ETSI TS 123 433 V19.7.1 (2025-10)

TECHNICAL SPECIFICATION

LTE;
5G;
Service Enabler Architecture Layer for Verticals (SEAL);
Data Delivery enabler for vertical applications
(3GPP TS 23.433 version 19.7.1 Release 19)

Reference
RTS/TSGS-0623433vj71

Keywords
5G,LTE

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.

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

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

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

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

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

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

can indicates that something is possible

cannot indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

Introduction

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 is specified in this document.

The data delivery service is part of the SEAL services specified in 3GPP TS 23.434 [4].

1 Scope

The present document specifies the application enabling layer platform architecture, capabilities and services to efficiently support storage and delivery for the application content/data for vertical applications as part of SEAL services specified in 3GPP TS 23.434 [4].

This work takes into consideration the existing stage 1 and stage 2 work within 3GPP related to data delivery and 3GPP system user plane aspects specified in 3GPP TS 22.261 [2] and 3GPP TS 23.501 [5].

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 22.261: "Service requirements for the 5G system; Stage 1".

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

[4] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

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

[6] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[7] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[8] 3GPP TS 23.548: "5G System Enhancements for Edge Computing ".

[9] 3GPP TS 23.554: "Application architecture for MSGin5G Service; Stage 2".

[10] 3GPP TS 23.558: "Architecture for enabling Edge Applications".

[11] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics (MDA)".

[12] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[13] 3GPP TS 23.436: "Functional architecture and information flows for Application Data Analytics Enablement Service".

[14] 3GPP TS 26.501: "5G Media Streaming (5GMS); General description and architecture".

[15] 3GPP TS 26.506: "5G Real-time Media Communication Architecture (Stage 2)".

[16] 3GPP TS 23.303: "Proximity-based Services (ProSe); Stage 2".

[17] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[18] ITU-T Recommendation P.1203.3: "Parametric bitstream-based quality assessment of progressive download and adaptive audiovisual streaming services over reliable transport - Quality integration module".

[19] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[20] 3GPP TS 26.118: "Virtual Reality (VR) profiles for streaming applications".

[21] 3GPP TS 23.435: "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service".

[22] 3GPP TS 23.482: "Functional architecture and information flows for AIML Enablement Service".

[23] 3GPP TS 23.542: "Application layer support for Personal IoT Network".

[24] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[25] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[26] 3GPP TS 24.543: "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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

Application connection: Association between the VAL client and the VAL service to provide the VAL service.

Application traffic: a set of signaling messages or a set of media packet constituting a application service flow. E.g., one or more picture(s) may be an application traffic, the audio stream and the video stream are two different application traffic.

Crossflow QoS measurement is an E2E measurement between SEALDD client and SEALDD server that considers multi-modal traffic routes in combination of uplink direction and downlink direction for same application.

Multi-modal SEALDD flows: a set of individual SEALDD flows that are associated with each other for a particular application that requires synchronization among the individual SEALDD flows.

SEALDD–S connection: Association between the SEALDD server and the VAL server to achieve data delivery of the application traffic. One application connection may have one SEALDD-S connection, e.g., for all the application traffic flows, or have more SEALDD-S connections, e.g., one for application signaling flow, and the other or application media traffic flow(s). A SEALDD-S connection shall be uniquely identified between the VAL server and the SEALDD server.

SEALDD-S flows: a set of packets have the same attributes, e.g., the same 5-tuple, media type. The application traffic flow may be mapped to one ore more SEALDD-S flow(s). A SEALDD-S flow should be uniquely identified with the SEALDD-S connection.

SEALDD-UU connection: Association between the SEALDD server and the SEALDD client to achieve the data delivery of the application traffic from the VAL server or the VAL client. One SEALDD-S connection may be associated with one SEALDD-UU connection or multiple SEALDD-UU connections. A SEALDD-UU connection shall be uniquely identified between the SEALDD client and the SEALDD server.

SEALDD-UU flows: a set of packets have the same attributes, e.g., the same 5-tuple, media type, QoS requirements. One SEALDD-S flow(s) may be mapped to one or multiple SEALDD-UU flows. A SEALDD-UU flow should be uniquely identified with the SEALDD-UU connection.

3.2 Symbols

None

3.3 Abbreviations

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

AF	Application Function
CAPIF	Common API Framework for northbound APIs
DD	Data Delivery
EAS	Edge Application Server
EDN	Edge Data Network
NRM	Network Resource Management
SBA	Service Based Architecture
SCEF	Service Capability Exposure Function
SEAL	Service Enabler Architecture Layer for verticals
SEALDD	SEAL Data Delivery
URSP	UE Route Selection Policy
VAL	Vertical Application Layer

4 Overview

4.1 General

This clause gives a functionality overview for SEALDD service.

4.2 Application signalling and data transmission

This SEALDD functionality provides a mechanism for application signalling data transmission and application media data transmission between VAL client(s) and VAL server(s). The SEALDD enabled regular connection management procedures (e.g. connection establishment, connection deletion) are specified in clause 9.2. For supporting URLLC feature, the SEALDD layer establishes E2E redundant transmission with packet duplication and elimination, as specified in clause 9.3.

4.3 Transmission quality measurement and transmission optimization

The transmission quality measurement procedure specified in clause 9.7, supports the E2E transmission quality measurement between SEALDD client and SEALDD server, and exposes the transmission reports to VAL servers and other consumers (e.g. SEALDD server, NSCE server, etc). Based on the SEALDD enabled E2E transmission measurement result, the SEALDD layer provides transmission optimization scheme (e.g. triggering redundant transmission, switching another SEALDD server) to improve transmission quality by interacting with 5GC. The transmission optimization procedures are specified in clause 9.9.

4.4 Data transmission rate control

The SEALDD layer provides the differentiated data delivery service with different bandwidth/transmission rate experience for VAL users, considering the network conditions (e.g. QoS monitoring, ECN marking for L4S report), which is described in clause 9.8.

4.5 Service continuity support

This functionality is provided to support service continuity due to UE mobility or load balance. The SEALDD layer maintains the transport layer connection by interacting SEALDD context, and requesting 5GC to perform seamless data transmission (e.g. IP replacement procedure, simultaneous connectivity). The service continuity support procedures are specified in clause 9.6.

4.6 Data storage

The SEALDD server supports the data storage and storage management for VAL server, SEALDD client and other SEALDD servers, etc, the corresponding procedure is specified in clause 9.5.

4.7 Background Data Transfer

This SEALDD functionality enables to keep data transmission costs lower by favouring time windows for data transfer to/from specific UEs in a geographical area, e.g. during non-busy hours, that are less costly and able to handle larger bitrates. The background data transfer procedures are specified in clause 9.11.

4.8 SEALDD enabled transmission for multi-modal service

This SEALDD functionality enables data transmission for multi-modal service, e.g., XR application service, etc. The supported services include SEALDD enabled multi-modal data transmission service for multi-modal application, SEALDD enabled multi-modal flow synchronization, SEALDD enabled UE-to-UE communication based on policy, and tethering link measurement and provisioning. The procedures are specified in clause 9.12.

5 Business relationships

5.1 General

The clause specifies the business relationships between the various stakeholders like VAL user, VAL service provider, SEALDD provider and PLMN operator.

5.2 Business relationship option-A

Figure 5.2-1 shows the business relationship option-A that exist and that are needed to support a single VAL user.

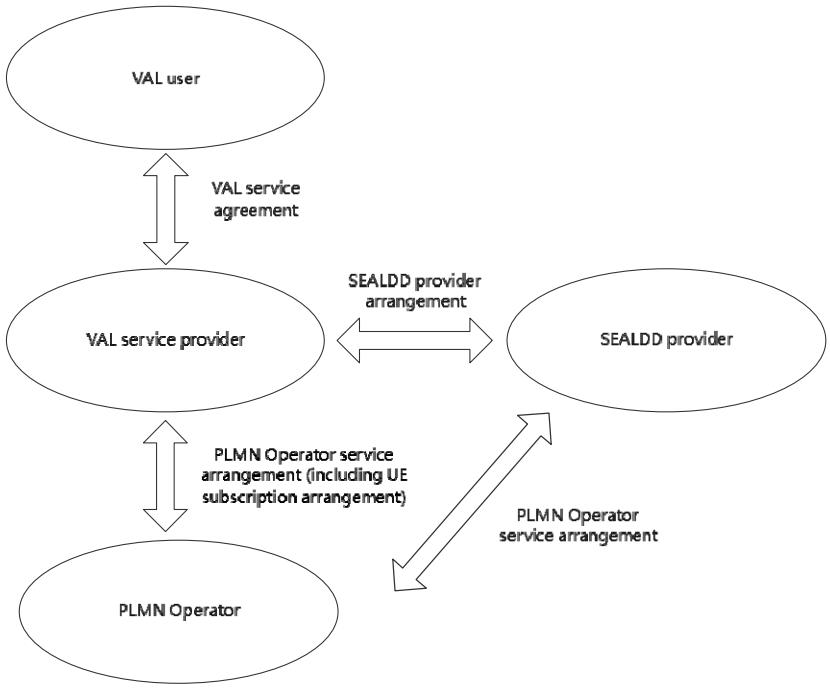

Figure 5.2-1: Business relationship option-A for VAL services

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 may have VAL service agreements with several VAL users. The VAL user may have VAL service agreements with several VAL service providers.

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

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

NOTE: The roaming cases are not discussed in this release.

5.3 Business relationship option-B

Figure 5.3-1 shows the business relationship option-B that exist and that are needed to support a single VAL user.

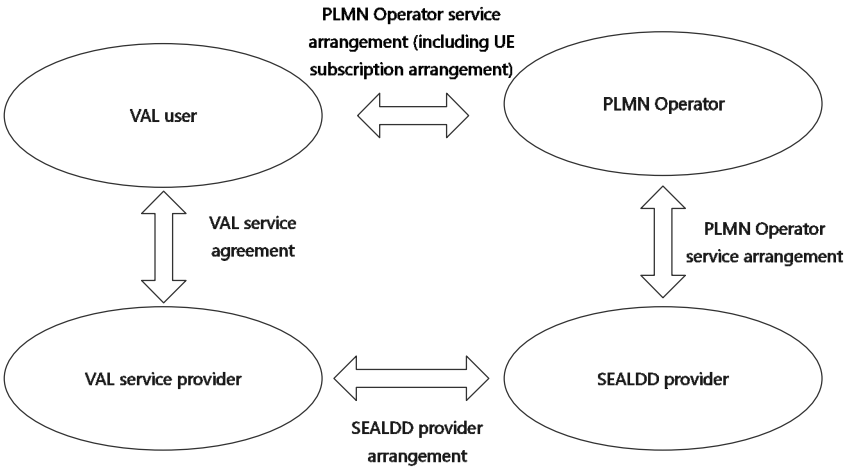

Figure 5.3-1: Business relationship option-B for VAL services

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 may have VAL service agreements with several VAL users. The VAL user may have VAL service agreements with several VAL service providers.

The VAL user may have PLMN operator service arrangements with the PLMN operator. The PLMN operator service arrangement includes the UE subscription arrangement which allows the VAL UEs to register with operator network.

The VAL service provider may have SEALDD provider arrangements with multiple SEALDD providers and the SEALDD provider may have SEALDD provider arrangements with multiple VAL service providers.

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

NOTE: The roaming cases are not discussed in this release.

6 Architectural requirements

6.1 General

6.1.1 Description

The general architecture requirements specified in clause 4.1 of 3GPP TS 23.434 [4] are applicable for SEALDD service. This clause specifies the general requirements for SEALDD service.

6.1.2 Requirements

[AR-6.1.2-a] The SEALDD service shall provide a discovery mechanism to support data delivery between VAL client(s) and VAL servers(s) considering different deployments of VAL server(s) (e.g. cloud or edge).

6.2 Data transmission requirements

6.2.1 Description

This clause specifies the data transmission requirements for SEALDD service.

6.2.2 Requirements

[AR-6.2.2-a] The SEALDD service shall provide a mechanism for application signalling data transmission and application media data transmission between VAL client(s) and VAL server(s).

[AR-6.2.2-b] The SEALDD service shall provide a mechanism to support the data transmission quality requirement configurations and measurements for the application data transmission between VAL client(s) and VAL server(s).

[AR-6.2.2-c] The SEALDD service shall provide a mechanism for application data transmission between VAL client(s) and VAL server(s) with guaranteed quality.

[AR-6.2.2-d] The SEALDD service shall provide a mechanism for application data packaging and un-packaging to support the data transmission between VAL client(s) and VAL server(s).

[AR-6.2.2-e] The SEALDD service shall provide a mechanism for E2E redundant data transmission between VAL client and VAL server.

[AR-6.2.2-f] The SEALDD service shall provide a mechanism to support the packet/data duplication, elimination and error recovery between VAL client and VAL server.

[AR-6.2.2-g] The SEALDD service shall provide a mechanism to support favouring time windows for data transfer between VAL client(s) and VAL server(s) that are less costly and/or able to handle larger bitrates.

6.3 Data storage requirements

6.3.1 Description

This clause specifies the data storage requirements for SEALDD service.

6.3.2 Requirements

[AR-6.3.2-a] The SEALDD service shall provide a mechanism for data storage supporting the CRUD operations.

[AR-6.3.2-b] The SEALDD service shall provide a mechanism to support the data storage status management.

6.4 SEALDD server discovery and selection requirements

6.4.1 Description

This clause specifies the SEALDD server discovery and selection requirements for SEALDD service.

6.4.2 Requirements

[AR-6.4.2-a] The SEALDD service shall provide a mechanism for supporting the SEALDD server discovery and selection for VAL server.

[AR-6.4.2-b] The SEALDD service shall provide a mechanism to provide the information of SEALDD server to VAL/SEALDD client.

6.5 MSGin5G message transfer requirements

6.5.1 Description

This clause specifies the MSGin5G message transfer requirements for SEALDD service.

6.5.2 Requirements

[AR-6.5.2-a] The SEALDD service shall provide a mechanism to support the SEALDD traffic transmission using MSGin5G message.

6.6 Data transmission bandwidth control requirements

6.6.1 Description

This clause specifies the data transmission bandwidth control requirements for SEALDD service.

6.6.2 Requirements

[AR-6.6.2-a] The SEALDD service shall provide a mechanism to support the transmission bandwidth control for VAL application.

7 Architecture

7.1 General

The architecture for the SEAL data delivery enabler is based on the generic functional model specified in clause 6.2 of 3GPP TS 23.434 [4].

This clause provides the overall architecture description:

- Clause 7.2 describes the functional architecture;
- Clause 7.3 describes the functional entities;
- Clause 7.4 describes the reference points; and
- Clause 7.5 describes the cardinality of functional entities and reference points.

7.2 Architecture

This clause describes the architecture for enabling SEAL Data Delivery applications in the following representations:

- A service-based representation as specified in 3GPP TS 23.434 [4], where the SEAL Data Delivery Enabler Layer functions (e.g. SEALDD server) enable other authorized Vertical Application Layer functions (e.g. VAL server) to access their services.
- A service-based representation as specified in 3GPP TS 23.501 [5], where the Network Functions (e.g. NEF) enable authorized SEAL Data Delivery Layer functions (e.g. SEALDD server) i.e. Application Functions, to access their services;
- A service-based representation, where the Core Network Northbound APIs as specified in 3GPP TS 23.501 [5] and 3GPP TS 23.502 [6], are utilized by authorized SEAL Data Delivery Enabler Layer functions via CAPIF core function specified in 3GPP TS 23.222 [3]; and

- A reference point representation, where existing interactions between any two functions (e.g. SEALDD client and SEALDD server) is shown by an appropriate point-to-point reference point (e.g. SEALDD-UU).

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

The service based representation of SEAL Data Delivery function in the overall SEAL service-based representation is specified in clause 15 of 3GPP TS 23.434 [4]. The SEALDD function exhibits service-based interfaces which are used for providing and consuming SEALDD services. The service-based interface for SEALDD function is representation as Sdd.

Figure 7.2-1 illustrates the service-based representation for utilization of the 5GS network services based on the 5GS SBA specified in 3GPP TS 23.501 [5].

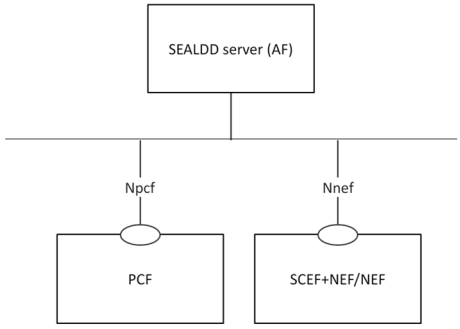

Figure 7.2-1: Utilization of 5GS network services based on the 5GS SBA – service based representation

The SEALDD server acts as AF for consuming network services from the 3GPP 5G Core Network entities over the Service Based Architecture specified in 3GPP TS 23.501 [5].

Figure 7.2-2 illustrates the service-based representation for utilization of the Core Network (5GC, EPC) northbound APIs via CAPIF.

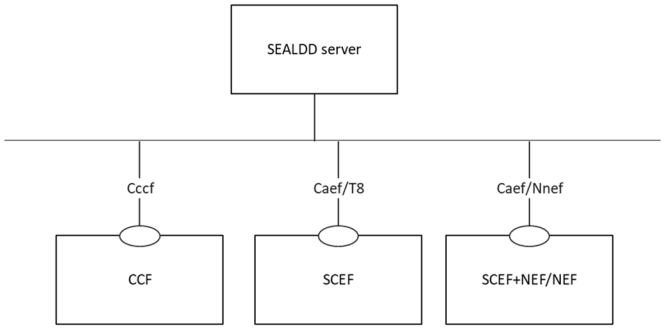

Figure 7.2-2: Utilization of Core Network Northbound APIs via CAPIF – service based representation

The SEALDD 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 [3].

The mechanism for northbound APIs discovery using the service-based interfaces depicted in figure 7.2-3 is as specified in 3GPP TS 23.222 [3].

Figure 7.2-3 illustrates the architecture for SEAL Data Delivery enabler service.

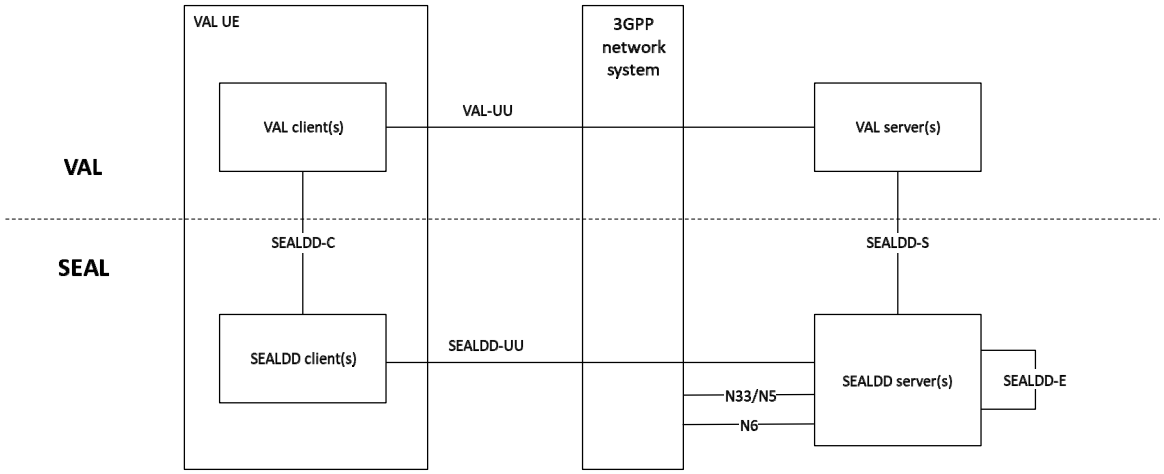

Figure 7.2-3: Architecture for SEAL Data Delivery Service

The SEALDD server communicates with the control plane of 3GPP core network via N33/N5 interface with the SEALDD control plane functionality. The SEALDD server may consume other SEAL (e.g. NRM) services.

For uplink traffic, VAL client sends application data traffic to SEALDD client for SEALDD service over SEALDD-C. After data plane packet processing by SEALDD client, the application data traffic is converted to SEALDD data traffic and transferred to SEALDD server over SEALDD-UU. The SEALDD server restores the application data traffic and sends it to VAL server over SEALDD-S. For downlink traffic, VAL server sends application data traffic to SEALDD server for SEALDD service over SEALDD-S. After data plane packet processing by SEALDD server, the application data traffic is converted to SEALDD data traffic and transferred to SEALDD client over SEALDD-UU. The SEALDD client restores the application data traffic and sends it to VAL client over SEALDD-C. Optionally, VAL deployments may choose to route application signalling traffic and application data traffic for some or all functions it offers using SEALDD service and figure 7.2-4 illustrates the architecture for achieving this. In this case the VAL client and VAL server may choose not to maintain application connection by themselves and transfer all the application traffic over SEALDD connections for those functions. The data storage functionality may be provided by SEALDD server or provided by other storage functions in VAL server, or other cloud platform.

To facilitate the specific optimization for XR application provided by 5G network, the application enablement architecture for the XRApp service is based on the generic functional model specified in 3GPP TS 23.434 [4].

NOTE 1: It is up to the implementation of VAL server about which storage entity (e.g. VAL server, SEALDD server, or other cloud platform) is selected and used.

NOTE 2: SEALDD capabilities are provided as APIs to the VAL Layer, it is up to VAL layer to decide which traffic to be transferred (e.g. application signalling, application data).

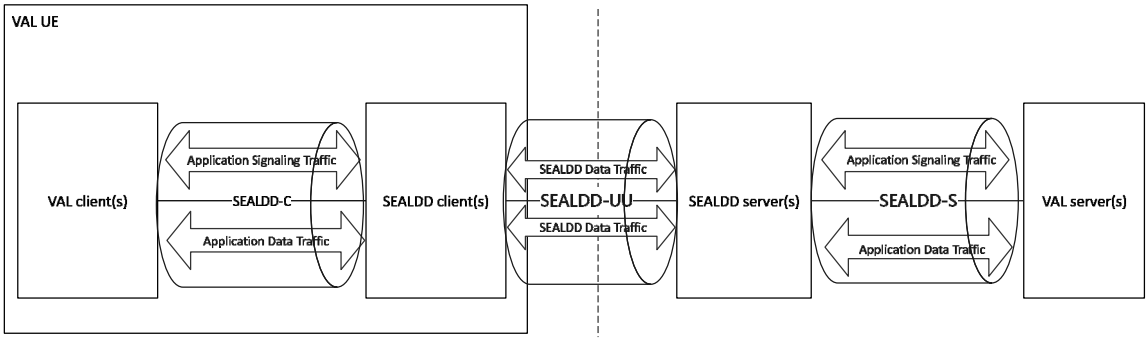

Figure 7.2-4: Architecture for application traffic transfer

The SEAL Data Delivery client interacts with the SEAL data delivery server to establish application layer data transport path.

Through this path, the SEALDD server and client provides data transport service capabilities such as data plane packet processing (e.g. packet duplication, elimination or transport coordination), data forwarding, data caching, background data transfer, etc. to support the VAL server and VAL client. Annex C describes a typical lifecycle of SEALDD to establish the SEALDD connection for the VAL client and VAL server.

Figure 7.2-5 illustrates the architecture for SEAL Data Delivery enabler service used to support UE-to-UE communication.

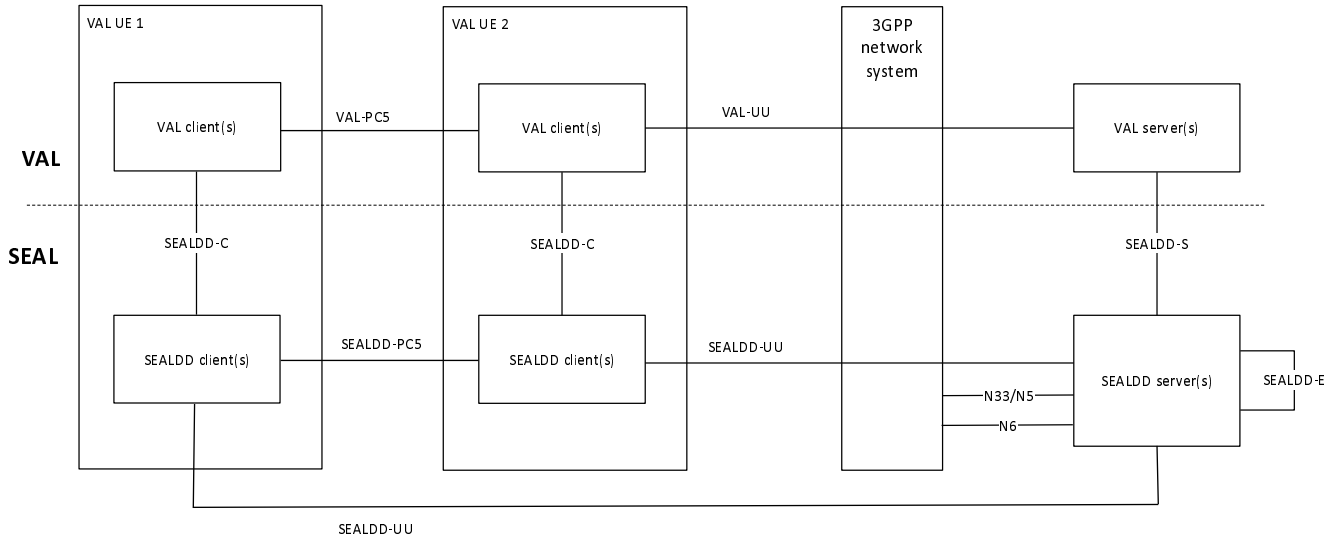

Figure 7.2-5: SEALDD architecture with on-network and off-network

VAL UE 1 and VAL UE 2 have on-network connectivity, and both VAL UEs directly communicate with each other via off-network connectivity (i.e. SEALDD-PC5 reference point) or via on-nework connectivity (i.e. SEALDD-UU reference point).

Multi-modal services are based on several data flows related to each other and subject to application coordination. The data flows transfers different types of data (for example audio, video, positioning, haptic data) and may come from different sources(e.g. a single UE, a single device or multiple devices connected to the single UE, or multiple UEs).

Figure 7.2-6 illustrates XR multi-modal services using two different XR Servers. To support E2E multi-modal communication flows between multiple VAL clients and servers, a SEALDD server and clients may support multi-

modal service capabilities. The SEALDD server and clients perform multi-modal traffic transfer and management processing (e.g., E2E synchronization of application traffic having multi-modal dependencies with one another).

