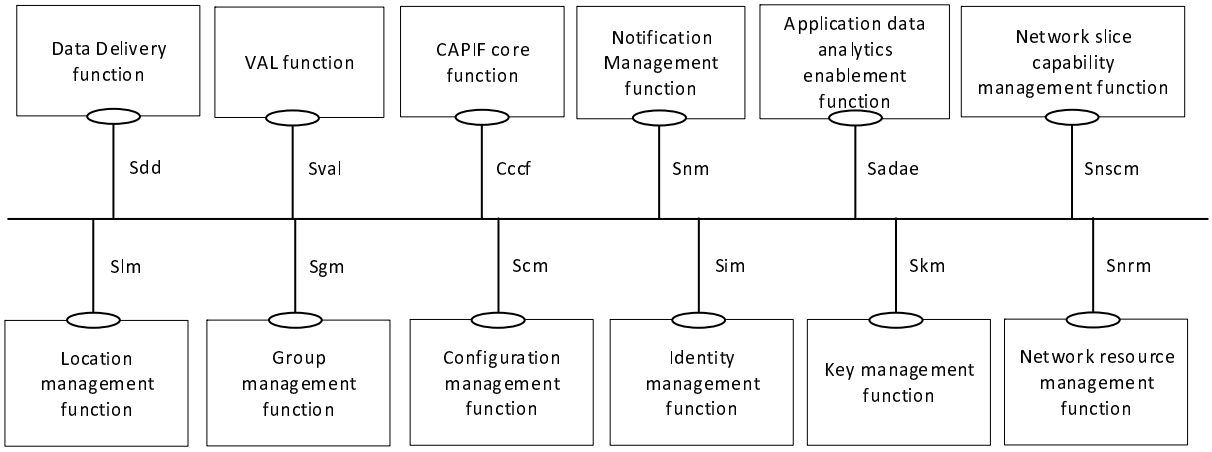

Figure 15.2-1: SEAL generic functional model representation using service-based interfaces

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].

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 3GPP TS 23.435 [40]
Sdd	Data delivery function	Data delivery server	Specified in 3GPP TS 23.433 [48]
Cccf	CAPIF core function	Not applicable	Specified in subclause 10 of 3GPP TS 23.222 [8]
Snm	Notification management function	Notification management server	Specified in subclause 17.4
Sadae	Application data analytics enablement function	Application data analytics enablement server	Specified in 3GPP TS 23.436 [49]

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. The NSCE service provides additional functionality and exposes slice capabilities based on 5GS management system services (e.g. MnS services) and 5GS network services (e.g. NEF APIs, NWDAF APIs, NSACF APIs). The detailed specification of NSCE is provided in 3GPP TS 23.435 [40].

16.2 Functional model

16.2.1 General

The functional model for the network slice capability enablement is specified in 3GPP TS 23.435 [40].

16.2.2 Void

16.2.3 Void

16.2.4 Void

16.3 Procedures and information flows for network slice capability enablement

The Procedures and information flows for the network slice capability enablement are specified in 3GPP TS 23.435 [40].

16.4 SEAL APIs for network slice capability enablement

The SEAL APIs for the network slice capability enablement are specified in 3GPP TS 23.435 [40].

17 Notification Management

17.1 General

The notification management is a SEAL service that offers the notification functionality to one or more verticals. This service enables VAL clients to subscribe and receive notifications from the VAL servers and thereby offloading the complexity of delivery and reception of notifications to the enabler layer. It provides common notification delivery service to vertical applications.

17.2 Functional model

17.2.1 General

The functional model for the notification management 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 notification management aspects required for vertical applications. Since the notification management is a feature which considers the Uu interfaces, only the on-network functional model is specified in this clause.

17.2.2 Functional model description

Figure 17.2.2-1 illustrates the generic functional model for notification management.

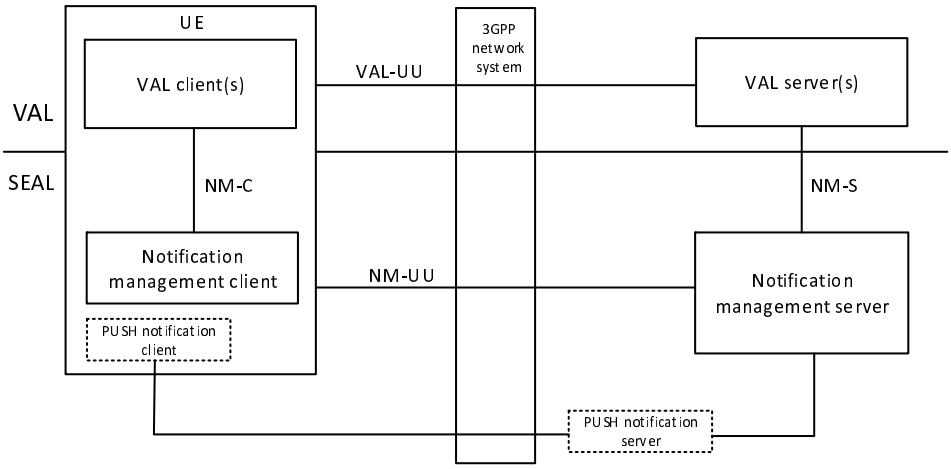

Figure 17.2.2-1: Functional model for notification management

The notification management client communicates with the notification management server over the NM-UU reference point. The notification management client provides the support for notification management functions to the VAL client(s) over NM-C reference point. The VAL server(s) communicates with the notification management server over the NM-S reference point for delivering the notification messages which is targeted for the VAL client(s). Notification management server sends these notification messages to the notification management client either through NM-UU interface for direct delivery (e.g. Long-polling, WebSocket) or through the OEM PUSH server for indirect delivery (e.g. FCM, APNS, OMA PUSH) which is implementation specific and outside the scope of this specification.