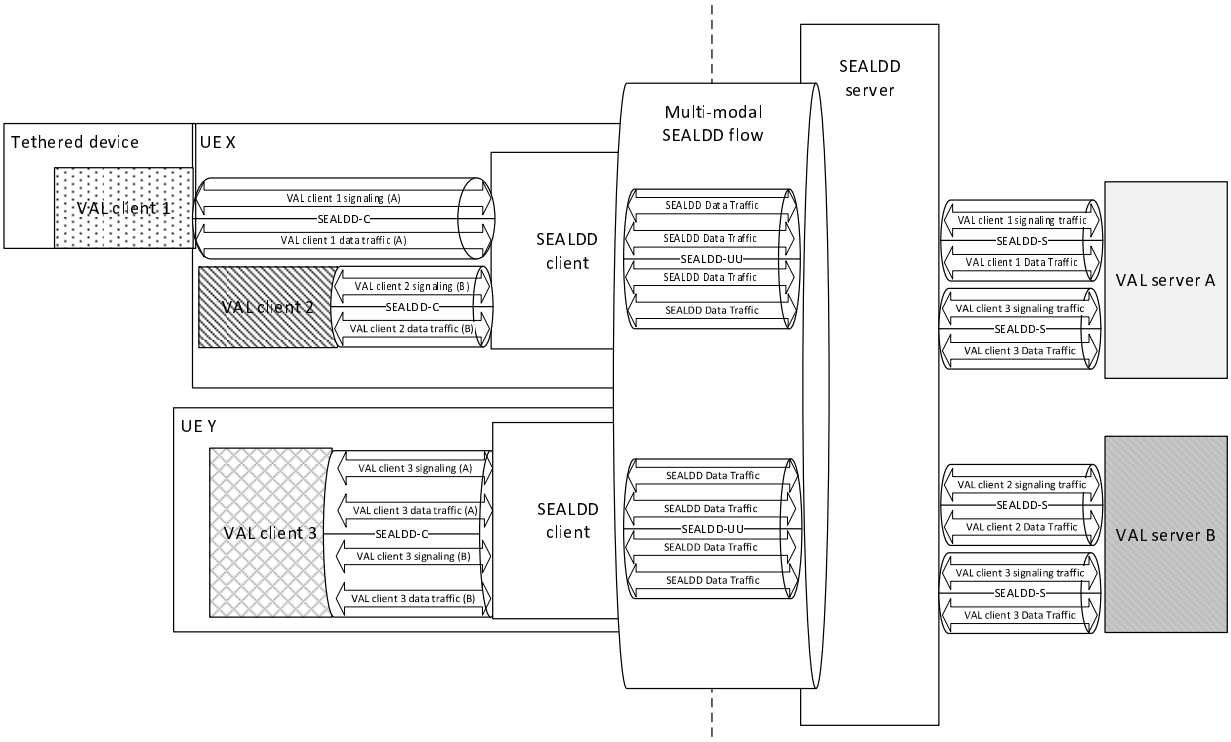

Figure 7.2-6: Architecture for multi-modal application traffic transfer with tethered devices.

To support the Tethered device, there are two types of Application enablement architectures based on SEALDD and PINAPP, corresponding to two types of tethered devices. One is the tethered XR device, where XR application client is deployed on the tethered XR device, i.e., Tethered Standalone AR Glasses, and Tethered AR Glasses with 5G Relay. The other is the Tethered Display XR device, who deploys the XR application on the 5G client, with only the XR runtime residing on the tethered UE.

For the tethered XR device, the application enablement layer architecture is shown in the figure 7.2-7. The SEALDD client on the 3GPP UE, acting as PIN client, could get tethered device information from the PEMC using the PIN-3 interface. Then the SEALDD client could interact with XR client on the tethered device to do the tethered link measurement. The interaction between the SEALDD client and XR client on different device is conducted over SEALDD-C.

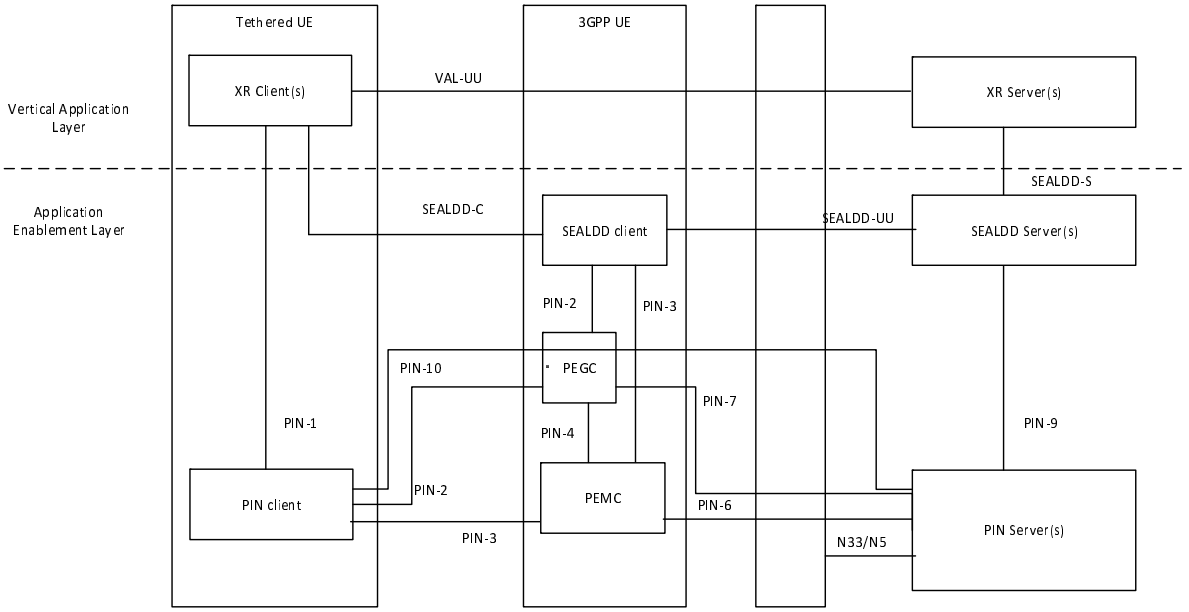

Figure 7.2-7: Application enablement architecture based on SEALDD and PINAPP without SEALDD client in the tethering device

For the Tethered Display XR device, the application enablement layer architecture is shown in the figure 7.2-8. The SEALDD client on the 3GPP UE, acting as PIN client, could get tethered device information from the PEMC using the PIN-3 interface. The SEALDD-UUc interface supports the interaction between the SEALDD client on the tethered UE and SEALDD client on the 3GPP UE.

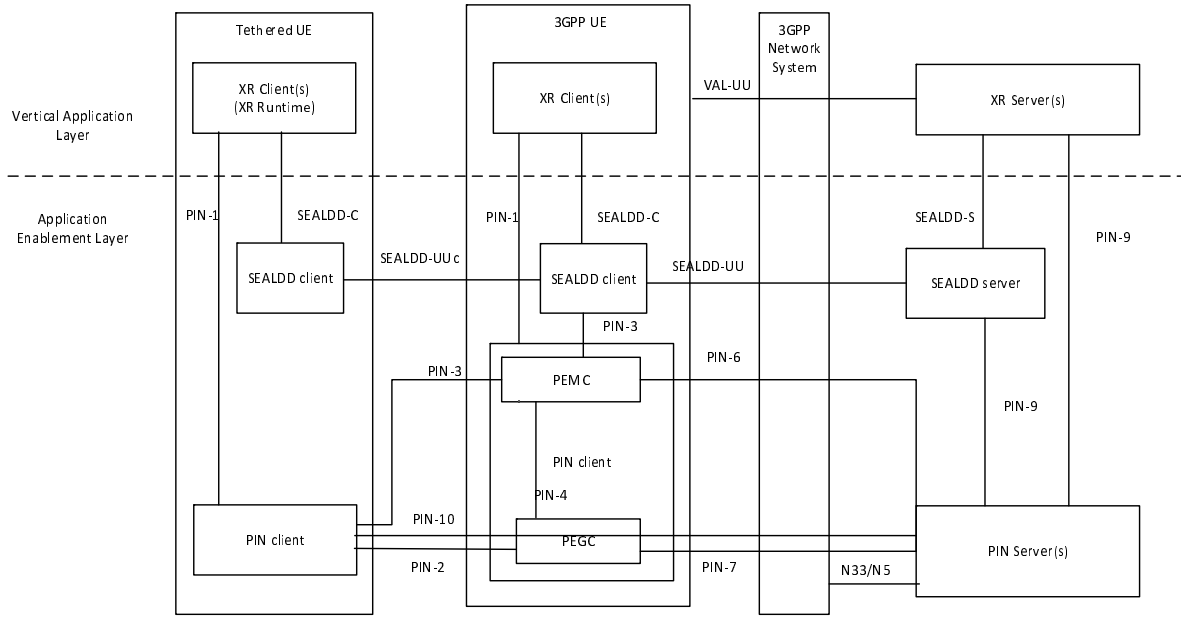

Figure 7.2-8: Application enablement architecture based on SEALDD and PINAPP with SEALDD client in the tethering device

7.3 Functional entities

7.3.1 General

The functional entities for SEALDD service are described in the following clauses.

7.3.2 SEAL Data Delivery server

The SEAL data delivery server functional entity acts as the application server for the data delivery enablement. The SEALDD server supports the following capabilities:

a) Support the signalling interaction with VAL server to negotiate the data delivery aspects including QoS requirement, protocols information, bandwidth settings, delivery policy provisioning, transmission quality measurement, background data transfer.

b) Support the signalling interaction with the SEALDD client to management the data delivery between the SEALDD server and the SEALDD client, including the establish/update/release of signalling plane and user plane of SEALDD-UU, bandwidth control, transmission quality measurement.

c) Providing the application data/media storage.

d) Interacting with 5GC via N33/N5 (i.e. send control plane requirements or receive control plane notification) with usage of capability exposed by 3GPP network.

e) Support user plane handlings including obtaining the application data/media and/or application signalling data from VAL server via SEALDD-S, delivering it to the SEALDD client via the SEALDD-UU, and receiving the application data/media and/or application signalling data from SEALDD client and providing it to the VAL server via SEALDD-S, enforce the rate control.

7.3.3 SEAL Data Delivery client

The SEAL data delivery client functional entity acts as the application client for the data delivery enablement. The SEALDD client supports the following capabilities:

a) Interact with the SEALDD server to management the data delivery between the SEALDD server and the SEALDD client, including the establish/update/release of signalling and user plane of SEALDD-UU, bandwidth control, transmission quality measurement.

b) Support user plane handlings including obtaining the application data/media and/or application signalling data from VAL client, delivering it to the SEALDD server via the SEALDD -UU, and receiving the application data/media and/or application signalling data from SEALDD client, providing it to the VAL server via the SEALDD-S.

7.4 Reference points

7.4.1 General

The reference points for the functional model for SEALDD are described in the following clauses.

7.4.2 SEALDD-UU

SEALDD-UU reference point is between the SEALDD client and the SEALDD server. It supports the user plane functionality of transferring data content and the signalling plane functionality of exchanging information for SEALDD service provisioning, control, reporting etc.

7.4.3 SEALDD-C

Reference point between SEALDD client and VAL client to enable northbound client side API exposed by SEALDD client to VAL client for data delivery and SEALDD service provisioning, control, reporting etc. This reference point should also enables the interaction between the VAL client on the tethered device and SEALDD client on the 3GPP device to support the tethering link management(e.e., measurement etc.).

NOTE: Detailed specification of this reference point is out of scope of this release of this specification.

7.4.4 SEALDD-S

SEALDD-S reference point is between the SEALDD server and the VAL server. It supports the user plane functionality of data content delivery and the signalling plane functionality SEALDD service provisioning, control, reporting etc.

NOTE: The data/content delivery between SEALDD server and VAL server can use the pull mode or push mode over SEALDD-S interface, as specified in clause 9.1.

7.4.5 SEALDD-E

Reference point enables interactions between two SEALDD servers to transfer data content and exchange information for SEALDD service provisioning, control, reporting etc.

7.4.6 N6

Reference point enables interactions between SEALDD server and 5GC to transfer SEALDD traffic packets.

7.4.7 N33/N5

Reference point enables interactions between SEALDD server and 5GC to send control plane requirements or receive control plane notification for optimized data transmission.

7.4.8 SEALDD-UUc

Reference point enables the interactions between the SEALDD client on the tethered device and SEALDD client on the 3GPP device.

7.4.9 SEALDD-PC5

SEALDD-PC5 reference point is between the SEAL clients of two VAL UEs. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [16] or 3GPP TS 23.304 [17]. It supports the user plane functionality of transferring data content and the signalling plane functionality of exchanging information for SEALDD service provisioning, control, reporting etc.

7.4.10 SEALDD-X

Reference point enables interactions between the SEALDD server and other SEAL enablers to exchange information for SEALDD service provisioning, control, reporting etc.

7.5 Cardinality rules

7.5.1 General

The cardinality rules for the SEALDD entities and SEALDD reference points are described in the following clauses.

7.5.2 Functional Entity Cardinality

7.5.2.1 VAL client

The following cardinality rules apply for VAL clients:

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

7.5.2.2 SEALDD client

The following cardinality rules apply for SEALDD clients:

a) One or more SEALDD client(s) may be located in a VAL UE.

7.5.2.3 SEALDD server

The following cardinality rules apply for SEALDD server:

a) One or more SEALDD server(s) may be located in network.

7.5.2.4 VAL server

The following cardinality rules apply for VAL server:

a) One or more VAL server(s) may be located in network.

7.5.3 Reference Point Cardinality

7.5.3.1 SEALDD-C (Between VAL client and SEALDD client)

The following cardinality rules apply for the reference of SEALDD-C:

a) One VAL client may communicate with only one SEALDD client; and

b) One SEALDD client may communicate with one or more VAL client(s) concurrently.

NOTE: Detailed specification of this reference point is out of scope of this release of this specification.

7.5.3.2 SEALDD-S (Between VAL layer and SEALDD server)

The following cardinality rules apply for the reference of SEALDD-S:

a) One VAL server may communicate with one or more SEALDD server; and

b) One SEALDD server may communicate with one or more VAL server(s) concurrently.

7.5.3.3 SEALDD-UU (Between SEALDD client and SEALDD server)

The following cardinality rules apply for the reference of SEALDD-UU:

a) One SEALDD client may communicate with one or more SEALDD servers.

b) One SEALDD server may communicate with one or more SEALDD client(s) concurrently.

7.5.3.4 SEALDD-E (Between SEALDD server and SEALDD server)

The following cardinality rules apply for the reference of SEALDD-E:

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

7.5.3.5 SEALDD-PC5 (Between SEAL clients of two VAL UEs)

The following cardinality rules apply for the reference of SEALDD-PC5:

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

7.5.3.6 SEALDD-X (Between SEALDD server and other SEAL server)

The following cardinality rules apply for the reference of SEALDD-X:

a) One SEALDD server may communicate with one or more SEAL server(s) concurrently.

7.5.3.7 SEALDD-UUc (Between the SEALDD client on the tethered device and SEALDD client on the 3GPP UE)

The following cardinality rules apply for the reference of SEALDD-UUc:

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

8 Identities and commonly used values

8.1 General

The common identities for SEAL refer to 3GPP TS 23.434 [4]. The following clauses list the additional identities and commonly used values for SEALDD.

8.2 SEALDD server ID

The SEALDD server ID uniquely identifies the SEAL data delivery server.

8.3 SEALDD client ID

The SEALDD client ID is a globally unique value that identifies the SEAL data delivery client.

8.4 SEALDD-UU flow ID

The SEALDD-UU flow ID is used by the SEALDD client and SEALDD server to identify different VAL application traffic, which has the same attributes, e.g. the same 5-tuple, media type, QoS requirements. The SEALDD-UU flow ID should be uniquely identified with the SEALDD-UU connection.

8.5 Multi-modal SEALDD flow ID

The multi-modal SEALDD flow ID is used by the SEALDD client and SEALDD server to uniquely identify associated multi-modal VAL application traffic flows per VAL service.

8.6 Multi-modal service ID

The Multi-modal Service ID is an identifier of the multi-modal service as defined in clause 6.1.3.27.3 of 3GPP TS 23.503 [7]. Data flows belonging to the same multi-modal service share the same Multi-modal Service ID.

9 Procedures and information flows

9.1 General

The VAL application data/content is stored in the VAL server, or the SEALDD server, or other cloud platform. For the downlink traffic transmission, the SEALDD server retrieves the data/content of VAL application, by using one of the following modes:

- Downlink pull mode: the SEALDD server pulls the data/content of VAL application from the address provided by the VAL server (i.e. pull from the data/content address in VAL server over SEALDD-S interface, or in other cloud platform).

- Downlink push mode: the VAL server pushes the data/content of VAL application to the SEALDD server over SEALDD-S interface.

For the uplink traffic transmission, the SEALDD server sends the data/content of VAL application to the address provided by the VAL server, by using one of the following modes:

- Uplink pull mode: the VAL server pulls the data/content of VAL application from the SEALDD server over SEALDD-S interface.
- Uplink push mode: the SEALDD server pushes the data/content of VAL application to the address provided by the VAL server (i.e. push to the data/content address in VAL server over SEALDD-S interface, or in other cloud platform).

9.2 SEALDD regular connection management

9.2.1 General

The following clauses specify procedures, information flow and APIs for establishing an SEALDD enabled end-to-end connection between VAL client and VAL server. The end-to-end connection (also termed SEALDD-UU flow) is uniquely identified in the SEALDD layer by the SEALDD-UU flow ID. The specific procedures detailed in the subsequent clauses are for cases in which the SEALDD regular connection is used respectively for application signalling, application data delivery initiated by VAL server, and application data delivery initiated based on DD policy.

NOTE 1: SEALDD server and VAL server may have different behaviour when establishing the connection for signalling transmission and regular data transmission. For signalling transmission, the VAL server may allocate the same address and port to send/receive the signalling traffic of all the users. For data transmission, the VAL server may allocate different addresses and ports to send/receive the data traffic of different users. And SEALDD server may need to identify the data traffic by checking the SEALDD connection establishment request since different SEALDD clients' application data traffic should be mapped to their specific SEALDD-S connection.

NOTE 2: The SEALDD client and the SEALDD server can use the same service operation to request the SEALDD regular transmission connection establishment and it is specified in 3GPP TS 24.543 [26].

9.2.2 Procedure

9.2.2.1 SEALDD enabled signalling transmission connection establishment procedure

Figure 9.2.2.1-1 illustrate the procedure for signalling transmission connection establishment.

Pre-condition:

- The VAL server has discovered and selected the SEALDD server by CAPIF functions.

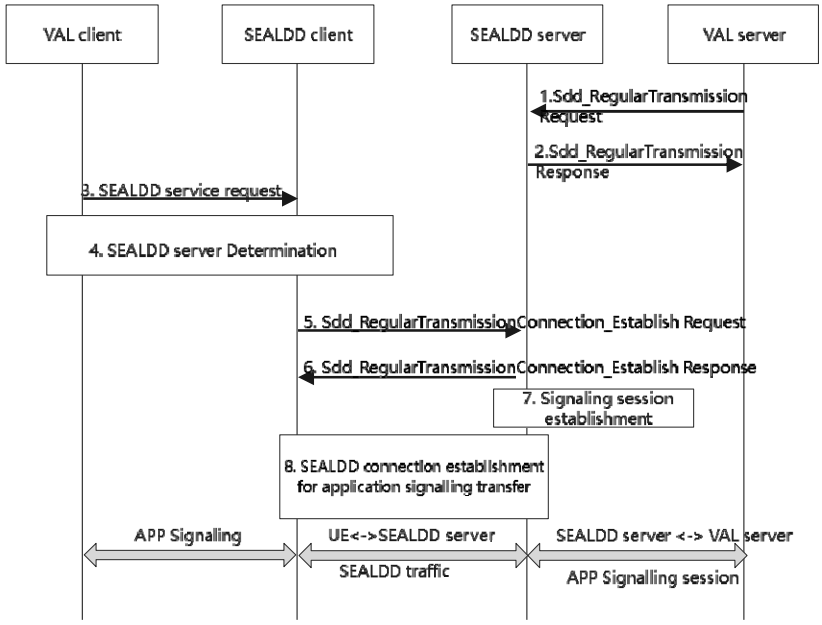

Figure 9.2.2.1-1: SEALDD signalling transmission connection establishment procedure

1. The VAL server decides to use SEALDD service for application signalling transfer and allocates as SEALDD-S connection information for receiving the application signalling traffic from SEALDD server. The VAL server sends Sdd_RegularTransmission request to the SEALDD server. The service request includes the VAL server ID, VAL service ID to identify the VAL application signalling traffic, the SEALDD-S connection information of the VAL server side.

2. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, the SEALDD server allocates a specific address used for SEALDD signalling traffic transfer with the incoming SEALDD client(s) for the VAL server and responds with a SEALDD service response.

NOTE 1: If the SEALDD server does not allocate SEALDD-S connection information in this step, then VAL server uses wildcard endpoint as SEALDD-S connection information for SEALDD-S reference point to receive all the application signalling traffic.

3. The VAL client sends a SEALDD service request to SEALDD client. The service request also indicates to establish application signalling transmission connection. The VAL client receives a SEALDD service response to the SEALDD client. The response indicates that whether the SEALDD service request is successful or not.

4. The VAL/SEALDD client discovers and selects the proper SEALDD server for the VAL application, as described in clause 9.4.3. After this step, the VAL server is discovered and selected along with the associated SEALDD server, and the SEALDD client obtains the SEALDD server's address.

5. The SEALDD client allocates SEALDD-UU flow ID(s) mapping to application signalling traffic for application signalling transmission. The SEALDD client sends Sdd_RegularTransmissionConnection_Establish request to SEALDD server with the SEALDD client ID, the SEALDD-UU flow ID(s), VAL server ID, VAL service ID and the SEALDD traffic descriptor of the SEALDD client side (the SEALDD-S connection information of the SEALDD client for receiving the downlink SEALDD-UU signalling traffic). The request message also contains the selected VAL server endpoint information. The SEALDD server retrieves the location information of the VAL UE or SEALDD client from SEAL LM services defined in 3GPP TS 23.434 [4] clause 9.3.12 and verifies with the Geofence policy configured by the VAL server to allow or restrict the signalling connection establishment. If the location information is allowed as per the configured geofence policy then the SEALDD server allows the signalling connection establishment, otherwise SEALDD server returns failed result e.g. performs connection reject.

NOTE 2: The SEALDD-UU flow ID is used by the SEALDD client and SEALDD server to identify different application signalling traffic, and it is mapped to the VAL service ID.

6. The SEALDD server responds to the SEALDD client with the SEALDD traffic descriptor of SEALDD server side (e.g. SEALDD-S connection information, transport layer protocol) mapping to the application traffic.

7. The SEALDD server stores the SEALDD client ID, SEALDD-UU flow ID(s) to identify the SEALDD-UU signalling traffic and establishes SEALDD-S connection with VAL server for the VAL client to transmit application signalling traffic mapping to the SEALDD traffic. SEALDD server may use different SEALDD connection information to establish the SEALDD-S signalling transmission connection for application signalling transfer towards the VAL server for different SEALDD client and SEALDD-UU flow. Then each VAL client will have different SEALDD-S signalling transmission connection at the SEALDD server side.

8. The SEALDD client uses the SEALDD traffic descriptor of SEALDD server side for SEALDD signalling connection establishment.

NOTE 3: If the UE's address for SEALDD traffic transfer is different from the address used in the control plane interaction (step 5 and 6), another SEALDD interaction procedure may be triggered to notify the SEALDD server about the SEALDD-S connection information used by the SEALDD client for SEALDD traffic transfer. Or the SEALDD server reuses the SEALDD client's address used in step 5 for SEALDD traffic transfer.

After this step, the SEALDD client and SEALDD server both get the whole SEALDD traffic descriptor (including the SEALDD client's address and SEALDD server's address for the SEALDD traffic transmission). The SEALDD client gets the mapping information (i.e. SEALDD-UU flow ID for the application signalling transfer). The SEALDD server gets the mapping information between the SEALDD-UU flow ID, the signalling transmission Session ID and the SEALDD-S connection. The SEALDD client and SEALDD server store the mapping between the application traffic and SEALDD traffic.

Upon receiving application signalling traffic from VAL client, the SEALDD client maps it into SEALDD traffic with SEALDD traffic descriptor as negotiated with SEALDD server. The SEALDD server maps the SEALDD traffic to the application traffic according to the stored SEALDD traffic descriptor, SEALDD client ID, SEALDD-UU flow ID. The SEALDD server sends the received application traffic to VAL server via the connection established in step 7 according to the mapping relationship between the SEALDD-S connection and the SEALDD traffic.

For the downlink application signalling traffic in response to the uplink application signalling, the VAL server responds to the source address (SEALDD-S address of the SEALDD server side) of the uplink signalling traffic. Upon receiving the downlink application signalling traffic from the SEALDD-S connection, the SEALDD server maps the downlink application signalling traffic to the related SEALDD client ID and SEALDD-UU flow ID and send the mapped SEALDD traffic to the SEALDD client. The rest of the downlink application traffic transfer is processed similarly with the uplink traffic.

After the connection establishment, the VAL server communicates with VAL client for application layer signalling traffic transfer via the established SEALDD connection.

9.2.2.2 SEALDD enabled regular data transmission connection establishment procedure

Figure 9.2.2.2-1 illustrate the procedure for establishing regular SEALDD data transmission connection.

Pre-condition:

- The VAL server has discovered and selected the SEALDD server by CAPIF functions.

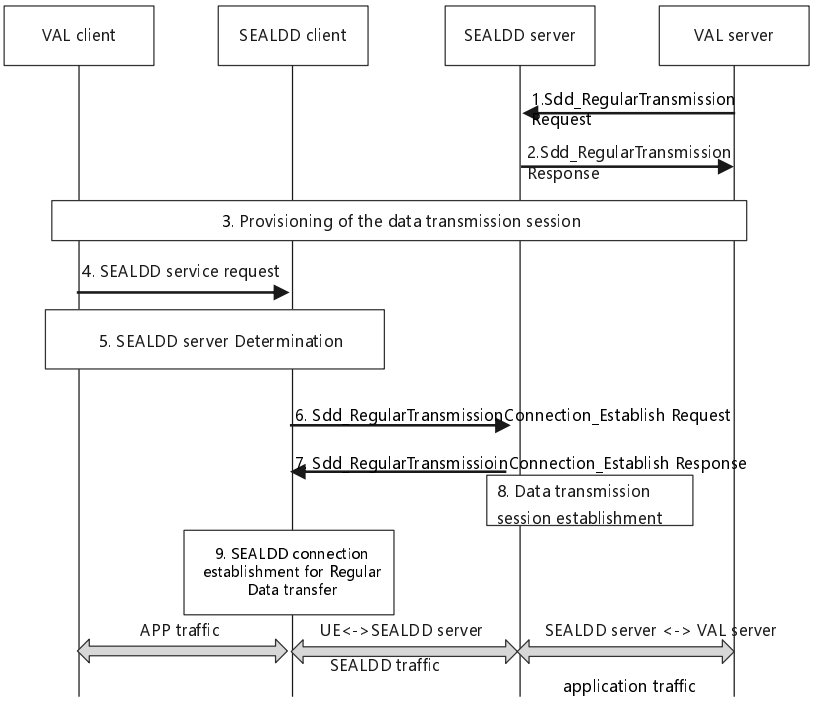

Figure 9.2.2.2-1: SEALDD enabled regular data transmission connection establishment procedure

1. The VAL server decides to use SEALDD service for application data traffic transfer and allocates address as SEALDD-S connection information for receiving the traffic packets from SEALDD server. The VAL server sends Sdd_RegularTransmission request to the SEALDD server discovered by CAPIF. The request includes UE ID/address, VAL server ID, VAL service ID, SEALDD-S connection information of the VAL server side, and optionally, the QoS information for the application traffic, e.g. QoS requirements.

2. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, SEALDD server allocates SEALDD-S connection information of the SEALDD server to receive the application data traffic from the VAL server for application data transfer as SEALDD-S connection information of the SEALDD server side. The SEALDD server allocates a specific SEALDD-S connection information used for SEALDD traffic transfer with the specific UE for the VAL server and responds with a SEALDD service response (including SEALDD-S connection information of the SEALDD server side). The VAL server and SEALDD server use SEALDD-S connection information to establish the data transmission connection between VAL server and SEALDD server for application data transfer.

   The SEALDD server may send the AF request to provide the required QoS information to 5GC via N33/N5, as defined in clause 5.2.6.9 and in clause 5.2.5.3 of 3GPP TS 23.502 [6]. The AF request includes the application traffic descriptor containing the SEALDD-S connection information allocated by SEALDD server, and the QoS information for application traffic. The QoS information may be determined by SEALDD server according to VAL service ID for different service type of application traffic if the QoS information is not provided by VAL server. The SEALDD server relies on the northbound Policy Authorization Service API exposed by the PCF as specified in 3GPP TS 23.502 [6] and 3GPP TS 23.503 [7], if the SEALDD server is connected to the PCF via the N5 reference point, or the northbound AF Session with QoS Service APIs and/or the PFD Management northbound APIs exposed by the NEF as specified in 3GPP TS 23.502 [6] and 3GPP TS 23.503 [7], if the SEALDD server is connected to the PCF via NEF. SEALDD may also rely upon the EES Session with QoS API as specified in 3GPP TS 23.558 [10] and/or the NRM QoS functionality as described in 3GPP TS 23.434 [4].

NOTE 1: The SEALDD-S connection information of the SEALDD server side is optional to respond to the VAL server, if the SEALDD server uses the downlink pull mode to obtain the data/content from the address provided by the VAL server in step 1, and uses the uplink push mode to send the data/content to the address provided by VAL server.

3. Data transmission session information is provisioned to the VAL client by the VAL server via application signalling. The data transmission session information may contain the SEALDD address information which is discovered and selected by VAL server.

NOTE 2: The SEALDD address information for VAL server and SEALDD client is the same.

NOTE 3: The application signalling may be transmitted via direct application layer connection or via the SEALDD layer.

4. The VAL client sends a SEALDD service request to SEALDD client. The VAL client receives a SEALDD service response to the SEALDD client. If the data transmission session information contains the SEALDD address information, then the VAL client sends the selected SEALDD address information to SEALDD client in service request message. The response indicates that whether the SEALDD service request is successful or not.

5. If the data transmission session information does not contain the SEALDD address information, then the VAL/SEALDD client discover and select the proper SEALDD server for the VAL application, as described in clause 9.4.3. After this step, the VAL server is discovered and selected along with the associated SEALDD server, the SEALDD client obtains the SEALDD server's address.

6. The SEALDD client allocates SEALDD-UU flow ID(s) mapping to the identifiers of the application traffic. The SEALDD client sends Sdd_RegularTransmissionConnection_Establish request to SEALDD server with the SEALDD client ID, the SEALDD-UU flow ID(s), the SEALDD traffic descriptor of the SEALDD client side (SEALDD-S connection information of the SEALDD client for receiving the downlink SEALDD traffic), VAL server ID, VAL service ID. The request message also contains the selected VAL server endpoint information and UE ID. The SEALDD server retrieves the location information of the VAL UE or SEALDD client from SEAL LM services defined in 3GPP TS 23.434[4] clause 9.3.12 and verifies with the Geofence policy configured by the VAL server to allow or restrict the data connection establishment. If the location information is allowed as per the configured geofence policy then the SEALDD server allows the data connection establishment, otherwise SEALDD server returns a failed result e.g. performs connection reject.

NOTE 4: The SEALDD server can use or update the association between SEALDD-UU connection and SEALDD-S connection that associated with UE ID, VAL service ID, VAL server endpoint, which is used to correlate the SEALDD traffic and the VAL application traffic.

NOTE 5: The SEALDD-UU flow ID is used by the SEALDD client and SEALDD server to identify different VAL application traffic of the same SEALDD client. The SEALDD-UU flow ID may be same with the identifiers of the application traffic or new simplified IDs allocated by SEALDD.

7. The SEALDD server responds to the SEALDD client with the SEALDD traffic descriptor of SEALDD server side (e.g. address allocated in step 2, transport layer protocol) mapping to the application data traffic.

8. If the connection between VAL server and SEALDD server is not established in step 2, the SEALDD server establishes connection with VAL server for the VAL client to transmit application data traffic mapping to the SEALDD traffic according to the SEALDD-S information negotiated in step 1-2.

9. The SEALDD client uses the SEALDD traffic descriptor of SEALDD server side for SEALDD connection establishment.

   After this step, the SEALDD client and SEALDD server both get the whole SEALDD traffic descriptor (including the UE's address and SEALDD server's address for the SEALDD traffic transmission).

After the negotiation and establishment of the connections, the SEALDD client gets the mapping information between application data traffic and SEALDD-UU flow ID. The SEALDD server gets the mapping information between the SEALDD-UU flow ID and the SEALDD-S connection. Upon receiving application data traffic from VAL client, the SEALDD maps it to SEALDD traffic with SEALDD traffic descriptors as negotiated with SEALDD server in step 6 and step 7. The SEALDD traffic is sent to the SEALDD server. The SEALDD server maps the SEALDD traffic to the application traffic according to the stored SEALDD traffic descriptor, SEALDD client ID and SEALDD-UU flow ID. The SEALDD server sends the recovered application traffic to the address provided by VAL server in step 1, via the connection established in step 2 or 8 according to the mapping information. The downlink application traffic sent from VAL server to VAL client is processed similarly.

The SEALDD server receives any UE location change notification using SEAL LM services defined in 3GPP TS 23.434 [4] clause 9.3.12, then the SEALDD server performs the data delivery in alignment with the geofence policy. If the UE is in the forbidden location or not allowed for the given VAL service to send/receive data as per the Geofence policy, then the SEALDD server performs action like releases the connection and informs the VAL server that UE is not reachable because in a forbidden location using connection event status procedure. If UE enters the allowed location area then the SEALDD server initiates the connection establishment using the procedure defined in clause 9.2.2.3.

9.2.2.3 SEALDD enabled regular data transmission connection establishment based on policy

The SEALDD servers has Data Delivery (DD) policy being provisioned. Before the application communication between VAL client and VAL server starts, the DD policy is enforced by the SEALDD server to establish the SEALDD connection.

Pre-conditions:

1. The SEALDD server has DD policies available.

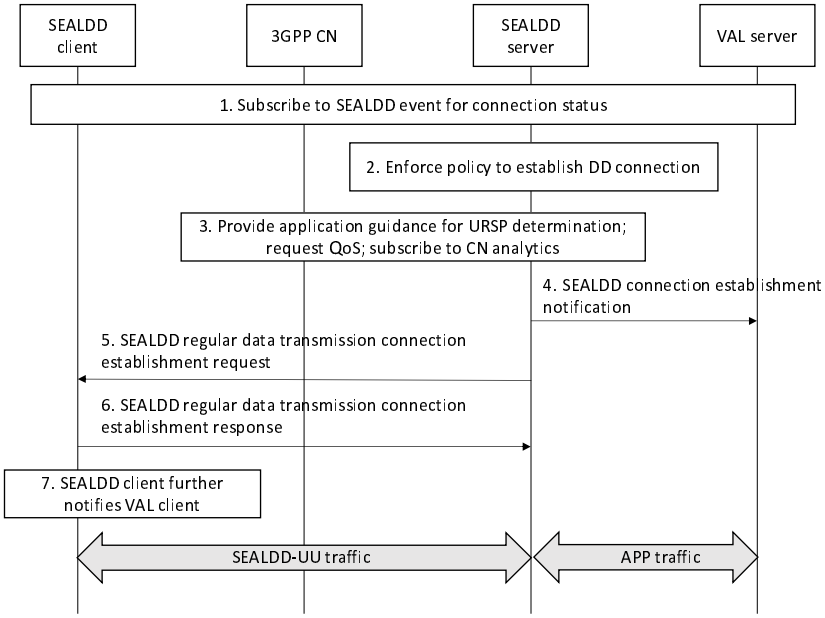

Figure 9.2.2.3-1: Policy enforced by SEALDD server for connectivity

1. The VAL server subscribes to SEALDD event exposure for connection status using the procedure defined in clause 9.2.2.6.

NOTE 1: The VAL server can update/delete an existing subscription at the SEALDD Server when required.

2. When the time for data transmission is about to start, the SEALDD server enforces the policy to trigger regular data transmission connection establishment. If spatial condition for UE is provided, the SEALDD server also ensures the UE's location requirement is satisfied when establishing regular data transmission connection (e.g. by using NEF service for monitoring UE location or SEAL location service for UE entering area of interest).

3. If there is a special routing requirement for SEALDD user plane traffic (e.g. running on a specific slice and DNN), the SEALDD server interacts with 3GPP CN to provision service specific parameters with NEF as described in 3GPP TS 23.502 [6], clause 4.15.6.10 and clause 4.15.6.7.

   If there are QoS requirements in the DD policy, the SEALDD server also applies QoS to ensure the quality for SEALDD traffic by utilizing NEF/PCF/NRM/EES service for QoS adjustment. Specifically, the SEALDD server relies on the northbound Policy Authorization Service API exposed by the PCF as specified in 3GPP TS 23.502 [6] and 3GPP TS 23.503 [7], if the SEALDD server is connected to the PCF via the N5 reference point, or the northbound AF Session with QoS Service API and/or the PFD Management northbound APIs exposed by the NEF as specified in 3GPP TS 23.502 [6] and 3GPP TS 23.503 [7], if the SEALDD server is connected to the PCF via NEF. SEALDD may also rely upon the EES Session with QoS API as specified in 3GPP TS 23.558 [10] and/or the NRM QoS functionality as described in 3GPP TS 23.434 [4].

   If the DD policy specifies failure detection report, the SEALDD server may subscribe to CN analytics (e.g. DN performance analytics) from NEF/NWDAF and further notify data delivery status of application traffic to VAL client (via SEALDD client) and VAL server based on analytics result.

4. The SEALDD server allocates an IP address and port for sending and receiving packet over SEALDD-S reference point, then SEALDD server sends SEALDD connection establishment notification (i.e. SEALDD connection status notification with establishment event, as described in Table 9.2.3.9-1) to the VAL server with VAL service ID, the address.

5-6. The SEALDD server allocates a SEALDD-S connection information for sending and receiving packet over SEALDD-UU reference point, then SEALDD server sends SEALDD regular data transmission connection establishment request to the SEALDD client with SEALDD-UU flow ID, VAL service ID, the address. The request is responded by the SEALDD client. UE IP address may be included by the SEALDD client in the response or sent in a separate update message by SEALDD client if a different UE IP address is to be used in SEALDD connection user plane.

NOTE 2: Step 4 and step 5 can be done in parallel.

NOTE 3: SEALDD server can know the UE address (e.g. via SEALDD connection establishment request initiated by SEALDD client, but rejected by SEALDD server due to policy condition not met) before step 5, if not, step 5 can be sent via application triggering.

7. The SEALDD client further notifies the VAL client about the SEALDD connection being established.

Upon receiving application traffic from VAL client (not shown in the figure), the SEALDD client sends it to SEALDD server in SEALDD traffic. The SEALDD server identifies application traffic based on the VAL service ID and further sends the application traffic to VAL server. The downlink application traffic sent from VAL server to VAL client is processed similarly.

9.2.2.4 SEALDD enabled regular data transmission connection deletion based on policy

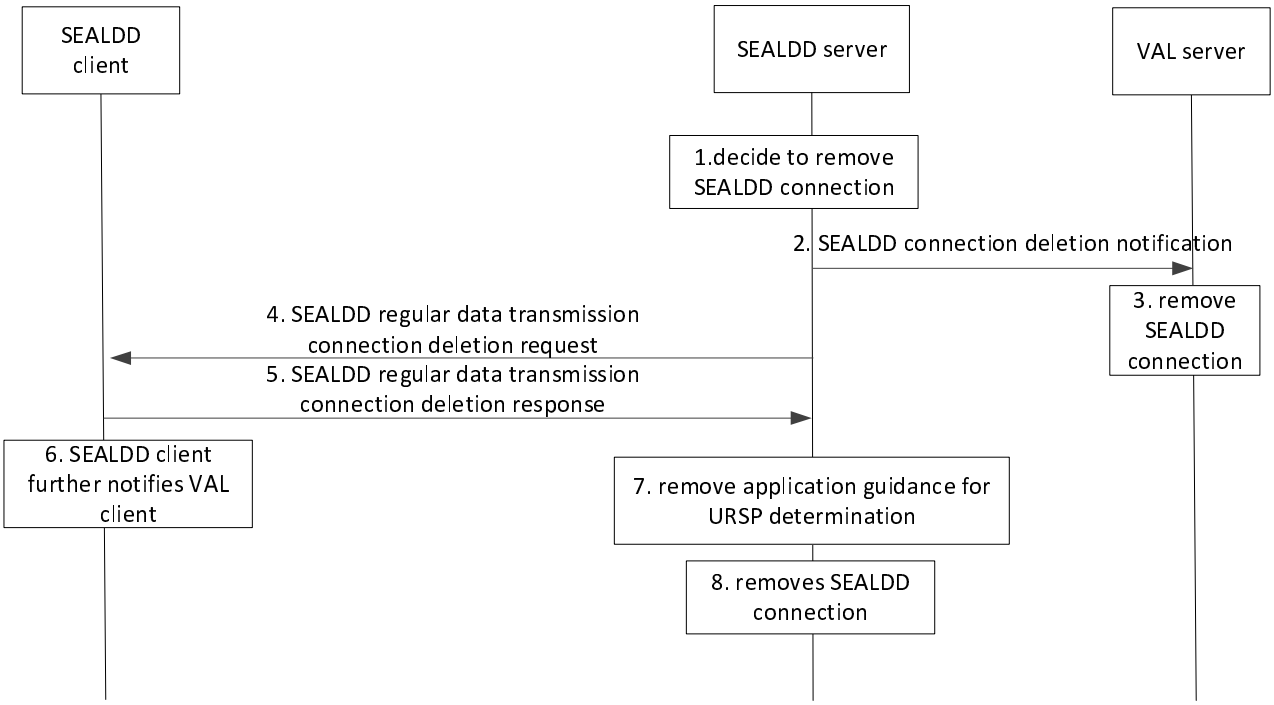

Figure 9.2.2.4-1: SEALDD enabled regular data transmission connection deletion

1. SEALDD server decides to remove the connection. Such a decision may be based on decision in SEALDD server in the following cases:

   a. DD policy removal or validity time expiration;

   b. DD policy specified end time reached for SEALDD communication;

   c. UE is leaving the area of interest (if spatial condition for UE is provided in the policy).

2-3. The SEALDD server notifies SEALDD connection deletion (i.e. SEALDD connection status notification with release event, as described in Table 9.2.3.9-1) to the VAL server. The VAL server removes the connection information. The application traffic is stopped on both sides.

4-5. The SEALDD server requests regular data transmission connection deletion to the SEALDD client. The request is responded by the SEALDD client. The application traffic is stopped on both sides.

NOTE 1: Step 2 and step 4 can be done in parallel.

NOTE 2: Step 5 can be sent via PDU session (if exist) or via application triggering (if no PDU session exists).

6. The SEALDD client further notifies the VAL client about the SEALDD connection being removed. The application traffic is stopped on both sides.

7. If a special routing requirement for SEALDD user plane traffic was provided to 3GPP CN, the SEALDD server interacts with 3GPP CN to remove service specific parameters with NEF as described in 3GPP TS 23.502 [6], clause 4.15.6.7.

8. The SEALDD server removes the SEALDD connection (i.e. deletes the SEALDD connection context).

9.2.2.5 SEALDD client initiated connection release

Figure 9.2.2.5-1 illustrates the procedure for SEALDD client initiated connection release procedure from the SEALDD client to the SEALDD server.

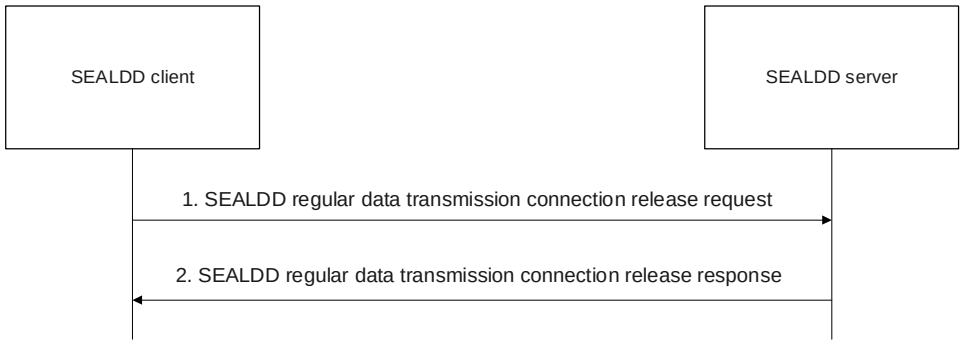

Figure 9.2.2.5-1: SEALDD client initiated connection release

1. The SEALDD client sends the SEALDD connection release request to the SEALDD server to release the established connection.

2. The SEALDD server releases the SEALDD-UU data transmission connection (which was established by SEALDD client or SEALDD server) and sends the response in the SEALDD connection release response message. Upon receiving the acknowledgement, the SEALDD client releases the connection resources.

9.2.2.6 SEALDD connection status procedure

Figure 9.2.2.6-1 illustrates the procedure for SEALDD connection status from the VAL server to the SEALDD server.

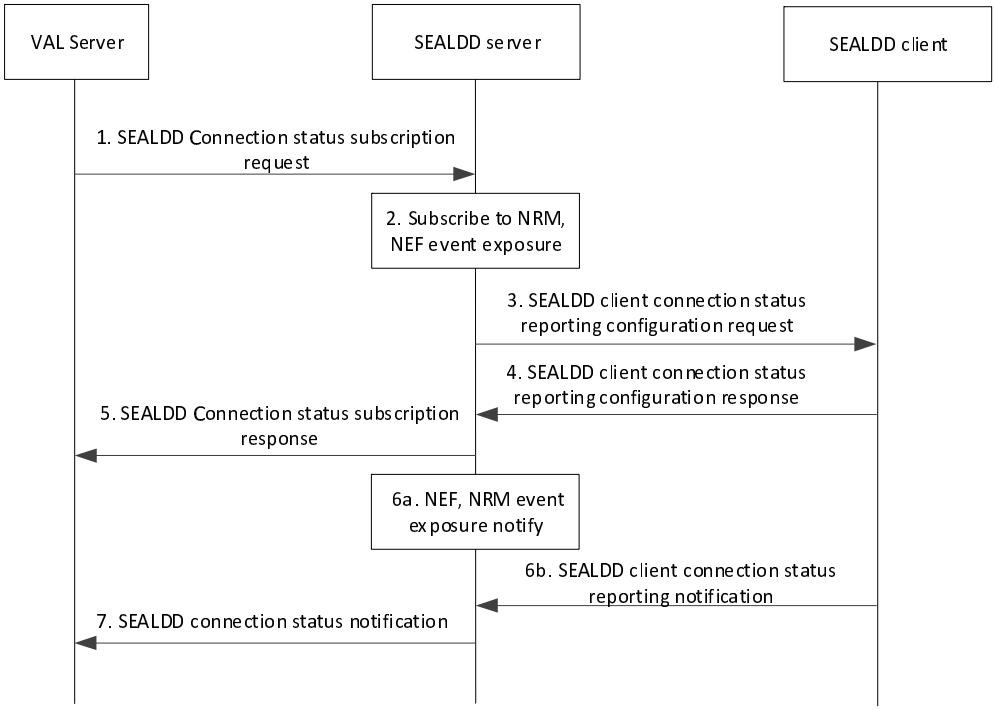

Figure 9.2.2.6-1: SEALDD connection status procedure

1. The VAL server sends the SEALDD connection status subscribe request to the SEALDD server. The request includes the identifiers of the application traffic (e.g. VAL service ID, VAL server ID), VAL UE identity, and the SEALDD client connection status check periodicity under "SEALDD client connection status" event as described in Table 9.2.3.7-1. The VAL server also includes the Non-3GPP access measurement information(like list of WLAN SSIDs, location-based measurement) in the request message.

2. The SEALDD server subscribes to the NEF UE reachability, Application Detection and Loss of connectivity events using the procedure defined in clause 4.15.3.2.3b 3GPP TS 23.502 [6]. It also uses the NRM Event monitoring procedure defined in clause 14.3.6.2.2 3GPP TS 23.434 [4].

3. The SEALDD server also sends a SEALDD client connection status reporting configuration request to the SEALDD client. The request message consists of SEALDD-UU flow ID and method of reporting, which includes the reporting interval when the mode of reporting is periodic, and optionally the SEALDD client connection status reporting priority. The SEALDD-UU flow ID identifies the application traffic flow for which the reporting notification is configured. The SEALDD client monitors the application using SEALDD-UU flow ID. The method of reporting is defined as periodic or event triggered. The periodic reporting method uses the reporting interval to send the notification. The event triggered reporting method sends the notification if the current connection status is different from the previous connection status or if the application state changes (like crash, close, stop).

   The SEALDD server includes the Non-3GPP access measurement in the SEALDD client connection status reporting configuration request. The SEALDD server uses the Non-3GPP access measurement information received in step 1 or Non-3GPP access measurement information configured in the SEALDD server as policy by VAL server or configured as internal policy.

4. The SEALDD client configures the reporting configuration and provides the response to the SEALDD server. If the Non-3GPP access measurement includes list of WLAN SSIDs, then the SEALDD client performs the signal strength measurement for the requested WLAN SSID. If the request contains location-based measurement, then the SEALDD client measures the signal strength of nearby WLAN SSIDs based on its location. The response also includes the list of WLAN SSIDs and their signal strength measurements.

5. The SEALDD server sends the connection status subscription response to the VAL server.

6a-6b. The SEALDD server receives the notification for the UE connection status from the subscribed NEF, NRM. It may also receive a notification from the SEALDD client regarding the connection status. If the UE is about to enter in power saving mode (e.g., IDLE mode), then the SEALDD client sends the connection status reporting notification with the status as sleeping with sleeping duration to the SEALDD server and suspends the connection status periodic reporting. If the UE exits power saving mode(e.g., CONNECTED mode), then the SEALDD client sends the connection status reporting notification with the status as reachable to the SEALDD server and resumes the connection status periodic reporting.

7. Based on the NRM, NEF event subscription response and SEALDD client connection status reporting notification message with "SEALDD client connection status" event as described in Table 9.2.3.9-1, the SEALDD server processes the responses and sends the SEALDD client connection status of unreachable or sleeping status notification to the VAL server.

NOTE: If the VAL server is not aware of the connection status like VAL UE reachability and may continue sending the application traffic, results in packet losses and degradation of the QoS of the VAL UEs.

9.2.2.7 Client initiated regular data transmission path establishment procedure

Figure 9.2.2.7-1 illustrates the procedure for client initiated regular data transmission establishment for data transfer per application layer transaction.

Pre-conditions:

1. The SEALDD client is authorized to request regular data transmission services on behalf of the VAL client when the VAL client initiates transmission service.

2. The VAL client has discovered the VAL server.

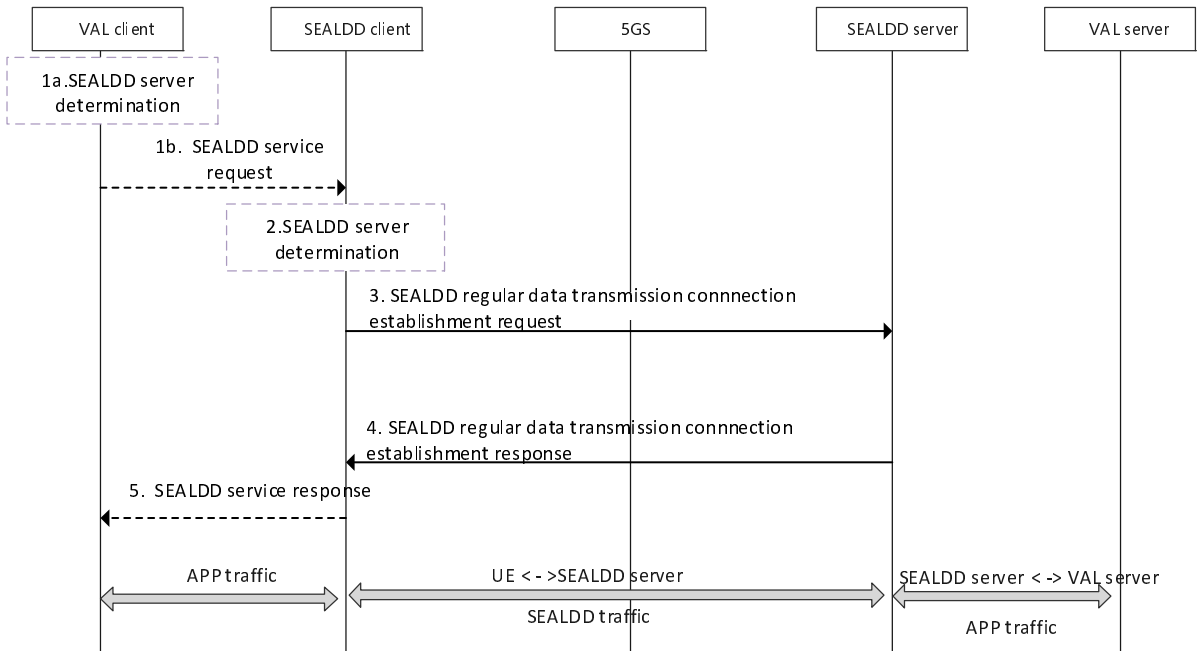

Figure 9.2.2.7-1: Client initiated regular data transmission path establishment

1a. A VAL client may discover and select a proper SEALDD server for the VAL application and VAL server as specified in clause 9.4.3.2.3.