NOTE: Notification messages from PUSH notification server to the PUSH notification client are delivered either through 3GPP network system or through any non-3GPP system, which is implementation specific.

17.2.3 Functional entities description

17.2.3.1 General

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

17.2.3.2 Notification Management client

The notification management client functional entity acts as the application client for notification management aspects. It interacts with the notification management server. It handles the notification messages received from the notification management server and deliver it to the corresponding VAL clients residing on the VAL UE.

The notification management client functional entity is supported by the HTTP client functional entities of the signalling control plane.

17.2.3.3 Notification Management server

The notification management server is a functional entity that handles the notification management aspects by interacting with the notification management client and the VAL servers. The notification management server receives the notification messages from the vertical application layer and delivers it to the notification management client. The notification management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8].

17.2.4 Reference points description

17.2.4.1 General

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

17.2.4.2 NM-UU

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

17.2.4.3 NM-C

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

17.2.4.4 NM-S

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

17.3 Procedures and information flows for notification management

17.3.1 General

This sub-clause describes the procedure and information flows for notification management service. The notification management procedures apply to on-network VAL service only.

17.3.2 Information flows for notification management

17.3.2.1 Create notification channel request

Table 17.3.2.1-1 describes the information flow create notification channel request from the notification management client to the notification management server.

Table 17.3.2.1-1: Create notification channel request

Information element	Status	Description
Requestor identity	M	Identity of the requesting notification management client
Channel type	M	Indicates PULL or PUSH method to be used for delivering the notification messages
PUSH channel details (see NOTE)	O	Carries the details of the type of PUSH delivery and its associated data
Validity Duration	M	How long the notification channel will last (i.e. channel lifetime) as requested by the notification management client.
NOTE : This IE shall be present of the channel type is PUSH		

17.3.2.2 Create notification channel response

Table 17.3.2.2-1 describes the information flow create notification channel response from the notification management server to the notification management client.

Table 17.3.2.2-1: Create notification channel response

Information element	Status	Description
Notification URL	O	The URL to receive the notification message if a PULL method is requested. For some PUSH method implementation (such as WebSockets) this URL is used to start the PUSH notification service from the notification management server
Callback URL	M	The URL to be shared to the VAL server by the VAL client for sending the notifications to the notification management server
Validity duration	O	How long the notification channel will last (i.e. channel lifetime) as granted by the notification management server.
Channel ID	M	Unique identifier for the created notification channel

17.3.2.3 Open notification channel

Table 17.3.2.3-1 describes the information flow open notification channel from the notification management client to the notification management server.

Table 17.3.2.3-1: Open notification channel

Information element	Status	Description
Identity	M	Identity of the requesting notification management client
Notification URL	M	The URL to receive the notification message and it is same as received in the Create notification channel response
Channel ID	M	Identifies the notification channel and the value shall be same as returned in Create notification channel response

17.3.2.4 Notification message

Table 17.3.2.4-1 describes the information flow notification message from VAL server to the notification management server and from notification management server to the notification management client.

Table 17.3.2.4-1: Notification Message

Information element	Status	Description
VAL Application ID	M	Identity of the VAL application residing in the VAL UE this notification message is targeted
VAL Service ID	M	Identity of the VAL service for which this notification is generated
Notification data	M	This information element carries the details of the notification data such as type of the event and the data corresponding to the event

17.3.2.5 Delete notification channel request

Table 17.3.2.5-1 describes the information flow delete notification channel request from notification management client to the notification management server.

Table 17.3.2.5-1: Delete notification channel request

Information element	Status	Description
Identity	M	Identity of the requesting notification management client
Channel ID	M	Identifies the notification channel to be deleted
Request type	M	De-register or delete channel

17.3.2.6 Delete notification channel response

Table 17.3.2.6-1 describes the information flow delete notification channel response from notification management server to the notification management client.

Table 17.3.2.6-1: Delete notification channel response

Information element	Status	Description
Identity	M	Identity of the requesting notification management client
Result	M	Indicates if the deletion of the channel is success or failure or if the VAL server de-registered from channel successfully

17.3.2.7 Update notification channel request

Table 17.3.2.7-1 describes the information flow Update notification channel request from notification management client to the notification management server.

Table 17.3.2.7-1: Update notification channel request

Information element	Status	Description
Requestor identity	M	Identity of the requesting notification management client
Channel ID	M	Identifies the notification channel to be updated
Validity Duration	O	How long the notification channel will last (i.e. channel lifetime) as requested by the notification management client.

17.3.2.8 Update notification channel response

Table 17.3.2.8-1 describes the information flow Update notification channel request from notification management server to the notification management client.

Table 17.3.2.8-1: Update notification channel response

Information element	Status	Description
Validity duration	O	How long the notification channel will last (i.e. channel lifetime) as granted by the notification management server.
Result	M	Indicates if updating of the channel is success or failure

17.3.3 Procedure for creating notification channel to receive notifications

Figure 17.3.3-1 below illustrates the procedure for receiving notifications from the notification management server by the notification management client.

Pre-conditions:

1. The notification management client does not have any notification channel open with the notification management server.

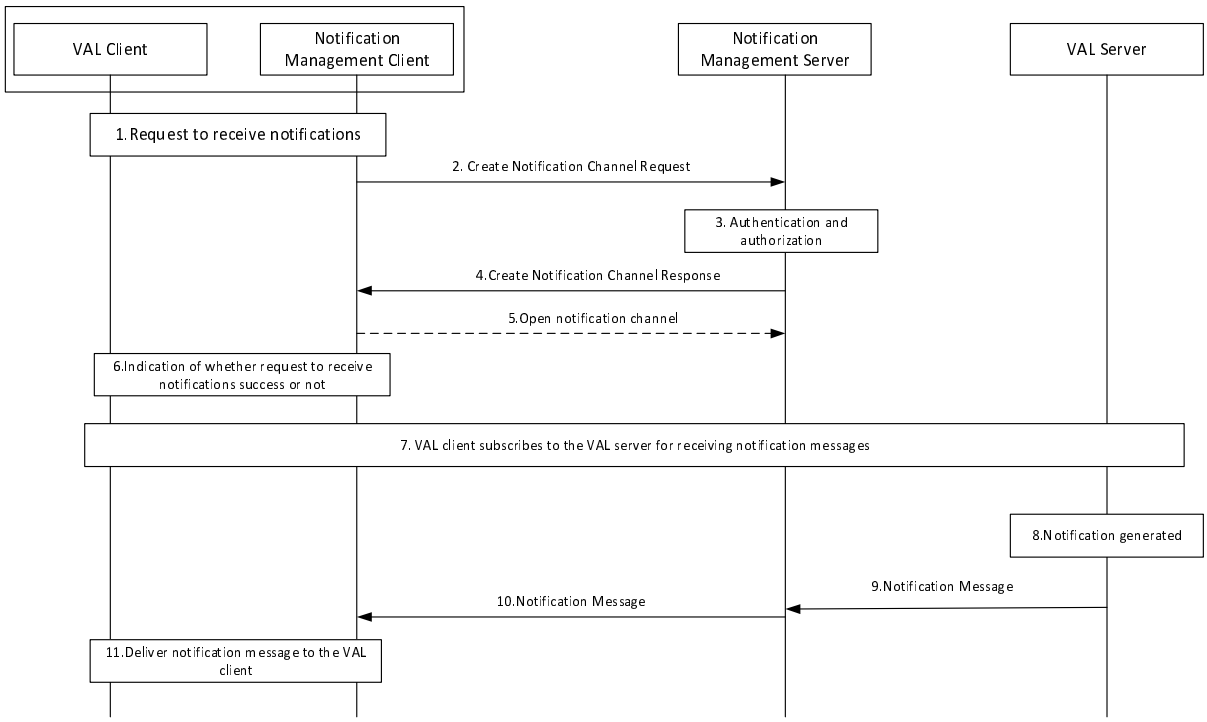

Figure 17.3.3-1: Receiving notifications from notification management server

1. The VAL client requests the notification management client to subscribe to and receive notifications from the VAL server.

2. The notification management client creates notification channels (i.e. endpoint URLs), if not created already, to be used by the VAL server to send notification messages. To create notification channel, the notification management client sends a create notification channel request to the notification management server. The desired validity duration for the channels to be used and the notification channel type (PUSH or PULL) are included in the request. The notification management client decides which type of the notification channel to be used based on the UE capability.

3. The notification management server authenticates the notification management client and authorizes its request.

4. The notification management server sends the notification management client the Create notification channel response with the endpoint URLs that will be used by the VAL server to send the notification messages and the notification management client to receive the notification messages. The notification management server also includes what is the valid duration for these endpoint URLs to be used and the channel ID to uniquely identify the channel created in the response.

5. If the notification type is PULL method, the notification management client sends the Open notification channel to the notification management server to start receiving the notification message. For certain PUSH method notification type (such as WebSockets) the notification management client requests the notification management server to start the PUSH notification service with its specific protocol that is outside the scope of this specification.

NOTE 1: This step is not required if the notification client wants to receive the notification messages via PUSH notification server.

6. The notification management client responds to the VAL client the status of its request as in step 1 to receive notifications from the VAL server. It also includes the callback URL which needs to be used by the VAL client while subscribing to the VAL server for receiving notifications.

7. The VAL client subscribes to the VAL server for receiving notifications. This request includes the subscription data and the callback URL returned from the notification management server in step 4.

NOTE 2: This step is outside the scope of this specification.

8. The VAL server generates the notification message for the subscription request from the VAL client.

9. The VAL server sends the notification message to the notification management server containing the VAL UE or VAL user ID, VAL service ID, VAL application ID and the notification data.

10. If the delivery method is PULL, the notification management server sends the notification message to the notification management client over the opened notification channel.

NOTE 3: If the delivery method is PUSH via PUSH notification server, the notification management server sends the notification message to the OEM Push server (not shown in the figure and is outside the scope of this specification) to deliver to the notification management client.

11. The notification management client delivers the received notification message to the appropriate VAL client based on the details as received in the notification message from the notification management server.

17.3.4 Procedure for deleting notification channel

Figure 17.3.4-1 below illustrates the procedure for deleting notification channel by the notification management client.

Pre-conditions:

1. The notification management client has notification channel open with the notification management server.

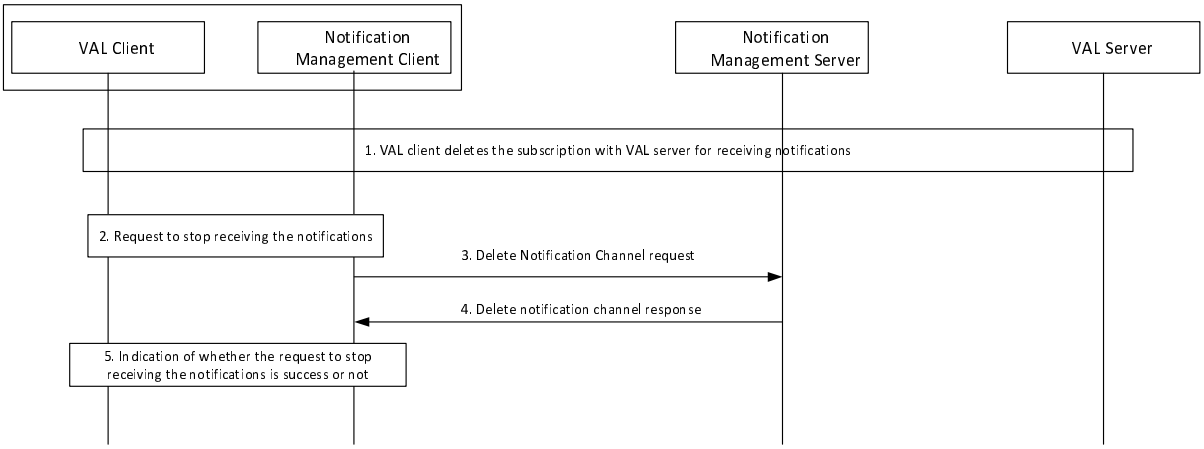

Figure 17.3.4-1: Deletion of notification channel by the notification management client

1. The VAL client decides to stop receiving notifications from the VAL server and deletes the subscription with the VAL server.