1b. A VAL client determines to use SEALDD service to ensure that the data transmission quality for the application traffic is met and makes a service request to the SEALDD client.

2. Upon receiving the request, the SEALDD client decides to establish regular data transmission path according to the QoS requirements. The SEALDD client discovers and selects the proper SEALDD server for the VAL

application and VAL server as specified in clause 9.4.3.2.3, if the SEALDD server and VAL server information are not received.

3-4. Same as step 6-7 of clause 9.2.2.2.

5. The SEALDD client responds with a SEALDD service response.

NOTE: Details of the VAL client service request in step 1 and the corresponding response in step 5 are out of scope of the current specification.

9.2.3 Information flows

9.2.3.1 SEALDD enabled regular transmission request

Table 9.2.3.1-1 describes the information flow from the VAL server to the SEALDD server for requesting the regular application transmission service.

Table 9.2.3.1-1: SEALDD enabled Regular transmission request

Information element	Status	Description
VAL server ID	M	Identity of the VAL server.
VAL service ID	O	Identity of the VAL service.
Identity	O	Identifier of specific UE or VAL user.
SEALDD-S connection information	M	Address information (e.g., IP address and/or port, URL) of the VAL server to receive the traffic from the SEALDD server.
QoS information	O	QoS information provided by VAL server.
VAL server's total bandwidth limit	O (See NOTE)	The total bandwidth limit of VAL server, including UL/DL.
VAL users' bandwidth limit	O (See NOTE)	The bandwidth limits (i.e. minimum bandwidth requirement and maximum bandwidth limit) for VAL users, including UL/DL.
NOTE: These IEs are used for the SEALDD enabled bandwidth control for different VAL users.		

9.2.3.2 SEALDD enabled regular transmission response

Table 9.2.3.2-1 describes the information flow from the SEALDD server to the VAL server for responding to the regular application transmission.

Table 9.2.3.2-1: SEALDD enabled regular transmission response

Information element	Status	Description
Result	M	Success or failure.
SEALDD-S information connection information	O	Address information (e.g., IP address and/or port, URL) of the SEALDD server to receive the packets from the VAL server for traffic transfer
Cause	O See NOTE	Indicates the reason for the failure, e.g. SEALDD policy mismatch.
NOTE: The IE is only present if the Result is failure.		

9.2.3.3 SEALDD regular transmission connection establishment request (Client to Server)

Table 9.2.3.3-1 describes the information flow from the SEALDD client to the SEALDD server for requesting the regular SEALDD connection establishment.

Table 9.2.3.3-1: SEALDD regular transmission connection establishment request

Information element	Status	Description
Requestor ID	M	Identity of the requestor (SEALDD client).
SEALDD-UU flow ID	M (See NOTE 1)	Identity of the SEALDD-UU flow.
VAL server ID	O	Identity of the VAL server, applicable for SEALDD client side initiated request.
VAL service ID	O	Identity of the VAL service
Selected VAL server endpoint	M	Endpoint of the selected VAL server
SEALDD traffic descriptor	O	SEALDD traffic descriptor (e.g. address, port, URL, transport layer protocol) of the SEALDD client side used to establish SEALDD connection.
Identity	O	The VAL user ID of the VAL user or VAL UE ID.
Capability for BAT and periodicity adaptation	O (See NOTE 2)	Indicates BAT and periodicity adaptation capability of the SEALDD client side (for client side initiated request) per SEALDD traffic descriptor.
Transmission assistance info	O (See NOTE 2, NOTE 4)	Indicates transmission assistance information for uplink SEALDD traffic of the SEALDD client side (for client side initiated request). It includes BAT, BAT window, periodicity, and periodicity range per SEALDD traffic descriptor.
L4S supporting capability	O (See NOTE 3)	Identifies the L4S support (i.e. ECN identification, L4S feedback and L4S based congestion control) for client side initiated request
VAL UE client access capability	O	Indicates the access technologies supported by VAL UE client. E.g.,3GPP, Non-3GPP(WLAN)
XR Application device capability information	O (See NOTE 5)	Indicates XR Application device capability information (i.e. codec(e.g. H.264), media resolution, media frame rate, media Field Of View(FOV)))

NOTE 1: The SEALDD-UU flow ID is used by the SEALDD client and SEALDD server to identify different application traffic, and it is mapped to the identifiers of the application traffic and data transmission session.
NOTE 2: If provided, BAT window and periodicity range are mutually exclusive with capability for BAT and periodicity adaptation.
NOTE 3: This IE is used for the SEALDD enabled congestion control for VAL applications, as specified in clause 9.8.2.2.
NOTE 4: The periodicity range may only be present together with the periodicity when BAT and BAT window are present. The BAT window may only be present together with the BAT.
NOTE 5: This IE is used for the SEALDD enabled bandwidth control for the XR traffic data delivery.

9.2.3.4 SEALDD regular transmission connection establishment response (Server to Client)

Table 9.2.3.4-1 describes the information flow from the SEALDD server to the SEALDD client server for responding to the regular SEALDD connection establishment.

Table 9.2.3.4-1: SEALDD regular transmission connection establishment response

Information element	Status	Description
Result	M	Indicates the success or failure of establishing the SEALDD connection.
SEALDD traffic descriptor	O	SEALDD traffic descriptor (e.g. address, port, URL, transport layer protocol) of the SEALDD server side (for client side initiated request).
Pending timer	O (See NOTE 1)	The pending timer to trigger the re-connection from SEALDD client when bandwidth limit check is failed.
Suggested traffic transmission bandwidth	O (See NOTE 1)	The suggested traffic transmission bandwidth used by SEALDD client or SEALDD server to perform bandwidth control for VAL users, including UL/DL.
Cause	O (See NOTE 2)	Indicates the reason for the failure, e.g. SEALDD policy mismatch.
NOTE 1: These IEs are used for the SEALDD enabled bandwidth control for different VAL users, applicable for client side initiated request. NOTE 2: This IE is only present if the Result is failure		

9.2.3.5 SEALDD regular data transmission connection release request

Table 9.2.3.5-1 describes the information flow from the SEALDD client to the SEALDD server or from the SEALDD server to the SEALDD client for requesting the SEALDD connection release.

Table 9.2.3.5-1: SEALDD regular data transmission connection release request

Information element	Status	Description
Requestor ID	M	Identity of the requestor (SEALDD client or SEALDD server).
SEALDD-UU flow ID	M	Identifies the SEALDD-UU flow.

9.2.3.6 SEALDD regular data transmission connection release response

Table 9.2.3.6-1 describes the information flow from the SEALDD server to the SEALDD client or from the SEALDD client to the SEALDD server for responding the SEALDD connection release request.

Table 9.2.3.6-1: SEALDD regular data transmission connection release response

Information element	Status	Description
Result	M	Result of the operation.

9.2.3.7 SEALDD connection status subscription request

Table 9.2.3.7-1 describes the information flow from the VAL server to SEALDD server to subscribe to SEALDD connection status information.

Table 9.2.3.7-1: SEALDD connection status subscription request

Information element	Status	Description
VAL server ID	M	Identity of the VAL server
Event ID list	M	Identifies a list of events such as establishment, release, congestion report, SEALDD client connection status.
VAL service ID	O	Identity of the VAL service
Identity	O	Identifier of VAL UE or VAL user.
SEALDD-S connection information	M	Address information (e.g., IP address and/or port, URL) to send/receive the traffic to/from the SEALDD server.
Immediate reporting flag	O	Indicates the immediate reporting of connection status notification
SEALDD client connection status check periodicity	O	Indicates the frequency to perform SEALDD client connection status check
Non-3GPP access measurement information	O	Indicates the Non-3GPP access measurement information like list of WLAN SSIDs, location-based measurement

9.2.3.8 SEALDD connection status subscription response

Table 9.2.3.8-1 describes the information flow from the SEALDD server to VAL server for responding SEALDD connection status subscription request.

Table 9.2.3.8-1: SEALDD connection status subscription response

Information element	Status	Description
Result	M	Success or failure.
Subscription ID	O (NOTE)	Subscription identifier corresponding to the subscription.
Expiration time	O (NOTE)	Indicates the expiration time of the subscription.
NOTE: These IEs shall be present when the result is success.		

9.2.3.9 SEALDD connection status notification

Table 9.2.3.9-1 describes the information flow from the SEALDD server to the VAL server to notify SEALDD connection status.

Table 9.2.3.9-1: SEALDD connection status notification

Information element	Status	Description
Event ID	M	Identifies event such as establishment, release, congestion report, SEALDD client connection status.
Identity	M	Identifier of VAL UE or VAL user.
VAL service ID	M	Identity of the VAL service.
SEALDD connection establishment data	O (see NOTE 1)	Data related to SEALDD connection establishment.
> SEALDD-S connection information	M	Address information (e.g., IP address and/or port, URL of the SEALDD server to send/receive the traffic to/from the VAL server.
> SEALDD communication lifetime	O	Identifies the DD communication lifetime.
Congestion level	O (See NOTE 2)	The congestion level of the VAL service
SEALDD client connection status	O (see NOTE 3)	Indicates the connection status of VAL UE/user e.g. reachable, unreachable, sleeping
NOTE 1: This IE is used for the establishment event. NOTE 2: This IE is used for the congestion report event. NOTE 3: This IE is used for the SEALDD client connection status event.		

9.2.3.10 SEALDD client connection status reporting configuration request

Table 9.2.3.10-1 describes the information flow from the SEALDD server to SEALDD client to configure the SEALDD client for connection status reporting.

Table 9.2.3.10-1: SEALDD client connection status reporting configuration request

Information element	Status	Description
SEALDD-UU Flow ID	M	Indicates the SEALDD-UU flow ID of the application for which the reporting is required.
Mode of reporting	O	Indicates the mode of reporting: periodic and/or event triggered. If omitted, the default value is event triggered.
> Reporting interval	O (See NOTE)	Indicates the reporting interval to report the notification.
SEALDD client connection status reporting priority	O	Indicates the priority of the requested SEALDD-UU flow ID for the reporting of the SEALDD client connection status.
Non-3GPP access measurement information	O	Indicates the Non-3GPP access measurement information for the SEALDD client to perform measurement. It contains list of WLAN SSIDs or location-based reporting and signal strengths (e.g., RSSI) values for measurement.
NOTE: This IE shall be present if the mode of reporting is periodic		

9.2.3.11 SEALDD client connection status reporting configuration response

Table 9.2.3.11-1 describes the information flow from the SEALDD client to the SEALD server for sending the SEALDD client connection status reporting configuration response.

Table 9.2.3.11-1: SEALDD client connection status reporting configuration response

Information element	Status	Description
Result	M	Success or failure.

9.2.3.12 SEALDD client connection status reporting notification

Table 9.2.3.12-1 describes the information flow from the SEALDD client to the SEALD server for sending the SEALDD client connection status reporting configuration response.

Table 9.2.3.12-1: SEALDD client connection status reporting notification

Information element	Status	Description
SEALDD client connection status	M	Indicates the status of VAL UEs/users like reachable, unreachable, or sleeping
Non-3GPP access measurement information reporting	O	Indicates the Non-3GPP access measurement information report.
> Measured non-3GPP access	O	List of measured non-3GPP access (e.g., WLAN SSID(s)/BSSID(s) or location information).
>> Signal strength value(s)	M	List of signal strength values (e.g., RSSI) for the measured non-3GPP access.
SEALDD data transmission connection access usage	M	Indicates which access (3GPP or Non-3GPP) is used for the SEALDD-UU data transmission

9.2.3.13 SEALDD connection status subscription update request

Table 9.2.3.13-1 describes the information flow from the VAL server to SEALDD server to update subscription for SEALDD connection status information.

Table 9.2.3.13-1: SEALDD connection status subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Event ID list	O	Identifies a list of events such as establishment, release, congestion report, SEALDD client connection status.
Immediate reporting flag	O	Indicates the immediate reporting of connection status notification
SEALDD client connection status check periodicity	O	Indicates the frequency to perform SEALDD client connection status check

9.2.3.14 SEALDD connection status subscription update response

Table 9.2.3.14-1 describes the information flow from the SEALDD server to VAL server for responding SEALDD connection status subscription update request.

Table 9.2.3.14-1: SEALDD connection status subscription update response

Information element	Status	Description
Result	M	Success or failure.
Expiration time	O (NOTE)	Indicates the expiration time of the subscription.
NOTE: This IE shall be present when the result is success.		

9.2.3.15 SEALDD connection status unsubscribe request

Table 9.2.3.15-1 describes the information flow from the VAL server to SEALDD server to unsubscribe the SEALDD connection status information.

Table 9.2.3.15-1: SEALDD connection status unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated

9.2.3.16 SEALDD connection status unsubscribe response

Table 9.2.3.16-1 describes the information flow from the SEALDD server to VAL server for responding SEALDD connection status unsubscribe request.

Table 9.2.3.16-1: SEALDD connection status unsubscribe response

Information element	Status	Description
Result	M	Success or failure.

9.2.3.17 SEALDD data transmission connection establishment request (Server to Client)

Table 9.2.3.17-1 describes the information flow from the SEALDD server to the SEALDD client for requesting the SEALDD data transmission connection establishment.

Table 9.2.3.17-1: SEALDD data transmission connection establishment request

Information element	Status	Description
Requestor ID	M	Identity of the requestor (SEALDD server).
SEALDD-UU flow ID	M (See NOTE 1)	Identity of the SEALDD-UU flow.
VAL service ID	O	Identity of the VAL service
Selected VAL server endpoint	M	Endpoint of the selected VAL server
SEALDD traffic descriptor	O	SEALDD traffic descriptor (e.g. address, port, URL, transport layer protocol) of the SEALDD server used to establish SEALDD connection.
Identity	O	The VAL user ID of the VAL user or VAL UE ID.
SEALDD communication lifetime	O	Identifies the DD communication lifetime.
NOTE 1: The SEALDD-UU flow ID is used by the SEALDD client and SEALDD server to identify different application traffic, and it is mapped to the identifiers of the application traffic and data transmission session.		

9.2.3.18 SEALDD data transmission connection establishment response (Client to Server)

Table 9.2.3.18-1 describes the information flow from the SEALDD client to the SEALDD server for responding to the SEALDD data transmission connection establishment.

Table 9.2.3.18-1: SEALDD data transmission connection establishment response

Information element	Status	Description
Result	M	Indicates the success or failure of establishing the SEALDD connection.
SEALDD traffic descriptor	O	SEALDD traffic descriptor (e.g. address, port, URL, transport layer protocol) of the SEALDD client side used to establish SEALDD-UU data connection.
Suggested traffic transmission bandwidth	O (See NOTE 1)	The suggested traffic transmission bandwidth used by SEALDD client to perform bandwidth control for VAL users, including UL/DL.
Cause	O (See NOTE 2)	Indicates the reason for the failure, e.g. SEALDD policy mismatch.
Capability for BAT and periodicity adaptation	O (See NOTE 3)	Indicates BAT and periodicity adaptation capability for SEALDD client.
Transmission assistance info	O (See NOTE 3, NOTE 4)	Indicates transmission assistance information for uplink SEALDD traffic of the SEALDD client. It includes BAT, BAT window, periodicity, and periodicity range per SEALDD traffic descriptor.
NOTE 1: These IEs are used for the SEALDD enabled bandwidth control for different VAL users. NOTE 2: This IE is only present if the Result is failure NOTE 3: If provided, BAT window and periodicity range are mutually exclusive with capability for BAT and periodicity adaptation. NOTE 4: The periodicity range may only be present together with the periodicity when BAT and BAT window are present. The BAT window may only be present together with the BAT.		

9.2.4 APIs

9.2.4.1 General

Table 9.2.4.1-1 illustrates the APIs exposed by SEALDD server for regular connection establishment.

Table 9.2.4.1-1: List of SEALDD server APIs for data distribution

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_RegularTransmission	Request	Request/Response	VAL server
Sdd_RegularTransmissionConnection	Establish	Request/Response	SEALDD client, SEALDD server
	Release	Request/Response	SEALDD client, SEALDD server
Sdd_ConnectionStatusEvent	Subscribe	Subscribe/Notify	VAL server
	Notify	Subscribe/Notify	VAL server
	Update	Subscribe/Notify	VAL server
	Unsubscribe	Subscribe/Notify	VAL server

9.2.4.2 Sdd_RegularTransmission operation

API operation name: Sdd_RegularDataTransmission_Request

Description: The consumer requests for one time for SEALDD enabled regular data transmission.

Inputs: See clause 9.2.3.1.

Outputs: See clause 9.2.3.2.

See clause 9.2.2.1 and 9.2.2.2 for details of usage of this operation.

9.2.4.3 Sdd_RegularTransmissionConnection_Establish operation

API operation name: Sdd_RegularTransmissionConnection_Establish

Description: The consumer requests for one time for SEALDD enabled regular data connection establishment.

Inputs: See clause 9.2.3.3. for SEALDD client side initiated operation and clause 9.2.3.17 for server side initiated operation.

Outputs: See clause 9.2.3.4. for SEALDD client side initiated operation and clause 9.2.3.18 for server side initiated operation.

See clause 9.2.2.1, 9.2.2.2 and 9.2.2.3 for details of usage of this operation.

9.2.4.4 Sdd_ConnectionStatusEvent_Subscribe operation

API operation name: Subscribe

Description: The consumer requests to subscribe to SEALDD connection status event.

Inputs: See clause 9.2.3.7.

Outputs: See clause 9.2.3.8.

See clause 9.2.2.6 and clause 9.3.2.3 for details of usage of this operation.

9.2.4.5 Sdd_ConnectionStatusEvent_Notify operation

API operation name: Notify

Description: The consumer is notified with SEALDD connection status.

Inputs: See clause 9.2.3.9.

Outputs: None.

See clause 9.2.2.3, clause 9.2.2.4, clause 9.2.2.6, clause 9.3.2.3 and clause 9.3.2.4 for details of usage of this operation.

9.2.4.6 Sdd_RegularTransmissionConnection_Release operation

API operation name: Sdd_RegularTransmissionConnection_Release

Description: The consumer requests to release the SEALDD connection resources.

Inputs: See clause 9.2.3.5.

Outputs: See clause 9.2.3.6.

See clause 9.2.2.5 for details of usage of this operation.

9.2.4.7 Sdd_ConnectionStatusEvent_Subscribe_Update operation

API operation name: Subscribe update

Description: The consumer requests to update the subscription of SEALDD connection status event.

Inputs: See clause 9.2.3.13.

Outputs: See clause 9.2.3.14.

See clause 9.2.2.3 for details of usage of this operation.

9.2.4.8 Sdd_ConnectionStatusEvent_Unsubscribe operation

API operation name: Unsubscribe

Description: The consumer requests to unsubscribe the subscription of SEALDD connection status event.

Inputs: See clause 9.2.3.15.

Outputs: See clause 9.2.3.16.

See clause 9.2.2.3 for details of usage of this operation.

9.3 SEALDD enabled E2E redundant transmission

9.3.1 General

The following clauses specify procedures, information flow and APIs for SEALDD enabled E2E redundant transmission.

SEALDD client and SEALDD server transfer SEALDD traffic via two redundant PDU sessions as specified in clause 5.33.2.1 of 3GPP TS 23.501 [5].

Figure 9.3.1-1 shows the data traffic flow of E2E redundant transmission. For uplink data delivery, VAL client sends application traffic to SEALDD client, the SEALDD client duplicates the application packets and maps them into two SEALDD traffic. Then the two SEALDD traffic are transferred to SEALDD server via the two redundant PDU sessions shown in figure 9.3.1-1. The SEALDD server eliminates the redundant packets and recovers the application traffic. The recovered application traffic is transferred to VAL server by the SEALDD server. For downlink data delivery, VAL server sends application traffic to SEALDD server, the SEALDD server duplicates the application packets and maps them into two SEALDD traffic. The two SEALDD traffic are transferred to UE via the two redundant PDU sessions. The SEALDD client eliminates the redundant SEALDD packets and recovers the application traffic, then sends the application traffic to the VAL client.

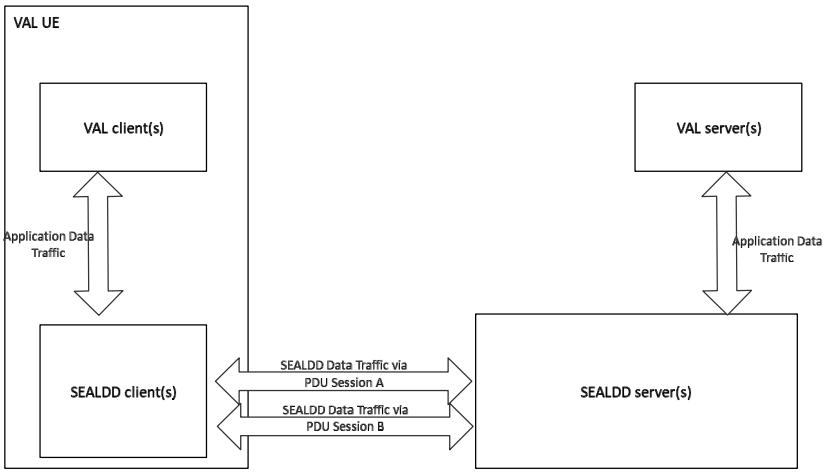

Figure 9.3.1-1: E2E redundant transmission traffic flow

Figure 9.3.1-2 shows the data traffic flow of E2E redundant transmission for multiple VAL servers. In this scenario, SEALDD server and SEALDD client use different SEALDD-UU flow IDs and SEALDD traffic descriptors to identify SEALDD traffic for different VAL servers.

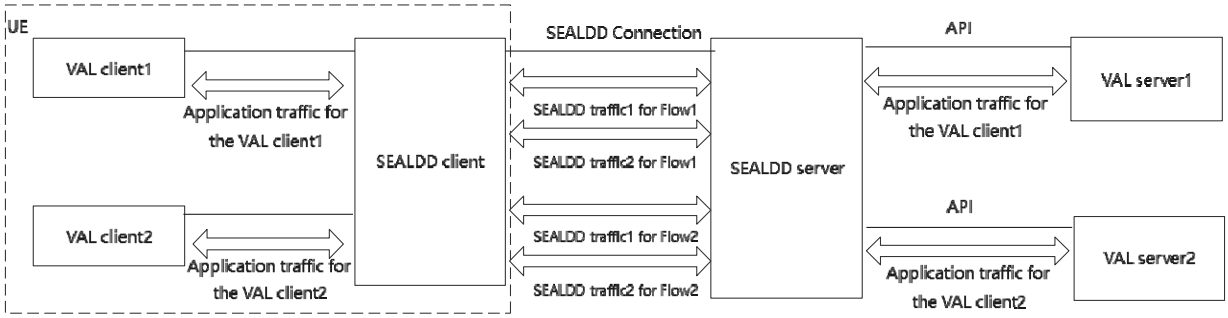

Figure 9.3.1-2: E2E redundant transmission traffic flow for multiple VAL servers

For outbound data delivery, VAL application traffic is sent to SEALDD enabler layer, the SEALDD enabler duplicates the application packets and maps them into two SEALDD traffic (with the different -SEALDD-UU Flow ID with the same SEALDD connection). Then according to the SEALDD traffic descriptors of the SEALDD-UU flow, the SEALDD traffic is sent out with different destination addresses or ports and different source addresses or ports. For inbound data delivery, two SEALDD traffic (with different source addresses or ports and different destination addresses or ports) are received. According to the SEALDD traffic descriptors, SEALDD enabler decides they belong to the same SEALDD-S Flow for the same service. Then after packet elimination and reordering, the two SEALDD traffic is aggregated to one VAL application traffic.

9.3.2 Procedure

9.3.2.1 E2E redundant transmission path establishment procedure

Figure 9.3.2.1-1 illustrates the procedure for redundant transmission establishment. This procedure may be triggered by a VAL server for data transfer per application layer transaction.

Pre-conditions:

1. The VAL server has discovered and selected the SEALDD server by CAPIF functions as specified in clause 9.4.2.

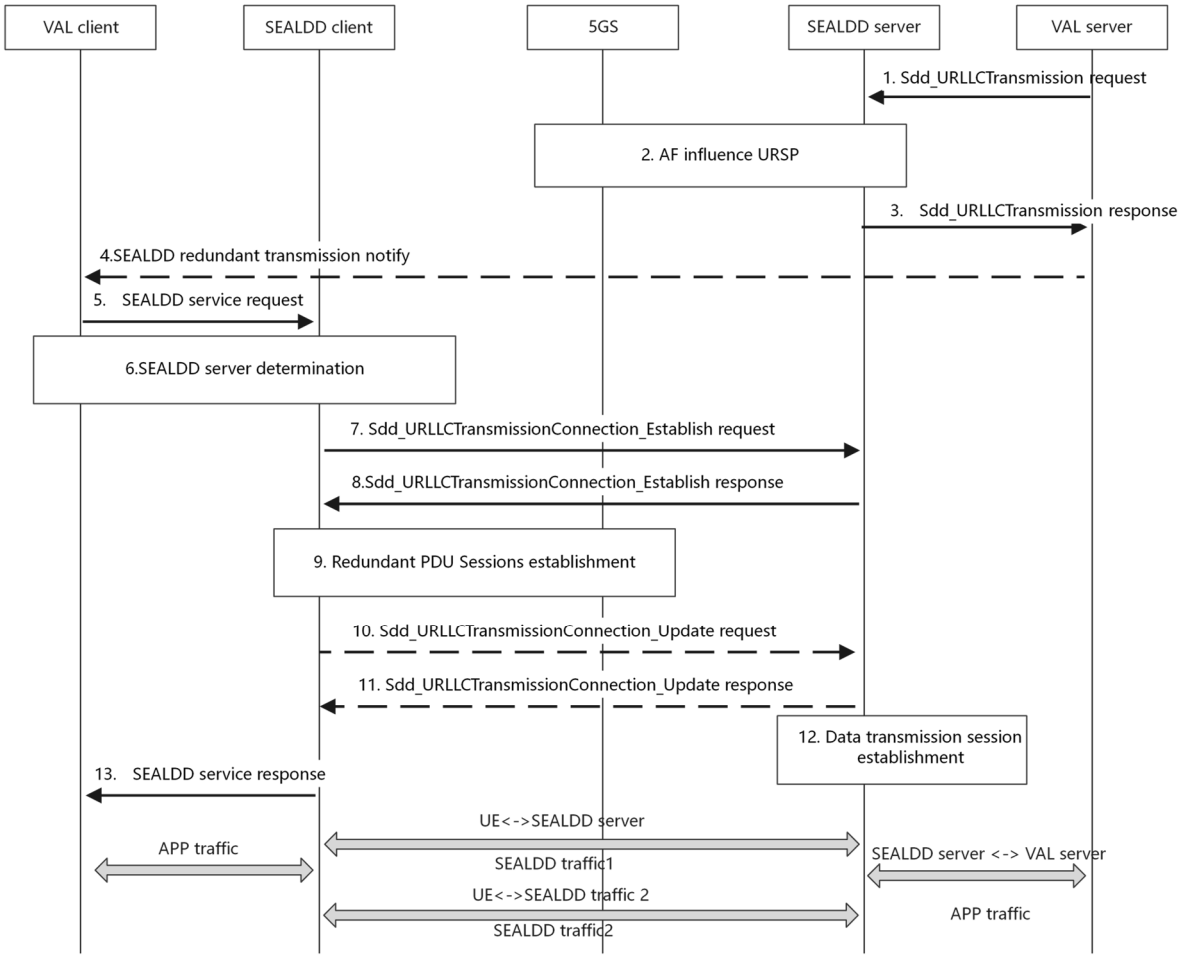

Figure 9.3.2.1-1: E2E redundant transmission path establishment

1. The VAL server decides to use SEALDD service to help ensuring data transmission quality for application traffic transfer and send a Sdd_URLLCTransmission request to the SEALDD server discovered by CAPIF. The request includes UE ID, VAL server ID, VAL service ID, SEALDD-S Data transmission connection information of the VAL server side, and optionally, the QoS information for the application traffic, e.g. QoS requirements. The VAL server ID and VAL service ID are used to identify the VAL application traffic.

2. Upon receiving the request, the SEALDD server decides to establish redundant transmission path. The SEALDD server allocates two different SEALDD-S connection information for the two redundant transmission paths and sends an AF request to 5GS to create or update URSP rules as described in clause 4.15.6.10 of 3GPP TS 23.502 [6] for the UE(s) going to use the redundant transmission service. The AF request includes Identifiers of the UE(s) and application traffic descriptor containing the SEALDD-S connection information allocated by SEALDD server. The SEALDD server may send the AF request to provide the required QoS information to 5GC via N33/N5, as defined in clause 5.2.6.9 and in clause 5.2.5.3 of 3GPP TS 23.502 [6].

3. If the processing of the request was successful, SEALDD server allocates SEALDD-S connection information of the SEALDD server to receive the packets from the VAL server for application data transfer as SEALDD-S data transmission connection information of the SEALDD server side. The SEALDD server responds with a SEALDD service response (including SEALDD-S data transmission connection information of the SEALDD server side) and indicates to the VAL server that redundant transmission service should be activated. The VAL server and SEALDD server uses SEALDD-S data transmission connection information to establish the data transmission connection between VAL server and SEALDD server for application data transfer.

4. If the redundant transmission requirement is not preconfigured or notified to the VAL client, the VAL server may notify the VAL client(s) which is going to use the redundant transmission service through application layer message.

NOTE 1: The application signalling may be transmitted via direct application layer connection or via the SEALDD layer.

NOTE 2: The VAL client can be preconfigured that the VAL service should always be transmitted via redundant transmission. Or this application layer notification may be notified to the UE in another period before the VAL application traffic is really transmitted.

5. The VAL client sends a SEALDD service request to use E2E redundant transmission for the application traffic.

6. The SEALDD client discovers and selects the proper SEALDD server for the VAL application as specified in clause 9.4.3. After this step, the SEALDD client obtains the SEALDD server's address.

7. The SEALDD client allocates two different SEALDD-UU flow IDs mapping to the application traffic. The SEALDD client sends Sdd_URLLCTransmissionConnection_Establish request to SEALDD server. The request includes the SEALDD client ID, SEALDD-UU flow IDs, VAL server ID, VAL service ID for SEALDD server to identify the specific application traffic.

8. Upon receiving the request, the SEALDD server sends SEALDD traffic descriptor for redundant transmission of the SEALDD server side (i.e. SEALDD-S connection information for the redundant transmission paths allocated in step 2 and the transport protocol used for the SEALDD traffic) to SEALDD client.

9. The UE uses the SEALDD traffic descriptor of the SEALDD server and the created or updated URSP rules to trigger two redundant PDU Sessions establishment procedure via 5GS as specified in clause 5.33.2.1 of 3GPP TS 23.501 [5].

10. [Optional] The SEALDD client sends Sdd_URLLCTransmissionConnection_Update request to SEALDD server. The request includes the SEALDD client ID, the SEALDD-UU flow IDs, the SEALDD traffic descriptors for redundant transmission of the SEALDD client side (i.e. UE addresses of the two redundant PDU Sessions). The two redundant SEALDD traffic use the different SEALDD-UU flow IDs with different SEALDD-S connection information for identification.

11. [Optional] The SEALDD server sends a response to SEALDD client. After this step, the SEALDD client and SEALDD server both get the whole SEALDD traffic descriptors (including the UE's addresses and SEALDD server's addresses for the SEALDD traffic transmission). The SEALDD client and SEALDD server store the mapping between the application traffic and SEALDD traffic.

12. [Optional] If the connection between VAL server and SEALDD server is not established in step 3, the SEALDD server establishes connection with VAL server for the VAL client to transmit application traffic mapping to the redundant SEALDD traffic according to the SEALDD-S information negotiated in step 1-3

NOTE 3: Step 10 and Step 11 are optional. If the redundant PDU sessions are already established before step 7, the IP addresses of the UE may be notified to the SEALDD server in step 7. In other cases, after the establishment of the two redundant PDU sessions, the SEALDD client may communicate with SEALDD server through the redundant PDU sessions to let the SEALDD server know the UE's address(es) of the redundant PDU session to fulfil the traffic mapping or the SEALDD client and SEALDD server may use other mapping mechanisms, it is up to the transport protocol used by SEALDD client and SEALDD server for the SEALDD traffic.

13. The SEALDD client responds with a SEALDD service response.

After the negotiation and establishment of the connections, the SEALDD client gets the mapping information between the application traffic and SEALDD-UU flow IDs. The SEALDD server gets the mapping information between the SEALDD-UU flow IDs and the SEALDD-S connection. Upon receiving application traffic from VAL client, the SEALDD client duplicates the application packets and maps them into two SEALDD traffic flows with SEALDD traffic descriptors as negotiated with SEALDD server in step 8 and step 11. The two SEALDD traffic is sent through two redundant PDU sessions to the SEALDD server. The SEALDD server maps the two SEALDD traffic to the same application traffic according to the stored SEALDD traffic descriptors, SEALDD client ID and SEALDD-UU flow IDs. After packet elimination and reordering the SEALDD server sends the aggregated application traffic to VAL server via the connection established in step 3 and step 12 according to the mapping information. The downlink application traffic sent from VAL server to VAL client is processed similarly.

9.3.2.2 Client initiated E2E redundant transmission path establishment procedure

Figure 9.3.2.2-1 illustrates the procedure for client initiated redundant transmission establishment for data transfer per application layer transaction.

Pre-conditions:

1. The SEALDD client is authorized to request redundant transmission services on behalf of the VAL client when the VAL client initiates redundant transmission service.

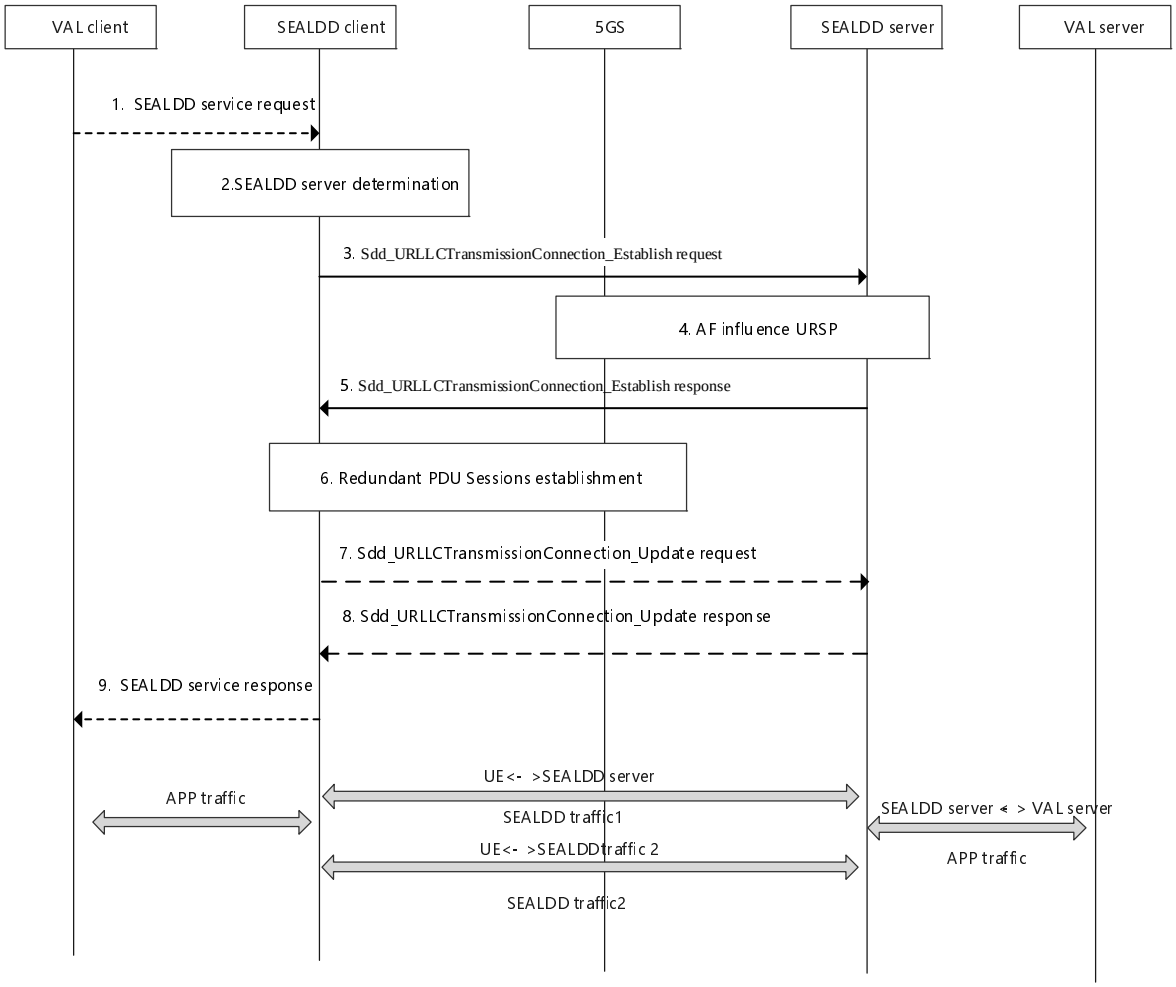

Figure 9.3.2.2-1: Client initiated E2E redundant transmission path establishment

1. A VAL client determines to use SEALDD service to ensure that the data transmission quality for the application traffic is met and makes a service request to the SEALDD client.

2. Upon receiving the request, the SEALDD client decides to establish redundant transmission path according to the QoS requirements. The SEALDD client discovers and selects the proper SEALDD server for the VAL application as specified in clause 9.4.3.

3. The SEALDD client sends a request to the SEALDD server to configure redundant transport for the application traffic. The SEALDD client allocates two different SEALDD-UU flow IDs mapping to the application traffic. The SEALDD client sends Sdd_URLLCTransmissionConnection_Establish request to SEALDD server. The request includes the SEALDD client ID, the SEALDD-UU flow IDs, the application ID, the UE ID/address, the VAL server ID/address, the QoS requirements, the UE location, and a request for redundant transport.

4. The SEALDD server allocates SEALDD-S connection information for the redundant transport paths and initiates the application guidance for URSP determination procedure with the 5G network to create or update URSP rules for the UE, as described in clause 4.15.6.10 of 3GPP TS 23.502 [6]. The request includes the UE ID and

application traffic descriptor containing the addresses allocated by SEALDD server. The UE receives the new or updated URSP rules from the 5G core network.

5. The SEALDD server responds to the SEALDD client providing the configuration status. The response includes the SEALDD-S connection information for the redundant transmission paths allocated in step 4. The SEALDD client and SEALDD server store the mapping between the application traffic and SEALDD traffic.

6. The UE establishes redundant PDU sessions with the 5G network using the new or updated URSP rules as specified in clause 5.33.2.1 of 3GPP TS 23.501 [5].

7. [Optional] The SEALDD client sends Sdd_URLLCTransmissionConnection_Update request to SEALDD server. The request includes the SEALDD client ID, the SEALDD-UU flow IDs, the application traffic descriptors for redundant transmission of the SEALDD client side (i.e. UE addresses and ports of the two redundant PDU Sessions). The two redundant SEALDD traffic use the same SEALDD-UU flow IDs for identification.

8. [Optional] The SEALDD server establishes connection with VAL server for the VAL client to transmit application traffic mapping to the redundant SEALDD traffic. The SEALDD server sends a response to the SEALDD client. After this step, the SEALDD client and SEALDD server both get the application traffic descriptors (including the UE's addresses/ports and SEALDD server's addresses/ports for the SEALDD traffic transmission). The SEALDD client and SEALDD server store the mapping between the application traffic and SEALDD traffic.

9. The SEALDD client responds with a SEALDD service response.

NOTE: Details of the VAL client service request in step 1 and the corresponding response in step 9 are out of scope of the current specification.

The VAL client sends application traffic to the SEALDD client, which duplicates the application data on the redundant PDU sessions. The SEALDD server receives the redundant traffic and reassembles the data to send to the VAL server. Similarly, the SEALDD server duplicates downlink traffic from the VAL server and sends the data to the SEALDD client on the redundant PDU sessions. The SEALDD client eliminates the redundant data and reassembles data to send to the VAL client.

9.3.2.3 SEALDD enabled URLLC transmission connection establishment based on policy

The SEALDD servers has Data Delivery (DD) policy being provisioned. The DD policy includes reliable transmission service for the associated VAL traffic. Before the application communication between VAL client and VAL server starts, the DD policy is enforced by the SEALDD server to establish the SEALDD connection.

Pre-conditions:

1. The SEALDD server has DD policies available.

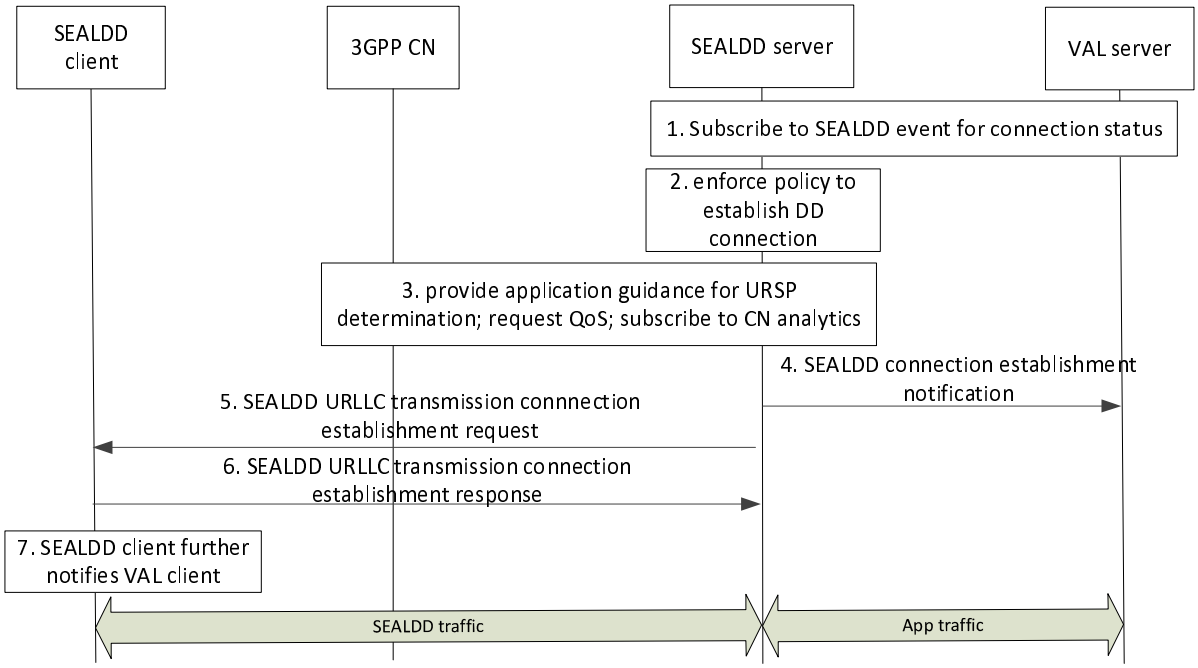

Figure 9.3.2.3-1: Policy enforced by SEALDD server for redundant connectivity

The procedure is same as step 1 to 7 in clause 9.2.2.3 with differences that:

- in step 2, the SEALDD server enforces the policy to trigger URLLC transmission connection establishment.
- in step 5 and 6, the SEALDD server allocates dual SEALDD-S connection information for sending and receiving packet over SEALDD-UU reference point, then SEALDD server sends URLLC transmission connection establishment request to the SEALDD client with SEALDD-UU flow IDs, VAL service ID, the dual IP address and port. The request is responded by the SEALDD client. Dual UE IP address (and port) may be included by the SEALDD client in the response or sent in a separate update message by SEALDD client if a different UE IP address is to be used in SEALDD connection user plane.

9.3.2.4 SEALDD enabled URLLC transmission connection deletion based on policy

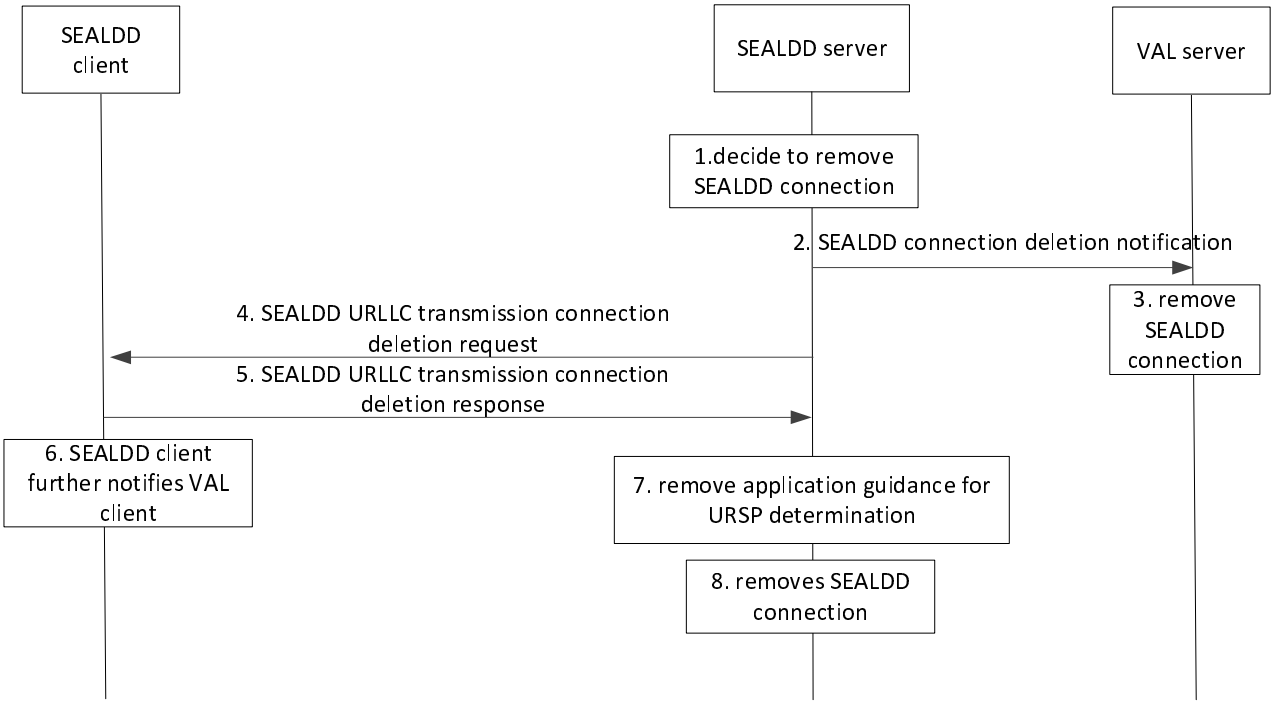

Figure 9.3.2.4-1: SEALDD enabled URLLC transmission connection deletion

The procedure is same as step 1 to 8 in clause 9.2.2.4 with differences that in step 4 to 5, the SEALDD server requests URLLC transmission connection deletion to the SEALDD client and the SEALDD client responds with URLLC transmission connection deletion response.

9.3.2.5 SEALDD client initiated connection release

Figure 9.3.2.5-1 illustrates the procedure for SEALDD client initiated connection release procedure from the SEALDD client to the SEALDD server.

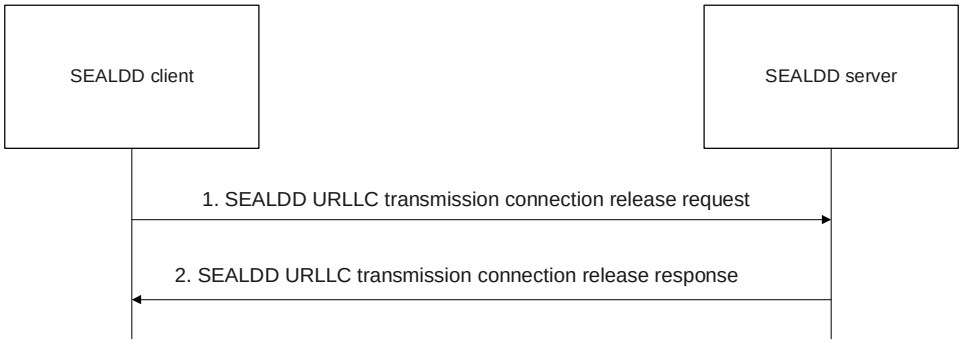

Figure 9.3.2.5-1: SEALDD client initiated connection release

1. The SEALDD client sends the SEALDD URLLC connection release request to the SEALDD server to release the established connection.

2. The SEALDD server releases the SEALDD-UU redundant data transmission connection (which was established by SEALDD client or SEALDD server) and sends the response in the SEALDD URLLC connection release response message. Upon receiving the acknowledgement, the SEALDD client releases the connection resources.

9.3.3 Information flows

9.3.3.1 SEALDD URLLC transmission request

See clause 9.2.3.1 for the details of information flow with the following clarification:

- The bandwidth related IEs are not applicable.

9.3.3.2 SEALDD URLLC transmission response

See clause 9.2.3.2 for the details of information flow.

9.3.3.3 SEALDD URLLC transmission connection establishment request

Table 9.3.3.3-1 describes the information flow from the SEALDD client to the SEALDD server or from the SEALDD server to the SEALDD client for requesting the URLLC transmission connection establishment.

Table 9.3.3.3-1: SEALDD URLLC transmission connection establishment request

Information element	Status	Description
SEALDD client ID	O	Identity of the SEALDD client.
Identity	O	The VAL user ID of the VAL user or VAL UE ID
SEALDD-UU flow IDs	M (See NOTE 1)	Identity of the SEALDD-UU flows.
VAL server ID	O (See NOTE 1)	Identity of the VAL server.
VAL service ID	O (See NOTE 1)	Identity of the VAL service.
SEALDD traffic descriptors	O	A pair of SEALDD traffic descriptors (e.g. address, port, transport layer protocol) of the SEALDD client side (for client side initiated request) or the SEALDD server side (for server side initiated request) used to establish redundant SEALDD connection.
Capability for BAT and periodicity adaptation	O (See NOTE 2)	Indicates BAT and periodicity adaptation capability of the SEALDD client (for client side initiated request). For URLLC transmission, it includes capability for BAT and periodicity adaptation per SEALDD traffic descriptor.
Transmission assistance info	O (See NOTE 2, NOTE 3)	Indicates transmission assistance information for uplink SEALDD traffic of the SEALDD client side (for client side initiated request). It includes BAT, BAT window, periodicity, and periodicity range. For URLLC transmission, it includes assistance information per SEALDD traffic descriptor.
NOTE 1: The SEALDD-UU flow ID is used by the SEALDD client and SEALDD server to identify different application traffic, and it is mapped from the VAL service ID. NOTE 2: If provided, BAT window and periodicity range are mutually exclusive with capability for BAT and periodicity adaptation. NOTE 3: The periodicity range may only be present together with the periodicity when BAT and BAT window are present. The BAT window may only be present together with the BAT.		

9.3.3.4 SEALDD URLLC transmission connection establishment response

Table 9.3.3.4-1 describes the information flow from the SEALDD server to the SEALDD client or from the SEALDD client to the SEALDD server for responding to the URLLC transmission connection establishment.