NOTE: Step 1 is outside the scope of 3GPP but triggers step 2.

2. The VAL client requests the notification management client to stop receiving the notifications.

3. If the same notification channel is being used for other VAL clients in the UE, the notification management client sends the delete notification channel request with request type as de-register otherwise the notification management client sends the delete notification channel request with request type as delete to the notification management server. The delete notification channel request carries the channel ID of the notification channel.

4. The notification management server acknowledges the request and sends the delete notification channel response to the notification management client.

5. The notification management client indicates to the VAL client about the status (de-registered or channel deleted or failure) of its request to stop receiving the notification.

17.3.5 Procedure for updating notification channel

Figure 17.3.5-1 below illustrates the procedure for updating the notification channel by the notification management client.

Pre-conditions:

1. The notification management client has notification channel open with the notification management server.

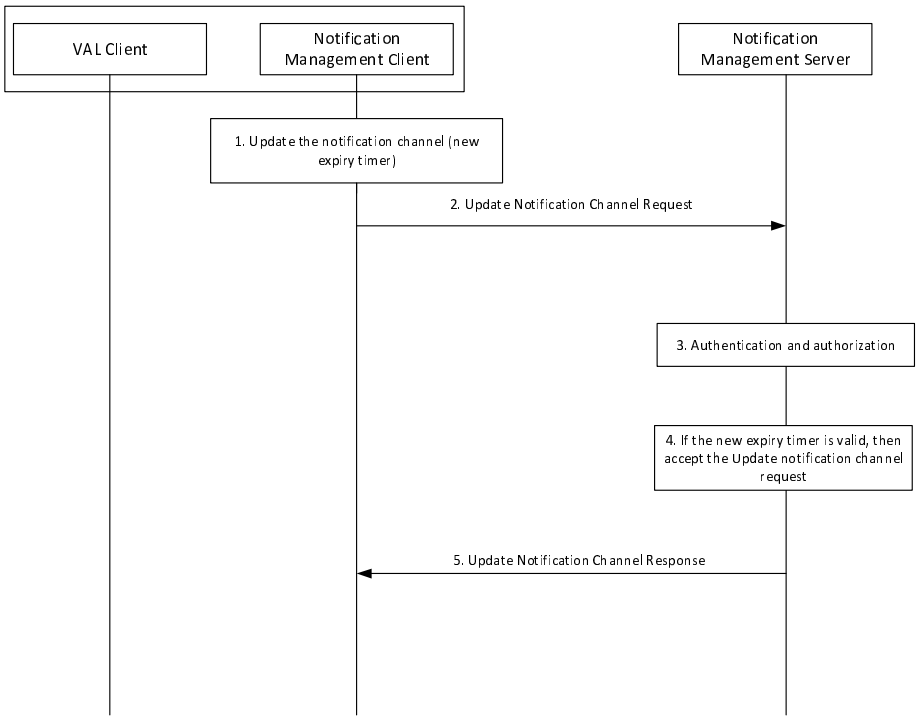

Figure 17.3.5-1: Updating notification channel by the notification management client

1. The notification management client detects the expiry timer of the active notification channel being approached and a need for updating the new expiry time on notification management server.

2. To update notification channel, the notification management client sends an update notification channel request to the notification management server with the proposed new validity duration for the active channel.

3. The notification management server authenticates the notification management client and authorizes its request.

4. The notification management server checks whether the new proposed expiry timer is valid or not. The NMS may accept the proposed validity duration from the request or assign a different validity duration based on the local policy.

5. The notification management server sends the notification management client the Update notification channel response with the valid duration for this active notification channel. The notification management client shall store the new valid duration of the notification management channel.

18 Data Delivery

18.1 General

With increasing demand of applications consumption over mobile networks, more and more application content is transmitted over the mobile networks. Vertical applications have diverse requirements for the application content distribution and delivery. To ease the various data delivery demands for vertical applications, a data delivery enabler offers the data delivery and storage capabilities to one or more vertical applications. The detailed specification of SEAL Data Delivery is provided in 3GPP TS 23.433 [48]

19 Application Data Analytics Enablement

19.1 General

The application data analytics enablement is a SEAL service that offers value-add application data analytics capabilities which cover stats/predictions for the end-to-end application service. Considering vertical-specific applications and edge applications as the major consumers of 3GPP-provided data analytics services, the application enablement layer can play role on the exposure of data analytics services from different 3GPP domains to the vertical/ASP in a unified manner; and on defining, at an overarching layer, value-add application data analytics services which cover stats/predictions for the end-to-end application service. The detailed specification of ADAE is provided in 3GPP TS 23.436 [49].

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.