Table 9.3.3.4-1: SEALDD URLLC transmission connection establishment response

Information element	Status	Description
Result	M	Indicates the success or failure of establishing the SEALDD connection.
SEALDD traffic descriptors	O	A pair of SEALDD traffic descriptors (e.g. address, port, transport layer protocol) of the SEALDD server side (for client side initiated request) or the SEALDD client side (for server side initiated request) used to establish redundant SEALDD connection.
Cause	O (See NOTE 1)	Indicates the reason for the failure, e.g. SEALDD policy mismatch.
Capability for BAT and periodicity adaptation	O (See NOTE 2)	Indicates BAT and periodicity adaptation capability for SEALDD client in server side initiated request. For URLLC transmission, it includes capability for BAT and periodicity adaptation per SEALDD traffic descriptor.
Transmission assistance info	O (See NOTE 2, NOTE 3)	Indicates transmission assistance information for uplink SEALDD traffic of the SEALDD client side (for server side initiated request). It includes BAT, BAT window, periodicity, and periodicity range. For URLLC transmission, it includes assistance information per SEALDD traffic descriptor.
NOTE 1: The IE is only present if the Result is failure. NOTE 2: If provided, BAT window and periodicity range are mutually exclusive with capability for BAT and periodicity adaptation. NOTE 3: The periodicity range may only be present together with the periodicity when BAT and BAT window are present. The BAT window may only be present together with the BAT.		

9.3.3.5 SEALDD URLLC transmission connection update request

Table 9.3.3.5-1 describes the information flow from the SEALDD client to the SEALDD server for requesting the URLLC transmission connection update.

Table 9.3.3.5-1: SEALDD URLLC transmission connection update request

Information element	Status	Description
SEALDD client ID	M	Identity of the SEALDD client.
SEALDD-UU flow IDs	M (See NOTE)	Identity of the SEALDD-UU flows.
VAL server ID	O (See NOTE)	Identity of the VAL server.
VAL service ID	O (See NOTE)	Identity of the VAL service.
SEALDD traffic descriptors	O	A pair of SEALDD traffic descriptors (e.g. address, port, transport layer protocol) of the SEALDD client side used to establish redundant SEALDD connection.
NOTE: The SEALDD-UU flow IDs is used by the SEALDD client and SEALDD server to identify different application traffic, and it is mapped from the VAL service ID.		

9.3.3.6 SEALDD URLLC transmission connection update response

Table 9.3.3.6-1 describes the information flow from the SEALDD server to the SEALDD client for responding to the redundant transmission connection update.

Table 9.3.3.6-1: SEALDD URLLC transmission connection update response

Information element	Status	Description
Result	M	Indicates the success or failure of updating the SEALDD connection.
Cause	O See NOTE	Indicates the reason for the failure, e.g. SEALDD policy mismatch.
NOTE: The IE is only present if the Result is failure		

9.3.3.7 SEALDD URLLC transmission connection release request

See clause 9.2.3.5 for the details of information flow.

9.3.3.8 SEALDD URLLC transmission connection release response

See clause 9.2.3.6 for the details of information flow.

9.3.4 APIs

9.3.4.1 General

Table 9.3.4.1-1 illustrates the APIs exposed by SEALDD server for URLLC transmission.

Table 9.3.4.1-1: List of SEALDD server APIs for redundant transmission

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_URLLCTransmission	Request	Request/Response	VAL server
Sdd_URLLCTransmission Connnection	Establish	Request/Response	SEALDD client, SEALDD server
	Update	Request/Response	SEALDD client, SEALDD server
	Release	Request/Response	SEALDD client, SEALDD server

9.3.4.2 Sdd_URLLCTransmission Request operation

API operation name: Sdd_URLLCTransmission Request

Description: The consumer requests for one time for URLLC transmission service.

Inputs: See clause 9.3.3.1.

Outputs: See clause 9.3.3.2

See clause 9.3.2.1 for details of usage of this operation.

9.3.4.3 Sdd_URLLCTransmissionConnection_Establish operation

API operation name: Sdd_URLLCTransmissionConnection_Establish

Description: The consumer requests for URLLC transmission connection establishment.

Inputs: See clause 9.3.3.3.

Outputs: See clause 9.3.3.4.

See clause 9.3.2.1 for details of usage of this operation.

9.3.4.4 Sdd_URLLCTransmissionConnection_Update operation

API operation name: Sdd_URLLCTransmissionConnection_Update

Description: The consumer requests or URLLC transmission connection update.

Inputs: See clause 9.3.3.5.

Outputs: See clause 9.3.3.6.

See clause 9.3.2.1 for details of usage of this operation.

9.3.4.5 Sdd_URLLCTransmissionConnection_Release operation

API operation name: Sdd_URLLCTransmissionConnection_Release

Description: The consumer requests for URLLC transmission connection release.

Inputs: See clause 9.3.3.7.

Outputs: See clause 9.3.3.8.

See clause 9.3.2.5 for details of usage of this operation.

9.4 SEALDD server discovery and selection

9.4.1 General

The following clauses specify procedures, information flow and APIs for SEALDD server discovery and selection for VAL server and SEALDD client.

There are two scenarios of how SEALDD service is used:

- Scenario (a): SEALDD service is used for both signalling and data traffic transfer.
- Scenario (b): SEALDD service is used only for data traffic transfer.

NOTE: For the same VAL application, VAL servers for Scenario (a) and Scenario (b) and VAL servers without SEALDD service may coexist in the same EDN. The three types of servers may use different EAS IDs or other information (e.g. EAS service, additional associated SEALDD server information) to differentiate each other for EAS discovery.

9.4.2 SEALDD server discovery and selection for VAL server

9.4.2.1 General

CAPIF architecture and functionalities are reused to enable VAL server discover and select SEALDD server.

9.4.2.2 Procedure

The SEALDD server and VAL server may support CAPIF as shown in Figure 9.4.2.2-1. When CAPIF is supported:

- The SEALDD server shall support the CAPIF API provider domain functions (i.e. CAPIF-2/2e (SEALDD-S interface), CAPIF-3/3e, CAPIF-4/4e and CAPIF-5/5e as specified in 3GPP TS 23.222 [3]);
- The VAL server shall act as API invoker and support the API invoker functions (i.e. CAPIF-1/1e and CAPIF-2/2e (SEALDD-S interface) as specified in 3GPP TS 23.222 [3]); and
- The SEALDD server shall act as API invoker and support the API invoker functions (i.e. CAPIF-1/1e and CAPIF-2/2e (SEALDD-E interface) as specified in 3GPP TS 23.222 [3]).

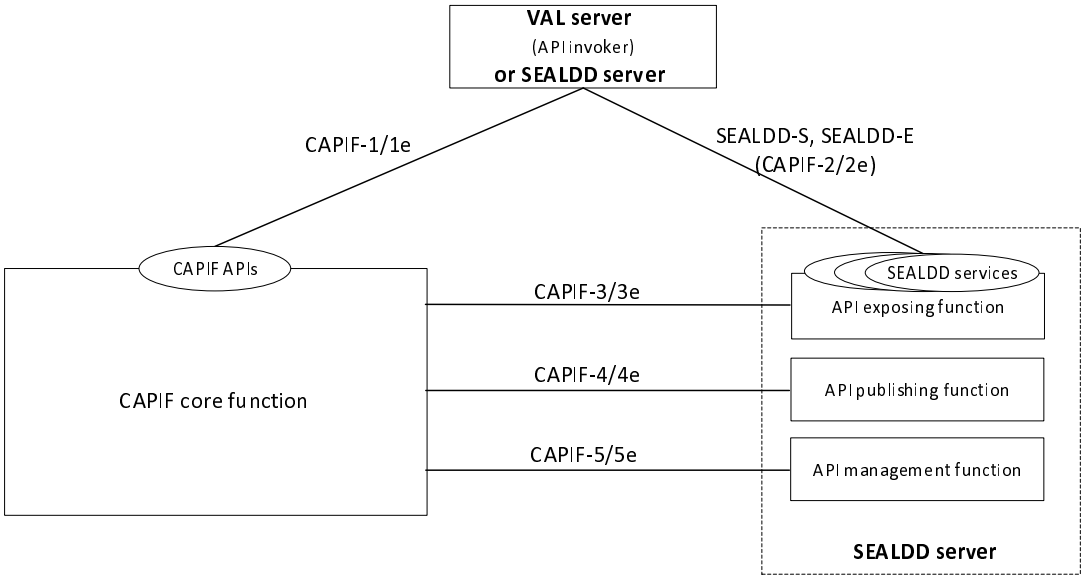

Figure 9.4.2.2-1: SEALDD adaptation in the CAPIF architecture

The VAL server discovers a proper SEALDD server from CAPIF core function with different discovery filters, e.g. expected AEF location. If a VAL server is changed during UE mobility, a new SEALDD server may be discovered and selected.This is also applicable for the VAL server acting as EAS to discover and select an SEALDD server in EDN scenario to use SEALDD-S services, if any.

9.4.3 SEALDD server discovery and selection for SEALDD client

9.4.3.1 General

The VAL client uses existing mechanisms (e.g. DNS query mechanism, application layer signalling mechanism) to find an appropriate SEALDD server in non-EDN scenario and EDN scenario. The VAL client provides the SEALDD server information to the SEALDD client when the SEALDD service is required.

NOTE: DNS query mechanism and application layer signalling mechanism are outside the scope of SA6.

The EAS registration procedure of 3GPP TS 23.558 [10] is enhanced to enable VAL/SEALDD client to discover and select proper SEALDD server in EDN scenario.

9.4.3.2 EDN scenario

9.4.3.2.1 VAL server registered to EES with associated SEALDD server address as VAL server endpoint

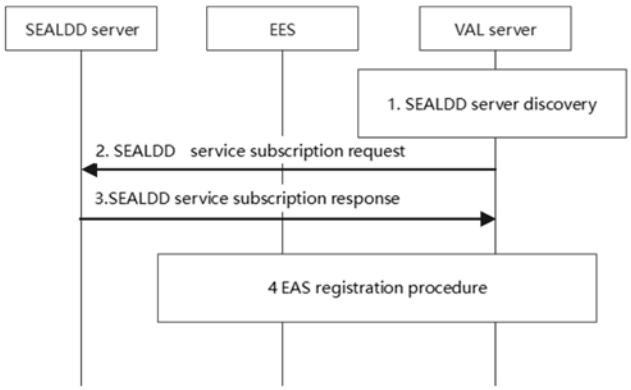

Figure 9.4.3.2.1-1: VAL server registered to EES with associated SEALDD server address as VAL server endpoint

1. The VAL server discovers and selects the SEALDD server (e.g. by CAPIF functions).
2. The VAL server decides to use SEALDD service to enhance data transmission and send a SEALDD data transmission subscription request (e.g. SEALDD enabled regular transmission request in clause 9.2.2) to the SEALDD server.
3. Upon receiving the request, the SEALDD server performs an authorization check and responds with a SEALDD data transmission subscription response (e.g. SEALDD enabled regular transmission response in clause 9.2.2).
4. The VAL server (as an EAS) registers to the EES as described in clause 8.4.3.2.2 of 3GPP TS 23.558 [10] with the associated SEALDD server address as EAS Endpoint in the EAS profile. The EAS ID used by VAL server in registration may indicate the application service association between the VAL service and SEALDD service implicitly or explicitly.

This procedure reuses the current procedure described in clause 8.4.3.2.2 of 3GPP TS 23.558 [10]. The VAL server (as an EAS) registers to the EES with the associated SEALDD server address as the EAS Endpoint in the EAS profile. Then the EEC uses the EAS discovery procedure defined in clause 8.5 of 3GPP TS 23.558 [10] to find the VAL server's address which is SEALDD server's address. The VAL client initiates SEALDD service via SEALDD client with the SEALDD server's address. This procedure is applicable to for scenario (a).

9.4.3.2.2 EAS registered to EES with associated SEALDD server information

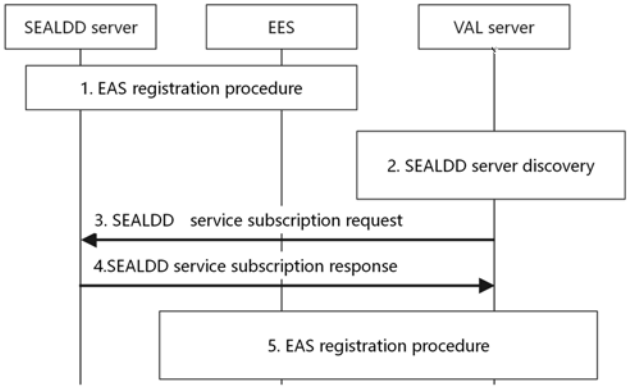

Figure 9.4.3.2.2-1: EAS register to EES with associated SEALDD server information

1. The SEALDD server (as an EAS) registered to EES with SEALDD profile (i.e. EAS profile) as an API provider.
2. The EAS (VAL) server discovers and selects the SEALDD server (e.g. by CAPIF functions).
3. The EAS (VAL server) decides to use SEALDD service to enhance data transmission and send a SEALDD data transmission subscription request (e.g. SEALDD enabled regular transmission request in clause 9.2.2) to the SEALDD server.
4. Upon receiving the request, the SEALDD server performs an authorization check and responds with a SEALDD data transmission subscription response (e.g. SEALDD enabled regular transmission response in clause 9.2.2).
5. The VAL server (as an EAS) registers to the EES as described in clause 8.4.3.2.2 of 3GPP TS 23.558 [10] with the associated SEALDD server information (i.e. SEALDD service and SEALDD server address) as associated EAS ID and EAS Endpoint in the EAS profile.

This procedure reuses the current procedure described in clause 8.4.3.2.2 of 3GPP TS 23.558 [10]. The VAL server (as an EAS) registers to the EES with the associated SEALDD server information (i.e. SEALDD service and SEALDD server address) as associated EAS ID and EAS Endpoint in the EAS profile. Then the EEC uses the EAS discovery procedure defined in clause 8.5 of 3GPP TS 23.558 [10] to find the VAL server's address and associated SEALDD server's address. The VAL client initiates SEALDD service via SEALDD client with the SEALDD server's address. For scenario (b), the VAL client also establishes the connection with VAL server using the VAL server's information for application signalling transfer and only use the SEALDD connection for application data transfer.

9.4.3.2.3 VAL server and SEALDD server registered to EES

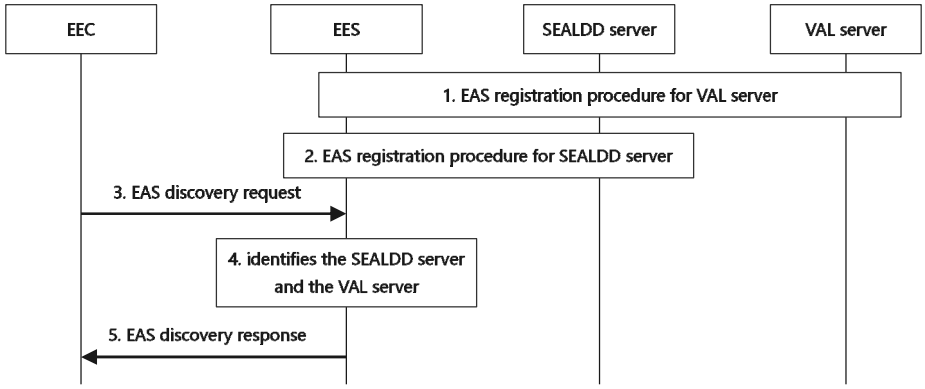

Figure 9.4.3.2.3-1: VAL server and SEALDD server registered to EES

1. The VAL server (acting as an EAS) registers to the EES, if the VAL server has not indicated the associated SEALDD server as described in clause 9.4.3.2.1 or clause 9.4.3.2.2, the VAL server includes an indication of whether using SEALDD service is needed.

2. Optionally, the SEALDD server (acting as an EAS) registers to the EES.

3. The EEC performs service provisioning procedure as described in clause 8.3.3.2.2 of 3GPP TS 23.558 [10]. The EEC is responded with the EES which supports the SEALDD server and the VAL server. The EEC sends the EAS discovery request for EAS bundle including VAL service and SEALDD service. The EES may collect the performance of VAL server and SEALDD server (e.g. E2E latency between the SEALDD server and client and load information of SEALDD and VAL server) from the ADAE server when receiving the EAS discovery request, as specified in clause 8.2.2 (for transmission quality, e.g. E2E latency) and 8.8.2 (for edge load) of 3GPP TS 23.436 [13].

4. The EES identifies the VAL server and the associated SEALDD server based on the performance of VAL server and the performance of SEALDD server (e.g. to satisfy the AC service KPI).

NOTE: In step 4, the EES identifies the VAL server that needs to use SEALDD server, based on the SEALDD service needed indication in step 1.

5. The EES sends the EAS discovery response to EEC, including the SEALDD server address, the VAL server address.

Upon receiving the SEALDD server address, the VAL server address, the VAL client initiates SEALDD service via SEALDD client with the SEALDD server's address. The data transmission between the VAL client and the VAL server is enabled via the SEALDD connection, as specified in clause 9.2.2.

9.4.4 Information flows

The information flow about the SEALDD server discovery for VAL server/SEALDD server reuses the defined information flow in CAPIF (e.g. service API publish in clause 8.3.2, Service API discover in clause 8.7.2), as specified in 3GPP TS 23.222 [3].

For SEALDD server discovery for VAL client in EDN scenario, the information flows for EAS registration and EAS discovery in caluse 8.4.3.3 and clause 8.5.3 of 3GPP TS 23.558 [10].

The information flow about regular SEALDD data transmission subscription refers to the SEALDD enabled regular transmission request/response in clauses 9.2.3.1 and 9.2.3.2.

9.4.5 APIs

The APIs about SEALDD server discovery for VAL server/SEALDD server reuses the defined APIs in CAPIF (e.g. CAPIF_Publish_Service_API in clause 10.3, CAPIF_Discover_Service _API in clause 10.2), as specified in 3GPP TS 23.222 [3].

The APIs about SEALDD server discovery for VAL client in EDN scenario, reuses the defined APIs in EDGEAPP (e.g. Eees_EASRegistration API in clause 8.4.3.4, Eees_EASDiscovery API in clause 8.5.4), as specified in 3GPP TS 23.558 [10].

The APIs about regular SEALDD data transmission subscription refers to the Sdd_RegularTransmission API, as defined in clause 9.2.4.

9.5 SEALDD enabled data storage

9.5.1 General

The following clauses specify procedures, information flows and APIs for SEALDD enabled data storage, the stored data may be queried by the creator or the other network functions for context or content transfer.

9.5.2 Procedure

9.5.2.1 Data storage creation

Pre-conditions:

1. The VAL server has discovered and selected the SEALDD server by CAPIF functions.
2. The SEALDD client has discovered and selected the SEALDD server as specified in clause 9.4.3.

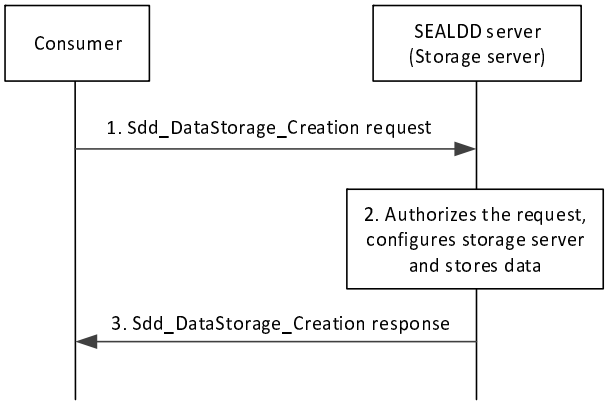

Figure 9.5.2.1-1: Storage service creation

1. The VAL client/server determines to use SEALDD storage service, which could store/host data on behalf of the VAL client/server. The consumer (e.g. SEALDD client, VAL server) send a Sdd_DataStorage_Creation request to the SEALDD server, e.g. using the downlink push mode by VAL server over SEALDD-S interface, as defined in clause 9.1. The request includes the data to be stored and information associated with the data, such as access control policy, expiration time of the storage, etc, and optionally, the identifier of application data. The consumer may also specify in the request the management or status information of the data storage that is required (e.g., information about how often the stored data is accessed or managed).

NOTE 1: If the VAL client determines to use SEALDD storage service, the request is first sent to the SEALDD client hosted on the same UE, and then the SEALDD client send the Sdd_DataStorage_Creation request to the SEALDD server.

NOTE 2: The detailed request between VAL client and SEALDD client is out of scope of this release of this specification.

NOTE 3: The identifier of application data can be included in step 1 for storing the same application data in multiple SEALDD servers. The consumer (e.g. SEALDD client) can retrieve the same application data from different SEALDD servers by using the identifier of application data, as specified in clause 9.5.2.3.

2. The SEALDD server checks for the authorization of the storage service creation request. If the request is successfully authorized, then the SEALDD server configures the storage service based on the request and stores the data at the storage server. If status information of the stored data is requested, the SEALDD server will start to monitor the status of the stored data, such as to track the accesses to the data for the data access status.

3. The SEALDD server sends a response to the requesting consumer (e.g. SEALDD client, VAL server). The response indicates if the request is accepted and the identifier of the stored data (if applicable). Upon receiving the response, the requesting consumer may create a record for the stored data.

9.5.2.2 Data storage reservation

Pre-conditions:

1. The VAL server has discovered and selected the SEALDD server by CAPIF functions.

2. The SEALDD client has discovered and selected the SEALDD server as specified in clause 9.4.3.

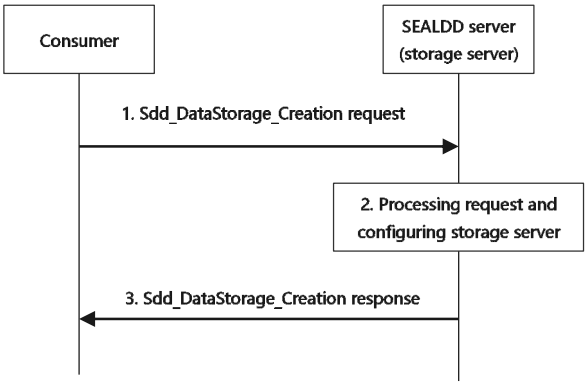

Figure 9.5.2.2-1: Storage service reservation

1. The consumer (e.g. SEALDD client, VAL server) send a Sdd_DataStorage_Creation request to the SEALDD server. The request includes the VAL service ID and the data length.

2. The SEALDD server checks for the authorization of the storage service Creation request. If the request is successfully authorized, then the SEALDD server allocates and reserves the address for data storage.

3. The SEALDD server sends a response to the requesting consumer (e.g. SEALDD client, VAL server). The response indicates if the request is accepted and the address for data storage. Upon receiving the response, the stored data may be delivered via push mode from the requesting consumer to the SEALDD server.

9.5.2.3 Data storage fetch

Pre-conditions:

1. VAL client/server has stored data in SEALDD server.

2. The consumer (e.g. SEALDD client/VAL server/other SEALDD server) requesting the stored data has got the identifier of the stored data (e.g. via application layer signalling or other mechanisms).

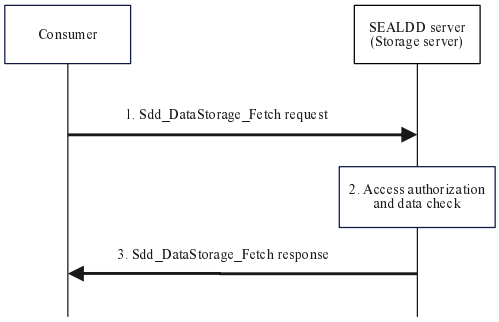

Figure 9.5.2.3-1: Access to stored data in SEALDD server

1. The consumer (e.g. SEALDD client/VAL server/other SEALDD server) sends a Sdd_DataStorage_Fetch request to the SEALDD server with the identifier of the stored data.

NOTE: The consumer requesting for the stored data can be the data storage creator or other network functions.

2. Upon receiving the request, the SEALDD server performs an authorization check to verify if the requested data (according to the data access control policy) is accessed by the consumer. The SEALDD server will also check whether the stored data is expired. If the requested data fetched by SEALDD client is not be stored by the

SEALDD server, the SEALDD server may use the downlink pull mode if possible, to retrieve the data/content from the VAL server over SEALDD-S interface, as defined in clause 9.1.

3. If the verification was successful, the SEALDD server responds with the requested data.

9.5.2.4 Data storage management

Pre-conditions:

1. The SEALDD service is configured to track and maintain data storage access information (i.e. status information).
2. A storage service creation request procedure from the consumer (e.g. SEALDD client, VAL server) to the SEALDD server has been performed. The request includes a subscription to data storage access information (i.e. status information).

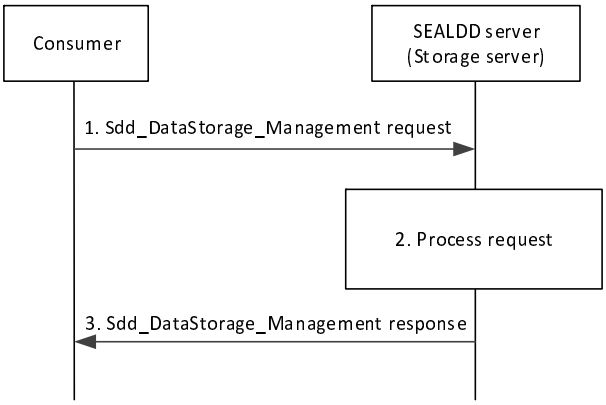

Figure 9.5.2.4-1: Storage management procedure

1. Based on the received stored data status information, the requesting consumer (e.g. SEALDD client, VAL server) determines to perform a management operation, such as to update, refresh, or delete the stored data. The VAL client/server sends a Sdd_DataStorage_Management request to the SEALDD server to perform the determined management operation.
2. The SEALDD server processes the storage management request. If the request is accepted, the SEALDD server performs the required management operation on the stored data.

NOTE: Based on the data management or storage status information available in SEALDD server as per the procedure in clause 9.5.2.1, the SEALDD server may send a notification to the requester (e.g. SEALDD client, VAL server) with the collected management or storage status information.

3. The SEALDD server sends a response to the requesting consumer (e.g. SEALDD client, VAL server) with the result of the management operation, which may include updated information of the stored data.

9.5.2.5 Stored data transfer between VAL servers via SEALDD server

Pre-conditions:

1. The source VAL server already obtains the serving target SEALDD server of the target VAL server.
2. The source VAL server may have stored data to the source SEALDD server and obtained the identifier of the stored data by invoking Sdd_DataStorage_Creation API in clause 9.5.2.1.

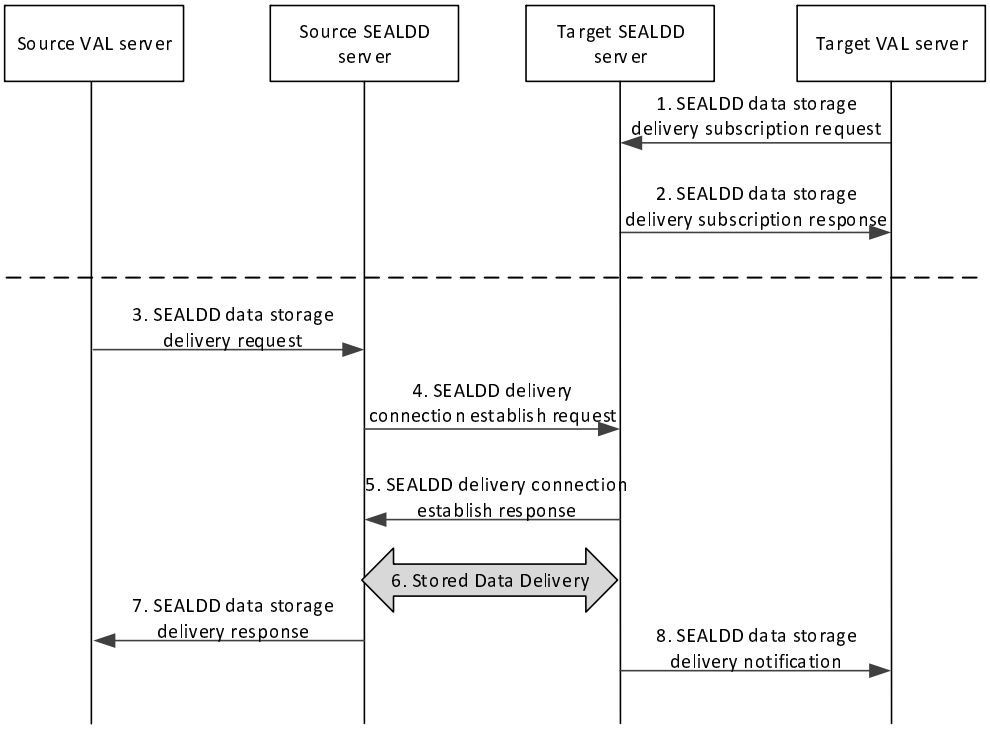

Figure 9.5.2.5-1: Stored data transfer procedure between VAL servers

1. The VAL server sends a SEALDD data storage delivery subscription request to its serving SEALDD server with the VAL server information, and the VAL server address to receive the stored data delivery.

2. The SEALDD sever responds to the requested VAL server with the subscription result, if successful, the response includes the subscription ID, expiration time.

3. The source VAL server determines to use the stored data transfer service provided by the serving SEALDD server. The source VAL server invokes a SEALDD data storage delivery request, the request includes the identifier of the stored data needed to be delivered, or the stored data (i.e., the source VAL server does not use data storage creation to store data to the source SEALDD server before), the target VAL server information and the target SEALDD server information.

4. The source SEALDD server sends a SEALDD delivery connection establish request towards the target SEALDD server with the source SEALDD server information, the target VAL server information, and the supporting transport layer protocols for data delivery.

5. The target SEALDD server responds to the source SEALDD server with the traffic descriptor of target SEALDD server (e.g. address/port, transport layer protocol). The target SEALDD server may allocate the storage for the target VAL server.

NOTE: The transport layer protocol between SEALDD server connection can be different depending on the specific application scenarios, compared with the connection between SEALDD client and SEALDD server in clause 9.2.

6. Upon receiving the traffic descriptor of target SEALDD server, the source SEALDD server sends the requested data corresponding to the identifier of the stored data to the target SEALDD server.

7. The source SEALDD server responds to the source VAL server with the result of data delivery.

8. The target SEALDD server sends the received data to the target VAL server via the notification message. Optionally, the target SEALDD server may only send the identifier of the received data to the target VAL server in the notification message, the target VAL server obtains the stored data originated from the source VAL server, by invoking the Sdd_DataStorage_Fetch API to the target SEALDD server, as specified in clause 9.5.2.2.

9.5.3 Information flows

9.5.3.1 SEALDD data storage creation request

Table 9.5.3.1-1 describes the information flow from the requesting consumer (e.g., VAL server, SEALDD client) to the SEALDD server for requesting the data storage creation.

Table 9.5.3.1-1: SEALDD data storage creation request

Information element	Status	Description
Application data	M (See NOTE 1)	The application data needed to be stored in the SEALDD server
Access control policy	O (See NOTE 1)	The control policy for the requested data access from other consumers (e.g. SEALDD client, VAL server, other SEALDD server)
Storage expiration time	O (See NOTE 1)	The expiration time for the stored data
Storage management or status information	O (See NOTE 1)	Management or status information of the stored data to be tracked or monitored by SEALDD server (e.g. statistics of the stored data, Indications of how often the stored data is accessed or managed) for corresponding notifications.
VAL service ID	M (See NOTE 2)	Identify of the data type to be stored, e.g. video, voice
Data length	O (See NOTE 2)	Identify of the data length to be stored
Identifier of application data	O	Identify of the application data
NOTE 1: These IEs are used for storing application data to the SEALDD server directly, as specified in clause 9.5.2.1. NOTE 2: These IEs are used for requesting the SEALDD server to reserve the data storage resource and address, as specified in clause 9.5.2.2.		

9.5.3.2 SEALDD data storage creation response

Table 9.5.3.2-1 describes the information flow from the SEALDD server to the requesting consumer (e.g., VAL server, SEALDD client) for responding the data storage creation request.

Table 9.5.3.2-1: SEALDD data storage creation response

Information element	Status	Description
Result	M	Success or failure.
Identifier of the stored data	O (See NOTE 1, NOTE 3)	Identify of the stored data
Address for data storage	O (See NOTE 2)	The reserved address for data storage
NOTE 1: This IE is used for returning the identifier of the stored data, as specified in clause 9.5.2.1. NOTE 2: This IE is used for returning the reserved address for data storage, as specified in clause 9.5.2.2. NOTE 3: This IE is same as the identifier of application data, if the identifier of application data is provided in SEALDD data storage creation request message.		

9.5.3.3 SEALDD data storage status notification

Table 9.5.3.3-1 describes the information flow from the SEALDD server to the requesting consumer (e.g., VAL server, SEALDD client) for sending notifications of the data storage status, as configured in the data storage creation request.

Table 9.5.3.3-1: SEALDD data storage status notification

Information element	Status	Description
Management or status information of stored data	M	The management or status information of the stored data requested in the storage creation request.

9.5.3.4 SEALDD data storage fetch request

Table 9.5.3.4-1 describes the information flow from the requesting consumer (e.g., SEALDD client, VAL server, other SEALDD server) to the SEALDD server for requesting the data storage fetch.

Table 9.5.3.4-1: SEALDD data storage fetch request

Information element	Status	Description
Identifier of the stored data	M	Identify the stored data queried by the requesting consumer

9.5.3.5 SEALDD data storage fetch response

Table 9.5.3.5-1 describes the information flow from the SEALDD server to the requesting consumer (e.g., SEALDD client, VAL server, other SEALDD server) for responding the data storage fetch request.

Table 9.5.3.5-1: SEALDD data storage fetch response

Information element	Status	Description
Result	M	Success or failure.
The fetched application data	O	The fetched application data returned to the requesting consumer

9.5.3.6 SEALDD data storage management request

Table 9.5.3.6-1 describes the information flow from the requesting consumer (e.g., SEALDD client, VAL server) to the SEALDD server for requesting the data storage management.

Table 9.5.3.6-1: SEALDD data storage management request

Information element	Status	Description
Storage management operation	M	The operation (e.g. update, refresh, or delete) to manage the stored data

9.5.3.7 SEALDD data storage management response

Table 9.5.3.7-1 describes the information flow from the SEALDD server to the requesting consumer (e.g., VAL server, SEALDD client) for responding the data storage management request.

Table 9.5.3.7-1: SEALDD data storage management response

Information element	Status	Description
Result	M	Success or failure.
The updated information of stored data	O	The updated management or status information of the stored data

9.5.3.8 SEALDD data storage delivery subscription request

Table 9.5.3.8-1 describes the information flow from the VAL server to the SEALDD server for data storage delivery subscription.

Table 9.5.3.8-1: SEALDD data storage delivery subscription request

Information element	Status	Description
VAL server information	M	Identify the requested VAL server to subscribe data delivery
VAL server address	M	Address/port of the VAL server to receive the data delivery from the SEALDD server

9.5.3.9 SEALDD data storage delivery subscription response

Table 9.5.3.9-1 describes the information flow from the SEALDD server to the VAL server for responding the data storage delivery subscription request.

Table 9.5.3.9-1: SEALDD data storage delivery subscription response

Information element	Status	Description
Result	M	Success or failure.
Subscription ID	O	Subscription identifier corresponding to the subscription.
Expiration time	O	Indicates the expiration time of the subscription.

9.5.3.10 SEALDD data storage delivery notification

Table 9.5.3.10-1 describes the information flow from the SEALDD server to the VAL server for notifying the received stored data.

Table 9.5.3.9-1: SEALDD data storage delivery notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Stored data	O (See NOTE)	The received data corresponding to the VAL server
Identifier of the stored data	O (See NOTE)	Identify of the received stored data in SEALDD server
NOTE: One of these IEs shall be present in the message.		

9.5.3.11 SEALDD data storage delivery request

Table 9.5.3.11-1 describes the information flow from the VAL server to the SEALDD server for requesting the data storage delivery.

Table 9.5.3.11-1: SEALDD data storage delivery request

Information element	Status	Description
Target VAL server information	M	Identify the target VAL server
Target SEALDD server information	O	Identify the target SEALDD server
Identifier of the stored data	O (See NOTE)	Identify of the stored data needed to be delivered
Stored data	O (See NOTE)	The data from the VAL server
NOTE: One of these IEs shall be present in the message.		

9.5.3.12 SEALDD data storage delivery response

Table 9.5.3.12-1 describes the information flow from the SEALDD server to the VAL server for responding the data storage delivery request.

Table 9.5.3.12-1: SEALDD data storage delivery response

Information element	Status	Description
Result	M	Success or failure.

9.5.3.13 SEALDD delivery connection establish request

Table 9.5.3.13-1 describes the information flow from the source SEALDD server to the target SEALDD server for requesting the SEALDD delivery connection establishment.

Table 9.5.3.13-1: SEALDD delivery connection establish request

Information element	Status	Description
Source SEALDD server information	M	Identify the source SEALDD server
Traffic descriptor of source SEALDD server	O	The traffic descriptor (e.g. address, port, transport layer protocol) of the source SEALDD server
Target VAL server information	M	Identify the target VAL server

9.5.3.14 SEALDD delivery connection establish response

Table 9.5.3.14-1 describes the information flow from the target SEALDD server to the source SEALDD server for responding the SEALDD delivery connection establishment request.

Table 9.5.3.14-1: SEALDD delivery connection establish response

Information element	Status	Description
Result	M	Success or failure.
Traffic descriptor of target SEALDD server	O	The traffic descriptor (e.g. address, port, transport layer protocol) of the target SEALDD server

9.5.4 APIs

9.5.4.1 General

Table 9.5.4.1-1 illustrates the APIs exposed by SEALDD server for data storage.

Table 9.5.4.1-1: List of SEALDD server APIs for data storage

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_ DataStorage_Creation	Request	Request/Response	SEALDD client, VAL server
Sdd_ DataStorage_Fetch	Request	Request/Response	SEALDD client, VAL server, other SEALDD server
Sdd_ DataStorage_Management	Request	Request/Response	SEALDD client, VAL server
Sdd_DataStorage_Delivery_Subscription	Request	Request/Response	VAL server
Sdd_DataStorage_Delivery_notification	Notify	Subscribe/notify	VAL server
Sdd_DataStorage_Delivery	Request	Request/Response	VAL server
Sdd_DeliveryConnection_Establish	Request	Request/Response	SEALDD server

9.5.4.2 Sdd_DataStorage_Creation Request operation

API operation name: Sdd_DataStorage_Creation Request

Description: The consumer requests for one time for data storage creation or data storage reservation.

Inputs: See clause 9.5.3.1.

Outputs: See clause 9.5.3.2

See clause 9.5.2.1 and clause 9.5.2.2 for details of usage of this operation.

9.5.4.3 Sdd_DataStorage_Fetch Request operation

API operation name: Sdd_DataStorage_Fetch Request

Description: The consumer requests for one time for data storage Fetch.

Inputs: See clause 9.5.3.4.

Outputs: See clause 9.5.3.5.

See clause 9.5.2.3 for details of usage of this operation.

9.5.4.4 Sdd_DataStorage_Management Request operation

API operation name: Sdd_DataStorage_Management Request

Description: The consumer requests for one time for data storage management.

Inputs: See clause 9.5.3.6.

Outputs: See clause 9.5.3.7.

See clause 9.5.2.4 for details of usage of this operation.

9.5.4.5 Sdd_DataStorage_Delivery_Subscription Request operation

API operation name: Sdd_DataStorage_Delivery_Subscription Request

Description: The consumer requests for one time for data storage delivery subscription.

Inputs: See clause 9.5.3.8.

Outputs: See clause 9.5.3.9.

See clause 9.5.2.5 for details of usage of this operation.

9.5.4.6 Sdd_DataStorage_Delivery_Notification operation

API operation name: Sdd_DataStorage_Delivery_Notification

Description: The consumer is notified with the received stored data from SEALDD server.

Inputs: See clause 9.5.3.10.

Outputs: None.

See clause 9.5.2.5 for details of usage of this operation.

9.5.4.7 Sdd_DataStorage_Delivery Request operation

API operation name: Sdd_DataStorage_Delivery Request

Description: The consumer requests for one time for data storage delivery.

Inputs: See clause 9.5.3.11.

Outputs: See clause 9.5.3.12.

See clause 9.5.2.5 for details of usage of this operation.

9.5.4.8 Sdd_DeliveryConnection_Establish Request operation

API operation name: Sdd_DeliveryConnection_Establish Request

Description: The consumer requests for one time for delivery connection establishment between SEALDD servers.

Inputs: See clause 9.5.3.13.

Outputs: See clause 9.5.3.14.

See clause 9.5.2.5 for details of usage of this operation.

9.6 SEALDD server relocation

9.6.1 General

The SEALDD server may be relocated due to UE mobility or load re-balance.

If SEALDD server is adapted to EDGEAPP as an EAS, the EAS relocation procedure is used to support SEALDD server relocation for both UE mobility and SEALDD server load re-balance. If SEALDD is not adapted to EDGEAPP, for UE mobility, the SEALDD client discovers (e.g. using DNS) a new SEALDD server in the target area and establish a new SEALDD communication channel including the old SEALDD communication channel information. For load re-balance, the SEALDD server discovers (e.g. using DNS) an equivalent SEALDD server and communicate with the new SEALDD server.

Based on existing service continuity mechanism supported by 3GPP core network (e.g. BP/ULCL), during SEALDD server relocation with UPF change, the new UPF takes care of the existing unfinished application traffic flow towards the old VAL server and inter-UPF tunnel is used to forward the traffic. For new application traffic flow which may have UE's new IP address as source IP address, the new SEALDD server sends it directly to the new VAL server.

For SEALDD server relocation, the inter-SEALDD server communication via SEALDD-E reference point is needed, which transfers the SEALDD context from the old SEALDD server to the new SEALDD server.

The following procedures detail the EDGEAPP ACT part between old SEALDD server (i.e. S-EAS) and new SEALDD server (i.e. T-EAS) as described in 3GPP TS 23.558 [10], clause 8.8.2.2 to clause 8.8.2.6. Also, a high-level flow is provided to show the scenario used in EDN.

NOTE 1: The way to provide SEALDD server endpoint can be via VAL server or via EES, and discovery of the new SEALDD server can utilize procedure described in clause 9.4. The ACT procedure in the VAL server is also executed according to EDGEAPP ACR scenario but its detail is out of scope of SA6.

NOTE 2: The SEALDD context scope (e.g. service level and/or UE level) has the same granularity with SEALDD transmission request information in clause 9.2.3.1.

NOTE 3: How context synchronization is performed between SEALDD server and VAL server in context transfer is out of scope in this document.

9.6.2 Procedures

9.6.2.1 SEALDD context transfer

Figure 9.6.2.1-1 describes SEALDD context transfer procedure in pull (step 1a and 2a) or push (step 1b and 2b) operation.

Pre-conditions:

1. For pull operation, the old SEALDD server endpoint is available in the new SEALDD server
2. For push operation, the new SEALDD server endpoint is available in the old SEALDD server.

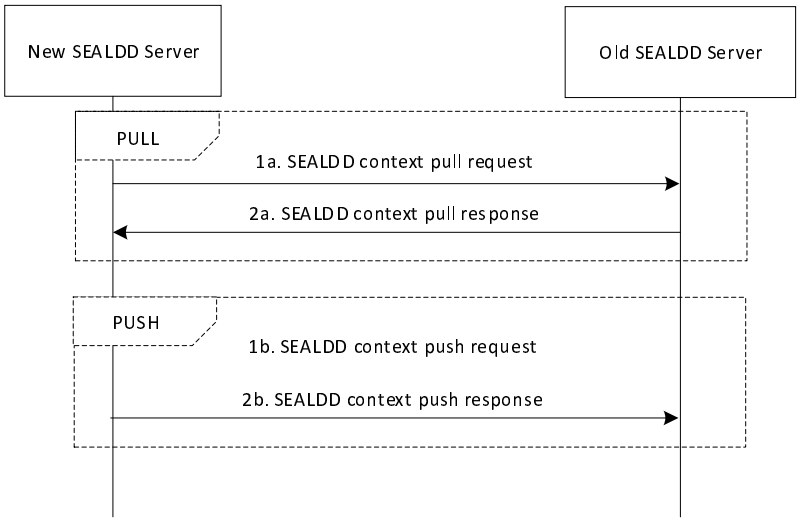

Figure 9.6.2.1-1: SEALDD context transfer

The transferred SEALDD context includes the service subscription information created upon VAL server's interaction for requesting SEALDD transmission service (e.g. step 1 and 2 in Figure 9.2.2.1-1), and also the SEALDD client and SEALDD server communication tunnel management information (e.g. UE IP address) which is created upon SEALDD client's interaction for requesting data transmission (e.g. step 5 and 6 in Figure 9.2.2.1-1). If new SEALDD server supports transportation layer service continuity, additional transport layer context (e.g. TCP/TLS/QUIC) is transferred from old SEALDD server to new SEALDD server. If the new SEALDD Server is not provisioned with the VAL server configured SEALDD policy, then it pulls from the Old SEALDD server via the pull operation. The push operation does not support the transfer of the VAL server configured SEALDD policy between Old and New SEALDD server.

The new SEALDD server, after receiving the SEALDD context from the old SEALDD server, allocates IP address and port for SEALDD-UU user plane communication. The new SEALDD server also sends back to the old SEALDD server with the allocated endpoint information If operation is push. Then the old SEALDD server requests 5GC to perform IP replacement procedure, as defined in clause 6.3.3 of 3GPP 23.548 [8]. The request includes the traffic descriptor of old SEALDD server (i.e., SEALDD-UU address/port), the traffic descriptor of new SEALDD server (i.e., SEALDD-UU address/port) and/or the target DNAI.

Optionally, after receiving the SEALDD context with the SEALDD-UU endpoint from the old SEALDD server, the new SEALDD server requests 5GC to perform IP replacement procedure.

NOTE: The TCP/TLS/QUIC context transfer is required to support the SEALDD server relocation with IP replacement procedure, as described in clause 9.6.2.2.

To improve the seamless SEALDD relocation, the old SEALDD server may stop the downlink data transmission before pushing the SEALDD context to the new SEALDD server, the context data may include content breakpoint information, as defined in clause 9.6.3.1. After the SEALDD client connects to the new SEALDD server, the new SEALDD server transmits the downlink traffic to the SEALDD client based on content breakpoint information.

9.6.2.2 SEALDD relocation in EDN

Pre-conditions:

1. VAL Server 1 and 2 are adapted to the EDGEAPP as EAS.
2. VAL Server 1 and 2 register its associated SEALDD server in EES as described in clause 9.4.3.2.

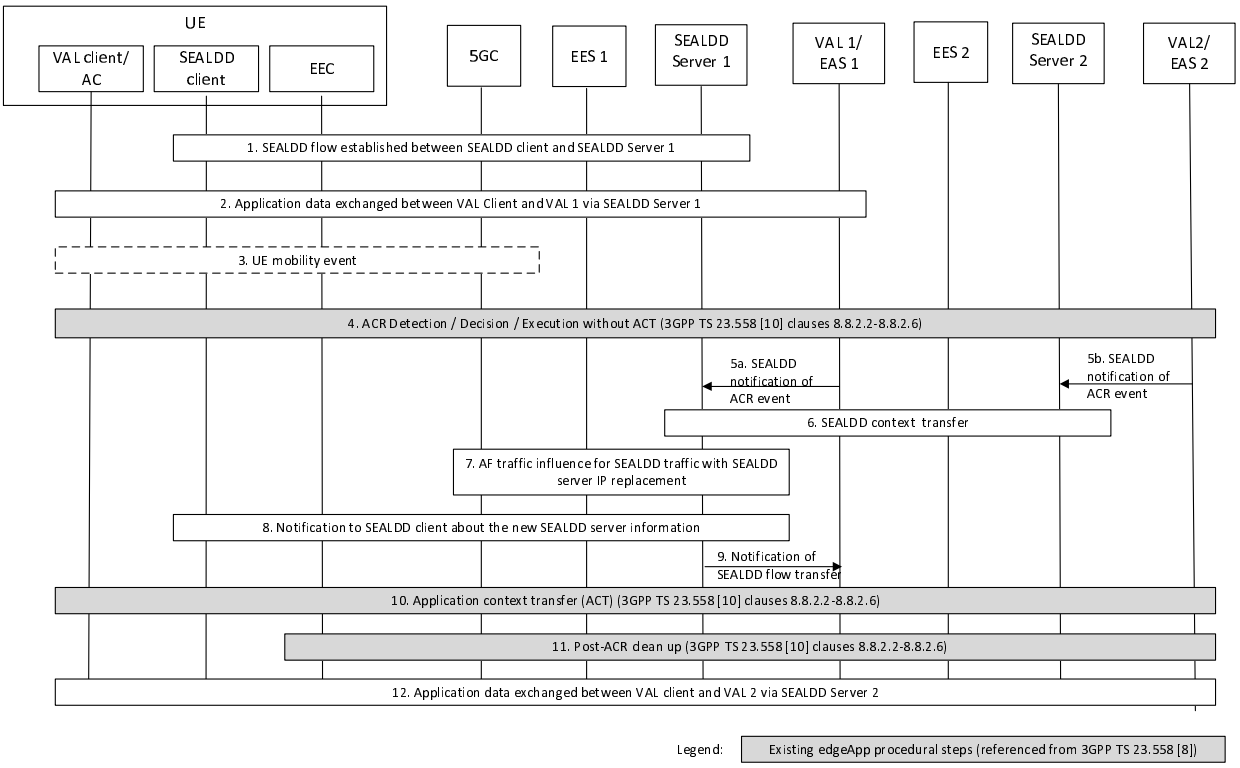

Figure 9.6.2.2-1: SEALDD support of UE's service continuity

1. An application client on a UE, acting as a VAL client, establishes a SEALDD-UU flow over SEALDD-UU to send application data to VAL Server 1. SEALDD client and SEALD server 1 maintain SEALDD-UU flow information (e.g., SEALDD-UU flow ID, VAL IDs/addresses, VAL requirements).

2. Application data between the VAL Client and VAL Server 1 is sent via the SEALDD-UU flow.

3. The UE moves and generates a mobility event in the 5GC.

4. The UE's mobility event triggers the execution of an Application Context Relocation (ACR) procedure as described in 3GPP TS 23.558 [10]; or VAL server 1 triggers ACR due to load re-balancing reason. Any of the ACR scenarios detailed in 3GPP TS 23.558 [10] clauses 8.8.2.2-8.8.2.6 may occur. In this step, the first three phases of the ACR procedure are performed, up to ACT. In this step VAL Server 1 acts as EAS 1 and VAL Server 2 as EAS 2, therefore participating in corresponding signalling. VAL server 2 has been selected as SEALDD-enabled server meeting the ACR criteria to be the target EAS. The associated SEALDD server 2 has also been selected and may support transportation layer (e.g. UDP/TCP/QUIC) service continuity.

5a. Before triggering ACT, VAL Server 1 sends a SEALDD notification of ACR event to SEALDD Server 1.

5b. Before triggering ACT, VAL Server 2 sends a SEALDD notification of ACR event to SEALDD Server 2.

6a. SEALDD server 1 transfers the SEALDD context to the SEALDD server 2 which serves VAL Server 2 as described in clause 9.6.2.1, with push operation. The SEALDD server 1 obtains the SEALDD server 2 endpoint for SEALDD-UU user plane to the SEALDD client, as specified in clause 9.6.2.1.

6b. SEALDD server 2 obtains the SEALDD context from the SEALDD server 1 by using the pull operation, as described in clause 9.6.2.1.

7. SEALDD server 1 applies the functionality specified in 3GPP TS 23.502 [6] clause 5.2.6.7 for AF traffic influence, providing the N6 routing information for the SEALDD client and SEALDD server 2. The SEALDD server 1 may:

- If the SEALDD server 2 supports transportation layer service continuity, additionally includes SEALDD IP replacement information (i.e. SEALDD server 1 endpoint and SEALDD server 2 endpoint for SEALDD-UU user plane) in the AF traffic influence. Since the UE is not aware of SEALDD server change, the new SEALDD traffic (due to new VAL traffic sent by VAL client) is sent by UPF towards the new SEALDD server, this handling in UPF is agnostic to the SEALDD server 2. Or,

- send AF traffic influence with target DNAI of SEALDD server 2, and simultaneous connectivity indicator, to request 5GC to maintain the simultaneous connectivity over source PSA and target PSA with source SEALDD server and target SEALDD server, as described in clause 6.3.4 of 3GPP TS 23.548 [8].

8. If the SEALDD server 2 has no transportation layer service continuity support, a SEALDD Connection info update notification is sent to SEALDD client, e.g. to update the allocated IP address and port for SEALDD-UU user plane communication. Then the SEALDD client acknowledges the received SEALDD Connection info update notification. After SEALDD client is aware of the new SEALDD-UU IP address and port, it starts to send new SEALDD traffic (received from the VAL client) over the new connection. The new SEALDD server maps the received SEALDD traffic to the application traffic according to the SEALDD traffic descriptor and VAL service ID. The new SEALDD server sends the recovered application traffic to new VAL server. The downlink application traffic sent from the new VAL server to VAL client is processed similarly.