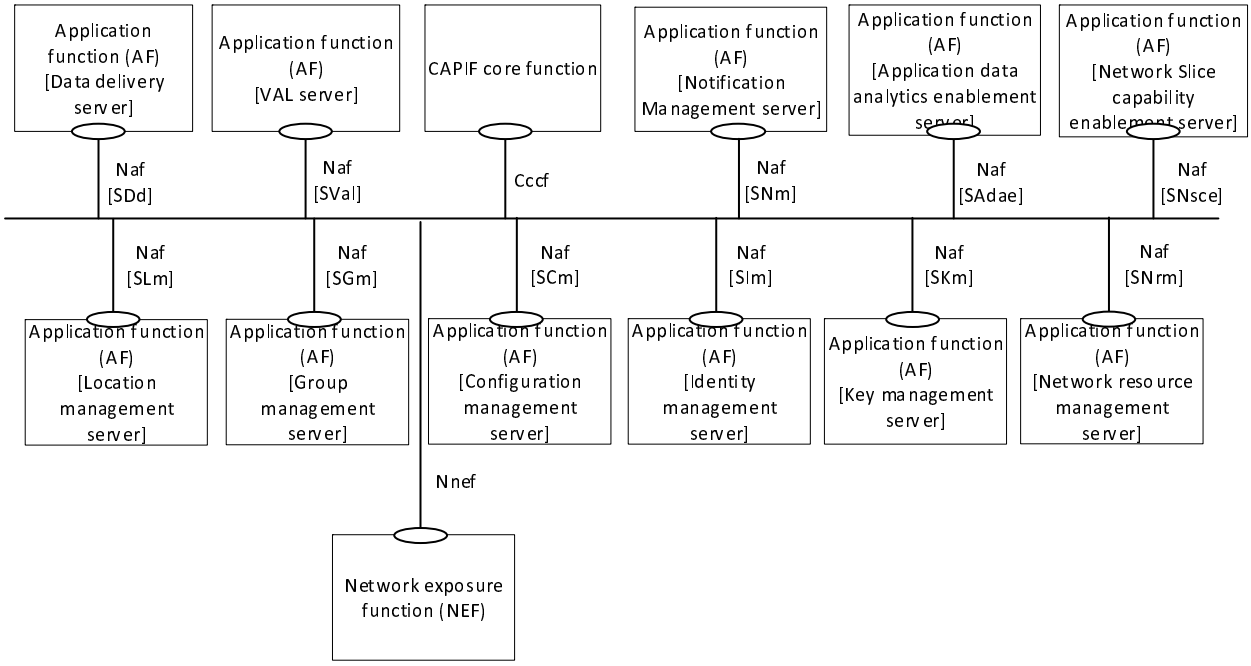

Figure A-1: SEAL integration with 5GC network exposure system

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.

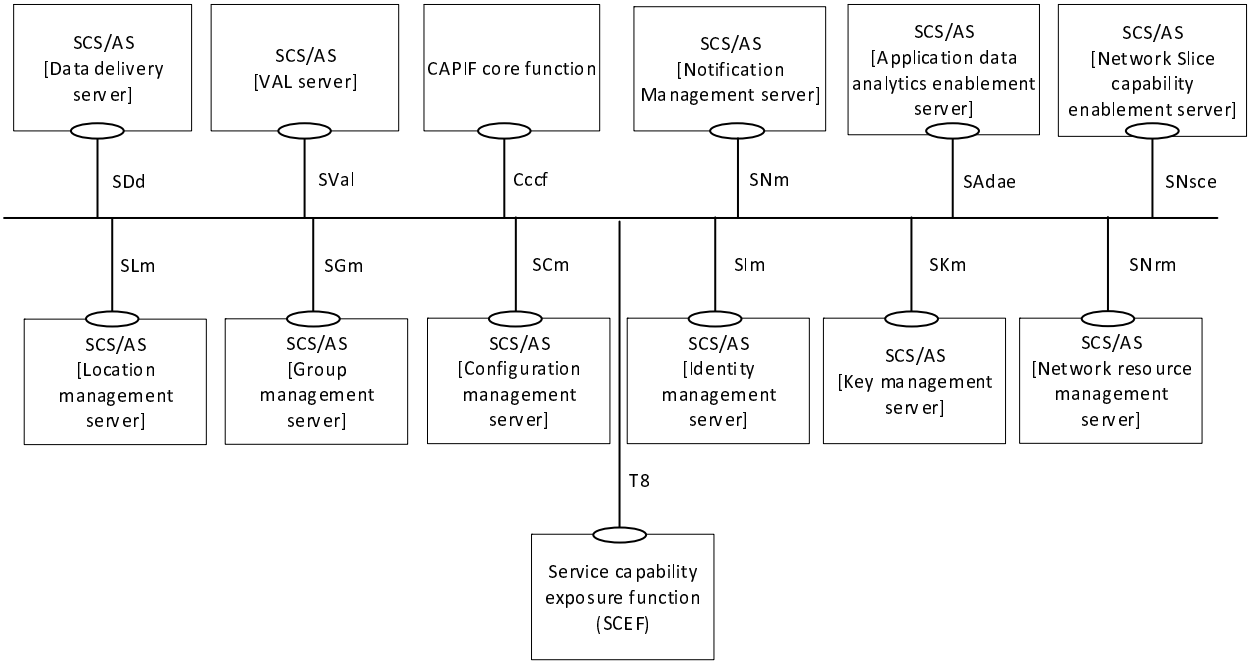

Figure A-2: SEAL integration with EPC network exposure system

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.

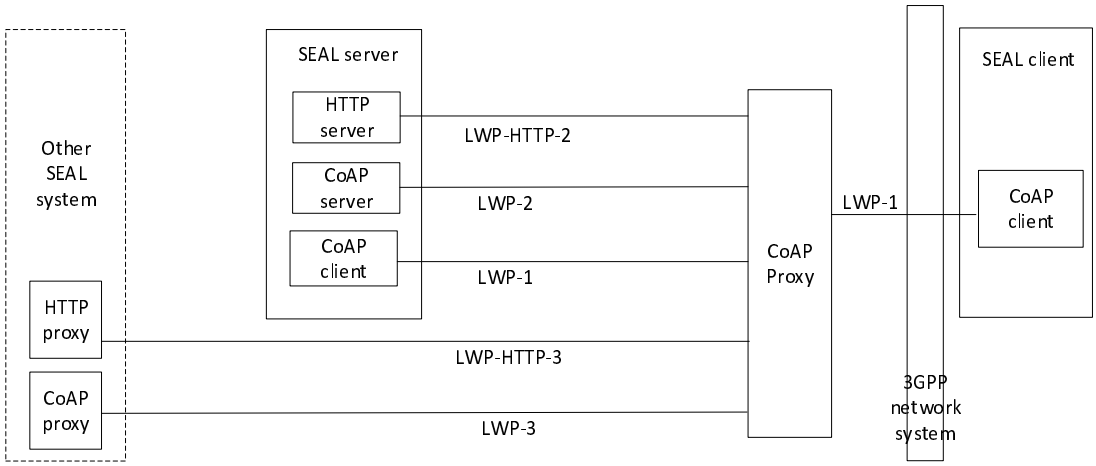

Figure C.2-1: Functional model for LWP signalling control plane when CoAP is used as LWP

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): Exemplary location profile attributes

The table D-1 shows the example of attributes that can be used for the location profiles.

Table D-1: Exemplary location profile attributes

Profile ID / name	Vertical / use case/environment	Positioning Service Level (for IIOT) / QoS / accuracy	Positioning Method(s) / Priorities	Involved 3GPP functionalities / Priorities	Required APIs / API info	Other
Location profile #1	Industrial scenario; indoors; mobile robots/ AGVs	Service Level 6 / cm level accuracy / absolute/relative/ both	1. DL-TDOA, 2. UL-TDOA, 3. Multi-RTT methods, 4. WLAN, 5. motion sensors, 6. Bluetooth	1. LMF 2. RAN-LMC, 3. SEAL LMS	NEF APIs, SEAL APIs	Verification / augmentation required
Location profile #2	V2X; outdoor	Decimeter level accuracy /... absolute/relative/both	1. DL-TDOA, 2. Multi-RTT methods, 3. GNSS-RTK, 4. Sensor fusion, 5. A-GPS	1. LMF 2. SEAL LMS 3. Other UEs	NEF APIs, MEC APIs	Support for sidelink positioning

Annex E (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
2022-03	SA#95-E	SP-220102	0091	1	B	Complete location retrieval in an area	18.0.0
2022-06	SA#96	SP-220473	0097	2	A	Minor essential corrections to TS 23.434	18.1.0
2022-06	SA#96	SP-220473	0101		A	Minor corrections on network resource management for 5G TSC	18.1.0
2022-06	SA#96	SP-220473	0103	2	A	QoS monitoring clarification	18.1.0
2022-09	SA#97-E	SP-220925	0104	3	B	SEAL Notification Management service – Functional Model	18.2.0
2022-09	SA#97-E	SP-220925	0105	3	B	SEAL Notification Management service – Information Flows and Procedures	18.2.0
2022-09	SA#97-E	SP-220920	0108	1	A	EN resolution for network slice adaptation request	18.2.0
2022-09	SA#97-E	SP-220925	0110	1	B	Establishing communication with service requirements	18.2.0
2022-09	SA#97-E	SP-220925	0111	2	B	Information flows and procedures to maintain notification channel	18.2.0
2022-09	SA#97-E	SP-220925	0112	1	B	Update_Unicast_QoS_Monitoring_Subscription operation in the SS_NetworkResourceMonitoring API	18.2.0
2022-09	SA#97-E	SP-220920	0115	2	A	Correction on location management information flow	18.2.0
2022-09	SA#97-E	SP-220925	0116		B	Update the scope and reference to support 5MBS	18.2.0
2022-09	SA#97-E	SP-220925	0117	2	B	Update the requirement to support 5MBS	18.2.0
2022-09	SA#97-E	SP-220925	0118	1	B	Update the NRM functional model to support 5MBS	18.2.0
2022-09	SA#97-E	SP-220925	0119	1	B	MBS session creation and MBS session announcement	18.2.0
2022-09	SA#97-E	SP-220925	0120	2	B	Updating MBS resources for group communications	18.2.0
2022-09	SA#97-E	SP-220925	0121	1	B	MBS session deletion	18.2.0
2022-09	SA#97-E	SP-220925	0122		B	Activate or de-activate multicast MBS sessions	18.2.0
2022-09	SA#97-E	SP-220925	0123		B	Group media transmissions over 5G MBS sessions	18.2.0
2022-09	SA#97-E	SP-220925	0124		B	Application level control signalling over 5G MBS sessions	18.2.0
2022-12	SA#98-E	SP-221244	0106	9	B	VAL Server provisioning	18.3.0
2022-12	SA#98-E	SP-221244	0126	2	B	Update the NSCE functional	18.3.0
2022-12	SA#98-E	SP-221244	0127	2	B	Enhance the APIs of the network slice adaptation	18.3.0
2022-12	SA#98-E	SP-221249	0129		B	Update to SEAL architecture to include SEALDD	18.3.0
2022-12	SA#98-E	SP-221244	0130	1	F	Definition of MBS session announcement	18.3.0
2022-12	SA#98-E	SP-221244	0131	1	B	Information flows for MBS procedures	18.3.0
2022-12	SA#98-E	SP-221244	0133	1	B	Updating MBS with dynamic PCC	18.3.0
2022-12	SA#98-E	SP-221244	0134	2	B	NRM coordination for redundant PDU Session establishment	18.3.0
2022-12	SA#98-E	SP-221244	0136	2	B	VAL service area identifier usage	18.3.0
2022-12	SA#98-E	SP-221244	0137		F	Add Cause IE to NSCE information flows	18.3.0
2022-12	SA#98-E	SP-221244	0138	2	F	ADAE functional model in SEAL architecture	18.3.0
2022-12	SA#98-E	SP-221244	0139	2	F	Service continuity between 5G MBS delivery and unicast delivery	18.3.0
2022-12	SA#98-E	SP-221244	0140	3	B	VAL service inter-system switching between 5G and LTE	18.3.0
2022-12	SA#98-E	SP-221244	0141	1	B	VAL service over 5GS supporting EPS interworking	18.3.0
2023-03	SA#99	SP-230283	0142	3	B	Update the on-network functional model and reference points for location management	18.4.0
2023-03	SA#99	SP-230283	0147	2	B	Location profiling for supporting fused location service enablement	18.4.0
2023-03	SA#99	SP-230283	0148	4	B	Add information flow for location reporting configuration update	18.4.0
2023-03	SA#99	SP-230283	0149	2	B	Location service registration and initialization	18.4.0
2023-03	SA#99	SP-230283	0152	1	B	Improved location monitoring procedure	18.4.0

2023-03	SA#99	SP-230293	0153	1	F	Service based interface representation of location management service	18.4.0
2023-03	SA#99	SP-230293	0154	1	F	Service based interface representation of group managment	18.4.0
2023-03	SA#99	SP-230293	0155	1	F	Service based interface representation of network resource management service	18.4.0
2023-03	SA#99	SP-230293	0156	1	F	Update Annex A with details of new SEAL services added	18.4.0
2023-03	SA#99	SP-230293	0158	1	F	Updates to service based interface represeentation of functional model	18.4.0
2023-03	SA#99	SP-230293	0159	2	B	Information flow for VAL server provisioning to the Identity Management Server	18.4.0
2023-03	SA#99	SP-230284	0162		D	Alignment between TS 23.434 and TS 23.436	18.4.0
2023-03	SA#99	SP-230292	0163	1	D	Alignment between TS 23.434 and TS 23.435	18.4.0
2023-03	SA#99	SP-230294	0164	1	B	Update to the SEALDD description	18.4.0
2023-03	SA#99	SP-230293	0168	3	F	Add “supplementary location information source” parameter in related information flows	18.4.0
2023-03	SA#99	SP-230283	0169	2	B	Update the Procedure and information flow to add location QoS	18.4.0
2023-03	SA#99	SP-230293	0170	1	F	Add the information flow for “Location reporting configuration cancel request response”	18.4.0
2023-03	SA#99	SP-230283	0172	2	B	Add third party location management server in existing procedure	18.4.0
2023-03	SA#99	SP-230293	0174		F	Adding missing SEAL services	18.4.0
2023-03	SA#99	SP-230293	0179	1	F	Resolving ENs related to functions enabled over SEAL-E reference point	18.4.0
2023-03	SA#99	SP-230293	0182	1	B	RAT change report via the LMS	18.4.0
2023-03	SA#99	SP-230293	0183	1	F	Clarification on MBS service area in pre-conditions	18.4.0
2023-03	SA#99	SP-230293	0184	1	F	Clarification on UE session join notification	18.4.0
2023-03	SA#99	SP-230293	0185	1	F	Clarification on the unicast deliver stop after multicast MBS delivery	18.4.0
2023-03	SA#99	SP-230293	0186	1	B	Adding MBS listening status report	18.4.0
2023-03	SA#99	SP-230293	0189	1	F	Minor correction on get VAL service	18.4.0
2023-04						Correction of the step 8 style in clause 9.3.14.2	18.4.1
2023-06	SA#100	SP-230712	0143	4	B	Service operations for the SS_VALServiceAreaConfiguration API	18.5.0
2023-06	SA#100	SP-230712	0160	4	B	VAL server provisioning for Key Management Server	18.5.0
2023-06	SA#100	SP-230696	0190	1	C	Update Location service registration request	18.5.0
2023-06	SA#100	SP-230696	0191	1	C	Update Location information request IE	18.5.0
2023-06	SA#100	SP-230696	0192	2	B	Add “location information unsubscribe” and “Monitor location unsubscribe” information flow, procedure and APIs	18.5.0
2023-06	SA#100	SP-230696	0193	1	B	Add “Location service update” procedure and information flow	18.5.0
2023-06	SA#100	SP-230696	0194	1	B	Add “Location service deregistration” procedure and information flow	18.5.0
2023-06	SA#100	SP-230696	0195	1	B	Add “Location service deregistration” procedure and information flow	18.5.0
2023-06	SA#100	SP-23712	0197	1	B	Notification channel expiry handling	18.5.0
2023-06	SA#100	SP-23712	0202	1	F	Create_Group service operation in the SS_GroupManagement API	18.5.0
2023-06	SA#100	SP-23712	0205	2	C	QoS management for network-assisted UE-to-UE communications update	18.5.0
2023-06	SA#100	SP-23704	0206	1	B	Location report considering non-3GPP positioning technology	18.5.0
2023-06	SA#100	SP-23712	0207		F	Minor fixes	18.5.0
2023-06	SA#100	SP-23712	0208	1	F	Abbreviation for Uu	18.5.0
2023-06	SA#100	SP-23712	0209		F	Correction to table 17.3.2.2-1	18.5.0
2023-06	SA#100	SP-23712	0212	2	B	Unified Traffic Pattern and Monitoring management	18.5.0
2023-06	SA#100	SP-23712	0213	2	B	NRM BDT configuration	18.5.0
2023-06	SA#100	SP-23712	0215	2	B	Coordinated application-level direct UE-to-UE communications	18.5.0
2023-06	SA#100	SP-23696	0216		F	Update reference for location access type	18.5.0
2023-06	SA#100	SP-23696	0217		F	Update Annex D	18.5.0
2023-06	SA#100	SP-23696	0218	1	B	Add SEAL-3P reference point	18.5.0
2023-06	SA#100	SP-23696	0219	1	F	Editorial change for Location area monitoring unsubscribe response	18.5.0
2023-06	SA#100	SP-23696	0221	1	F	Clarify non-3GPP access	18.5.0
2023-06	SA#100	SP-23712	0223	2	B	SEAL NRM determines time synchronization activation for TSC stream	18.5.0
2023-09	SA#101	SP-231009	0225	1	F	Correct location monitoring verification	18.6.0
2023-09	SA#101	SP-231009	0226		F	Correct NRM reference point in TSC	18.6.0
2023-09	SA#101	SP-231009	0227	2	F	VAL service area triggering criteria in the SS_LocationReporting API	18.6.0
2023-09	SA#101	SP-231009	0228	2	F	EN resolution for the subscribe-notify service operations for the SS_VALServiceAreaConfiguration API	18.6.0
2023-09	SA#101	SP-231009	0229		F	Add reason IE to Group deletion	18.6.0
2023-09	SA#101	SP-231000	0231	2	F	NRM BDT configuration API	18.6.0
2023-09	SA#101	SP-231000	0232		F	NRM united traffic pattern and monitoring management API	18.6.0
2023-12	SA#102	SP-231565	0233	1	F	Complete functional description of VAL-UDB reference point	18.7.0
2023-12	SA#102	SP-231565	0235		F	Missing Notification Target URI in Location area monitoring subscription operations	18.7.0
2023-12	SA#102	SP-231565	0237	1	F	Update subscription service operation for SS_LocationInfoEvent	18.7.0
2023-12	SA#102	SP-231565	0238	1	F	Update subscription service operation for SS_LocationMonitoring	18.7.0
2023-12	SA#102	SP-231564	0241		A	Notification service operation in the SS_LocationReporting API	18.7.0
2023-12	SA#102	SP-231555	0243		A	Correction of the TSC stream creation request	18.7.0

2023-12	SA#102	SP-231565	0244	2	F	Subscription update service operation for the SS_VALServiceAreaConfiguration API	18.7.0
2023-12	SA#102	SP-231565	0246	2	F	SS_IdmParameterProvisioning API service operations	18.7.0
2023-12	SA#102	SP-231565	0248	1	F	Removal of KMS service provisioning procedure	18.7.0
2023-12	SA#102	SP-231555	0250	2	A	Corrections to Location-based group creation request Information flow	18.7.0
2023-12	SA#102	SP-231564	0253	1	A	Corrections to the Information flows and APIs for Group Management	18.7.0
2023-12	SA#102	SP-231564	0256	1	A	Corrections to the information flows related to CM	18.7.0
2023-12	SA#102	SP-231564	0259		A	Subscription procedure for group membership changes is missing	18.7.0
2023-12	SA#102	SP-231565	0262	1	F	Clarification on Location reporting trigger	18.7.0
2023-12	SA#102	SP-231565	0264	1	F	Correction steps in VAL service area identifier procedure	18.7.0
2023-12	SA#102	SP-231565	0265	2	F	Missing request expiration time in BDT configuration request	18.7.0
2023-12	SA#102	SP-231565	0266	1	A	Group configuration data unsubscribe	18.7.0
2023-12	SA#102	SP-231565	0267	1	A	Group configuration data subscription update	18.7.0
2023-12	SA#102	SP-231565	0270	1	F	Correction duplicated numbering clause 14.3.2.57	18.7.0
2023-12	SA#102	SP-231565	0271	1	F	Adding the information flow and AP for NRM reliable transmission	18.7.0
2023-12	SA#102	SP-231565	0272		F	Corrections for BDT configuration	18.7.0
2023-12	SA#102	SP-231565	0273	1	F	Corrections for BDT configuration information flows	18.7.0
2023-12	SA#102	SP-231565	0274	1	F	Correction to add missing get operation for BDT configuration	18.7.0
2023-12	SA#102	SP-231565	0275	1	F	Correction to add missing update operation for BDT configuration	18.7.0
2023-12	SA#102	SP-231565	0276	2	F	Correction to add missing delete operation for BDT configuration	18.7.0
2023-12	SA#102	SP-231565	0277	1	F	Correction to add missing API operations for BDT configuration	18.7.0
2024-03	SA#103	SP-240298	0284	1	A	UE identifiers correction in the SS_LocationAreaInfoRetrieval API	18.8.0
2024-03	SA#103	SP-240298	0290		A	Correct IE presence condition	18.8.0
2024-06	SA#104	SP-240750	0295		A	Solve EN in location info request	18.9.0
2024-06	SA#104	SP-240762	0297		F	Correct location triggering criteria in update request	18.9.0
2024-06	SA#104	SP-240762	0299		F	Solve EN in NM related to CAPIF	18.9.0
2024-06	SA#104	SP-240762	0301		F	Solve EN in SEAL clause 14.3.12	18.9.0
2024-12	SA#106	SP-241710	0317	1	F	Remove reference for 23.545 in SEAL	18.10.0
2024-12	SA#106	SP-241710	0321	2	F	TS 23.434 Rel-18 - Handling Editors Notes	18.10.0
2024-12	SA#106	SP-241710	0348	2	F	Void MBMS bearer event notification procedure in clause 14.3.4.8	18.10.0
2024-12	SA#106	SP-241710	0350		F	Resolve the 2nd EN in clause 15.2	18.10.0
2024-12	SA#106	SP-241710	0352	1	F	Resolve the EN in clause 14.3.4.5.2	18.10.0
2024-12	SA#106	SP-241710	0359	1	F	MBS service area handling at NRM	18.10.0
2024-12	SA#106	SP-241710	0319	2	F	Solve EN in SEAL clause 9.5.1	18.10.1
2025-03	SA#107	SP-250201	0365	1	F	Resolve the EN about the security and privacy aspects for location management	18.11.0

History

Document history		
V18.8.0	April 2024	Publication
V18.9.0	July 2024	Publication
V18.10.1	January 2025	Publication
V18.11.0	April 2025	Publication