9. SEALDD Server 1 notifies VAL Server 1 of the completion of the SEALDD-UU flow transfer.

10. VAL Server 1 (acting as EAS1) and VAL Server 2 (acting as EAS 2) execute the Application Context Transfer (ACT) procedure step corresponding to the pending ACR scenario (3GPP TS 23.558 [10] clauses 8.8.2.2-8.8.2.6), which is out the 3GPP scope.

11. The post-ACR clean-up phase is executed, as described in the corresponding ACR scenario (3GPP TS 23.558 [10] clauses 8.8.2.2-8.8.2.6).

12. The application data from the VAL Client is sent via the SEALDD-UU flow (with SEALDD server 2) to VAL Server 2.

NOTE: The SEALDD-UU client endpoint of the SEALDD-UU flow in this step is maintained the same as in step 1.

9.6.3 Information flows

9.6.3.1 SEALDD context push request

Table 9.6.3.1-1 describes the information flow from the old SEALDD server to the new SEALDD server to push the SEALDD context.

Table 9.6.3.1-1: SEALDD context push request

Information element	Status	Description
Requestor ID	M	Identifies the requestor (i.e. old SEALDD server).
SEALDD-UU Context	M	Identifies the context related to SEALDD-UU connection, which is created upon SEALDD connection establishment.
SEALDD-S Context	M	Identifies the context related to SEALDD-S subscription.
Transport layer context	O	Identifies the context related to Transport layer (e.g. TCP/TLS/QUIC) for SEALDD-UU user plane communication.
Content breakpoint information	O	The downlink data breakpoint information for pre-provisioned data.

9.6.3.2 SEALDD context push response

Table 9.6.3.2-1 describes the information flow from the new SEALDD server to the old SEALDD server for responding to the SEALDD context push request.

Table 9.6.3.2-1: SEALDD context push response

Information element	Status	Description
Result	M (NOTE)	Success or failure.
New SEALDD server endpoint	O	The endpoint (IP address and port) on the new SEALDD for SEALDD-UU user plane communication. Applicable for successful result.
NOTE: The result is failed if the new SEALDD server rejects the relocation for SEALDD client.		

9.6.3.3 SEALDD context pull request

Table 9.6.3.3-1 describes the information flow from the new SEALDD server to the old SEALDD server to pull the SEALDD context.

Table 9.6.3.3-1: SEALDD context pull request

Information element	Status	Description
Requestor ID	M	Identifies the requestor (i.e. new SEALDD server).
SEALDD policy indication	O	Indicates the need to transfer the VAL server configured SEALDD policy.

9.6.3.4 SEALDD context pull response

Table 9.6.3.4-1 describes the information flow from the old SEALDD server to the new SEALDD server for responding to the SEALDD context pull request.

Table 9.6.3.4-1: SEALDD context pull response

Information element	Status	Description
Result	M	Success or failure.
SEALDD-UU Context	O (NOTE)	Identifies the context related to SEALDD-UU connection, which is created upon SEALDD connection establishment.
SEALDD-S Context	O (NOTE)	Identifies the context related to SEALDD-S subscription.
Transport layer context	O (NOTE)	Identifies the context related to Transport layer (e.g. TCP/TLS/QUIC) for SEALDD-UU user plane communication.
SEALDD policy	O (NOTE)	Indicates the VAL server configured SEALDD policy.
NOTE: These IEs are applicable when the result is success.		

9.6.3.5 SEALDD inform ACR event request

Table 9.6.3.5-1 describes the information flow from the VAL server to the SEALDD server to inform the ACR event, for ACR coordination purpose.

Table 9.6.3.5-1: SEALDD inform ACR event request

Information element	Status	Description
VAL server ID	M	Identity of the VAL server
VAL service ID	O	Identity of the VAL service

9.6.3.6 SEALDD inform ACR event response

Table 9.6.3.6-1 describes the information flow from the SEALDD server to the VAL server for responding to the SEALDD inform ACR event request.

Table 9.6.3.6-1: SEALDD inform ACR event response

Information element	Status	Description
Result	M	Success or failure.

9.6.3.7 SEALDD inform ACR event notification

Table 9.6.3.7-1 describes the information flow from the SEALDD server to the VAL server for notifying ACR event related information.

Table 9.6.3.7-1: SEALDD inform ACR event notifiation

Information element	Status	Description
SEALDD flow transfer result	M	Success or failure.

9.6.4 APIs

9.6.4.1 General

Table 9.6.4.1-1 illustrates the APIs exposed by SEALDD server for UE's service continuity.

Table 9.6.4.1-1: List of SEALDD server APIs for UE's service continuity

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_DDContext	Push Request	Request/Response	SEALDD server
	Pull Request	Request/Response	SEALDD server
Sdd_InformACREvent	Request	Subscribe/Notify	VAL server
	Notify	Subscribe/Notify	VAL server

9.6.4.2 Sdd_DDContext_Push Request operation

API operation name: Sdd_DDContext_Push Request

Description: The consumer requests to push SEALDD context.

Inputs: See clause 9.6.3.1.

Outputs: See clause 9.6.3.2

See clause 9.6.2.1 for details of usage of this operation.

9.6.4.3 Sdd_DDContext_Pull Request operation

API operation name: Sdd_DDContext_Pull Request

Description: The consumer requests to pull SEALDD context.

Inputs: See clause 9.6.3.3.

Outputs: See clause 9.6.3.4

See clause 9.6.2.1 for details of usage of this operation.

9.6.4.4 Sdd_InformACREvent_Request operation

API operation name: Sdd_InformACREvent_Request

Description: The consumer informs ACR event to SEALDD server, for ACR coordination purpose.

Inputs: See clause 9.6.3.5.

Outputs: See clause 9.6.3.6.

See clause 9.6.2.2 for details of usage of this operation.

9.6.4.5 Sdd_ InformACREvent _Notify operation

API operation name: Sdd_ InformACREvent_Notify

Description: SEALDD server notifies information about previously informed ACR event.

Inputs: See clause 9.6.3.7.

Outputs: See clause 9.6.3.7.

See clause 9.6.2.2 for details of usage of this operation.

9.7 SEALDD enabled data transmission quality measurement

9.7.1 General

The following clauses specify procedures, information flows and APIs for SEALDD enabled data transmission quality measurement.

9.7.2 Procedures

9.7.2.1 Data transmission quality measurement

Figure 9.7.2-1 illustrate the procedure for SEALDD enabled data transmission quality measurement. The SEALDD client and SEALDD server is enhanced to carry out the data transmission quality measurement.

Pre-conditions:

1. The SEALDD server and SEALDD client are synchronized to the time source provided by 5GS as specified in 3GPP TS 23.501 [5].
2. The VAL server discovers and selects the SEALDD server by CAPIF functions.

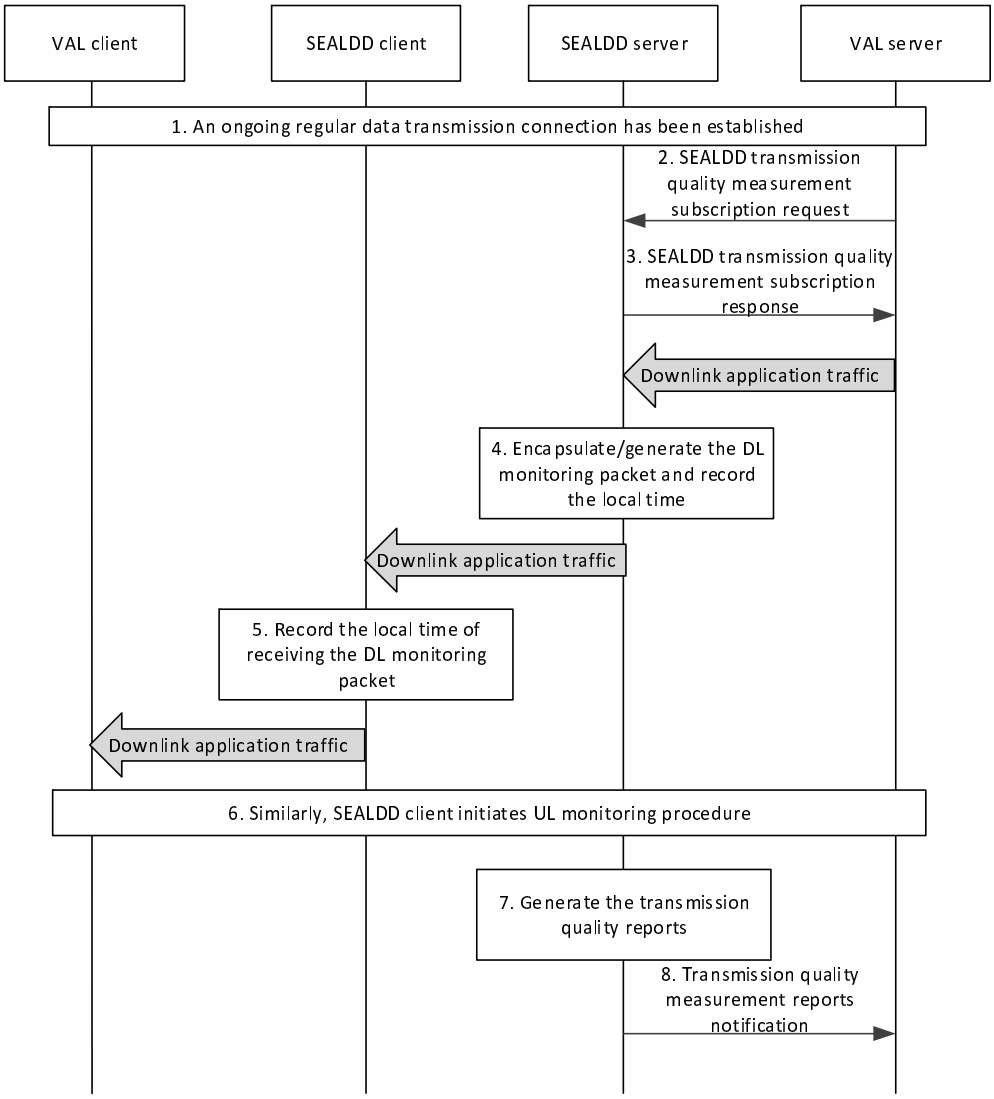

Figure 9.7.2.1-1: SEALDD enabled data transmission quality measurement procedure

1. An on-going regular data transmission connection is established according to clause 9.2.2.2.

2. The VAL server sends a SEALDD transmission quality measurement subscription request to the SEALDD server. The request includes the identifiers of the application traffic (e.g. VAL service ID, VAL server ID), requirement of transmission quality measurement (e.g. latency, jitter, bitrate, packet loss rate) and measurement target UE (e.g. a single UE, a group of UEs or all UEs), flow(s) traffic descriptor(s), and may also include reporting criteria, reporting frequency, spatial condition and temporal condition.

NOTE 1: The spatial and/or temporal condition can be used by SEALDD server to apply when and where the measurement is performed. For instance, the measurement is expected to be done for a group of VAL UEs with a scheduled route (from city A to city B via highway A2 and A3), from 9:00 a.m. to 11:00 a.m. on Tuesday and from 1:00 p.m. to 5:00 p.m. on Thursday.

3. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, the SEALDD server sends a response to the VAL server with the subscription ID, expiration time.

4. If the transmission quality measurement requirement list provided by VAL server in step 2, indicates that the latency is needed to be measured, the SEALDD server initiates the DL packet delay measurement. The SEALDD server encapsulates the DL monitoring packet (i.e. DL SEALDD packet with SEALDD DL monitoring header and VAL traffic as payload, or dummy DL SEALDD packet generated for data transmission quality monitoring) with local time T1 when the SEALDD server sends out the DL monitoring packets. The SEALDD server considers the spatial and/or temporal conditions when starting/resuming the transmission quality measurement. If the conditions are not satisfied, the SEALDD server stops/suspends the transmission quality measurement.

NOTE 2: For other metrics in transmission quality measurement requirement list (e.g. bitrate), the transmission quality result can be obtained by performance detection on the SEALDD server within a period of time.

5. The SEALDD client receives the DL monitoring packet, and records the local time T2. If the endpoint for the SEALDD traffic is located at the tethered device, the SEALDD client in 5G UE measures the QoS between the SEALDD client in 5G UE and the SEALDD client (i.e. for architecture that has the SEALDD client on the tethered device) or the VAL client (i.e. for architecture that without the SEALDD client on the tethered device) in tethered device, e.g., the SEALDD client may measure the tethered link delay using the ICMP ping protocol as defined in IETF RFC792 [RFC792]). The detailed procedures of Tethering link measurement and provisioning is defined in clause 9.12.2.3.

NOTE 3: The tethered link measurement between SEALDD client and VAL client is based on assumption that there is business agreement between the VAL provider and the SEALDD provider, which request the VAL client to respond to ICMP Ping packet.

NOTE 4: Only RTT can be measured for the link between SEALDD client and the tethered device.

6. Similarly, the SEALDD client encapsulates the UL monitoring packet (i.e. UL SEALDD packet with SEALDD UL monitoring header and VAL traffic as payload, or dummy UL SEALDD packet generated for data transmission quality monitoring) with local time T2 recorded in step 5 and local time T3 when the SEALDD client sends out the UL monitoring packet. If the endpoint for the VAL traffic is located at the tethered device, the measurement delay in the tethered link (step 5) is considered in T2 and T3 timestamps, e.g., T2 timestamp includes the half of the measurement delay and T3 timestamp excludes the half of the measurement delay.

NOTE 5: With ICMP ping over tethered link, it is assumed that the UL packet delay and the DL packet delay are the same between the tethering UE and the tethered device.

7. The SEALDD server records the local time T4 when the SEALDD server receives the UL monitoring packet and calculates the latency with T1, T2, T3, T4. The SEALDD server also calculates the bitrate, jitter and packet loss rate over a certain period over a specific SEALDD connection by recording the status of the SEALDD packets carrying VAL traffic or dummy SEALDD packets generated for transmission quality measurement reports. The SEAL DD server also evaluates the reporting criteria if present in the SEALDD transmission quality measurement subscription request in order to generate the transmission quality measurement report.

8. The SEALDD server reports the data transmission quality measurement results (e.g. latency, jitter, bitrate, packet loss rate) to the VAL server via the notification message.

When a VAL group ID or a list of VAL UE IDs or all VAL UEs indication is received in step 2, step 4 to step 7 is repeated for VAL UEs in the group/list or for all VAL UEs. The SEALDD server maps the VAL UE group ID to a list of VAL UE IDs if a VAL group ID is received. The SEALDD server identifies SEALDD connections corresponding to the desired VAL UE(s) or flow(s) traffic descriptor(s) to trigger measurement. And depending on the reporting requirement for multiple UEs, the SEALDD server calculates the needed report for the VAL server. When the VAL server decides to update or unsubscribe transmission quality measurement subscription after performing step 2 and step 3, the VAL server sends data transmission quality measurement subscription update request and data transmission quality measurement unsubscribe request to SEALDD server, as specified in Table 9.7.3.9-1 and Table 9.7.3.11-1, respectively.

9.7.2.2 Data transmission quality query

Figure 9.7.2.2-1 illustrate the procedure for SEALDD enabled data transmission quality query. This procedure is used to obtain the historical transmission quality result already measured as described in clause 9.7.2.1.

Pre-conditions:

1. The SEALDD server performs the data transmission quality measurement procedure, as described in clause 9.7.2.1.

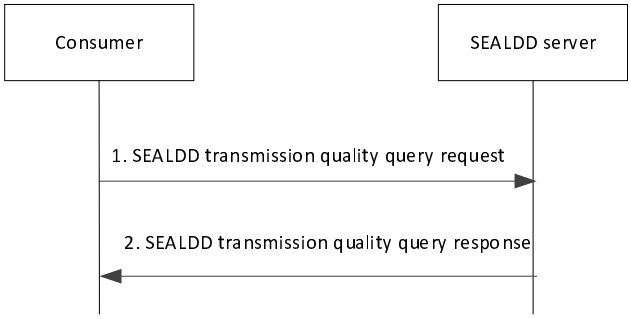

Figure 9.7.2.2-1: SEALDD enabled data transmission quality query procedure

1. The consumers (e.g. VAL server, SEALDD server, NSCE server, ADAE server) sends a SEALDD transmission quality query request to the SEALDD server to obtain the transmission quality measurement result. The request includes the identifiers of the application traffic (e.g. VAL service ID, VAL server ID), VAL UE ID or VAL UE group ID, flow(s) traffic descriptor(s), or crossflow measurement information.

2. The SEALDD server responds with the transmission quality measurement result (e.g. packet delay, bitrate, packet loss rate).

9.7.2.3 Data transmission quality measurement reported by SEALDD client

Figure 9.7.2.3-1 illustrate the procedure for SEALDD enabled data transmission quality measurement for VAL traffic. The SEALDD client receives transmission quality measurement requirement, decides to start VAL data transmission monitoring and generates measurement reports.

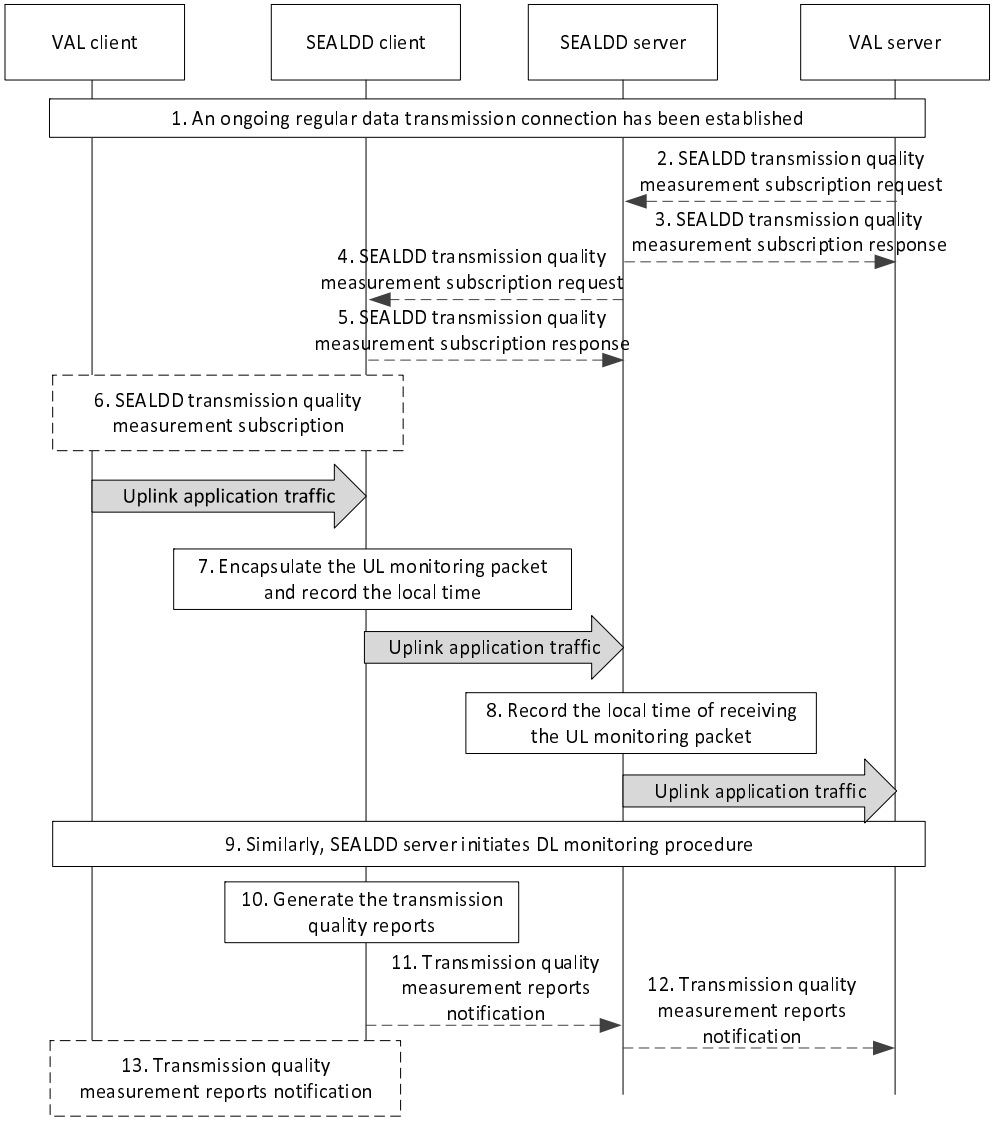

Figure 9.7.2.3-1: VAL data transmission quality measurement reported by SEALDD client

1. An on-going regular data transmission connection is established according to clause 9.2.2.2.

   The transmission quality measurement may be triggered by VAL server or VAL client, which is described in step 2 to step 5 and step 6, correspondingly.

   The request may include the crossflow measurement information (e.g. {[traffic descriptor 1, UL]; [traffic descriptor 2/DL]}) associated in the same multi-modal service for crossflow RTT measurement.

   The detailed procedures of Tethering link measurement and provisioning is defined in clause 9.12.2.3.

2. The VAL server sends a SEALDD transmission quality measurement subscription request to the SEALDD server. The request includes the identifiers of the application traffic (e.g. VAL service ID, VAL server ID), requirement of transmission quality measurement (e.g. latency, jitter, bitrate) and measurement target UE (e.g. a single UE, a group of UEs or all UEs), and may also include reporting criteria, reporting frequency, spatial condition and temporal condition.

NOTE 1: The spatial and/or temporal condition can be used by SEALDD client to apply when and where the measurement is performed. For instance, the measurement is expected to be done for a group of VAL UEs with a scheduled route (from city A to city B via highway A2 and A3), from 9:00 a.m. to 11:00 a.m. on Tuesday and from 1:00 p.m. to 5:00 p.m. on Thursday.

3. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, the SEALDD server responds to the VAL server.

4-5. The SEALDD server sends a SEALDD transmission quality measurement subscription request to the SEALDD client and the SEALDD client responds to the SEALDD server.

If crossflow RTT measurement requirement is received from the VAL server, the SEALDD server identifies the SEALDD connections for the involved VAL UEs and sends to the SEALDD client(s) with crossflow RTT measurement requirement including corresponding UL/DL flow information.

The SEALDD server sends the Non-3GPP access measurement information in the SEALDD transmission quality measurement subscription request to the SEALDD client.

6. The VAL client triggers the SEALDD transmission quality measurement procedure to the SEALDD client, in order to collect the measurement report information.

7. After SEALDD client determines to start measurement process, upon UL packet arrival, the SEALDD client initiates the UL packet delay measurement. The SEALDD client encapsulates the UL monitoring packet (i.e. UL SEALDD packet with SEALDD UL monitoring header and VAL traffic as payload for VAL data transmission quality monitoring) with local time T1 when the SEALDD client sends out the UL monitoring packet. The SEALDD client considers the spatial and/or temporal conditions when starting/resuming the transmission quality measurement. If the conditions are not satisfied, the SEALDD client stops/suspends the transmission quality measurement.

   For crossflow RTT measurement, the SEALDD client received UL flow information starts recording local time T1 when sending out the 1st UL packet matching the UL flow information to the SEALDD server. The T1 is sent in the encapsulated UL monitoring packet to the SEALDD server.

8. The SEALDD server receives the UL monitoring packet, and records the local time T2.

9. Similarly, the SEALDD server encapsulates the DL monitoring packet (i.e. DL SEALDD packet with SEALDD DL monitoring header and VAL traffic as payload, or dummy DL SEALDD packet generated for data transmission quality monitoring in case there is no DL VAL traffic for DL packet delay monitoring) with local time T2 recorded in step 8 and local time T3 when the SEALDD server sends out the DL monitoring packet.

NOTE 2: When the SEALDD server sends the dummy DL packet as monitoring response to the SEALDD client depends on SEALDD server implementation.

   For crossflow RTT measurement, when the 1st DL packet matching the received DL flow information is to be sent, the SEALDD server encapsulates the DL monitoring packet with previously received T1 and sends the DL monitoring packet to the SEALDD client.

10. The SEALDD client records the local time T4 when the SEALDD client receives the DL monitoring packet and calculates the latency with T1, T2, T3, T4. The SEALDD client also calculates the bitrate and jitter over a certain period over a specific SEALDD connection by recording the status of the SEALDD monitoring packets. The SEALDD client also evaluates the reporting criteria and the flow alignment reporting criteria if present in the SEALDD transmission quality measurement subscription request in order to generate the transmission quality measurement report.

    For crossflow RTT measurement, if T1 is received in the DL packet, the SEALDD client records local time T2 and calculates RTT based on T1 and T2.

    Depending on which entity triggers the data transmission quality measurement, step 11 and step 12 corresponds to step 2 to step 5, step 13 corresponds to step 6.

    For the Non-3GPP access measurement, if the Non-3GPP access measurement information includes list of WLAN SSIDs, then the SEALDD client performs the signal strength measurement for the requested WLAN SSID. If the request contains location-based measurement then the SEALDD client measures the signal strength of nearby WLAN SSIDs based on its location.

    If the delay difference, i.e., the bound of the difference of the end-to-end time delay among all associated flows, is requested, the SEALDD client calculates the delay difference between VAL server and SEALDD client, based on the arrival time and the timestamp (e.g., timestamp as recorded in the RTP header) among all associated flows identified by the Multi-modal SEALDD flow ID. The arrival time of first detected flow and last detected flow, Ta and Tb, are recorded, and the delay difference is the difference between Ta and Tb. Then SEALDD client sends the calculated delay difference to the SEALDD server.

NOTE 3: The cross flow RTT measurement calculated by the SEALDD client does not need to differentiate whether the RTT measures are taken over the PDUs of a PDU set.

11-12. The SEALDD client reports the data transmission quality measurement results (e.g. latency, jitter, bitrate) to the VAL server via the SEALDD server. The report also includes the list of WLAN SSIDs and their signal strength measurements (like RSSI). The Measurement range indicate the scope of the measurement, e.g., end to end measurement, tethering link measurement etc.

13. The SEALDD client reports the data transmission quality measurement results to the VAL client.

NOTE 4: The crossflow RTT measurement calculated by the SEALDD client in step 10 can be used as an estimation of the lower bound for the Motion-to-Photon latency in the XR scenarios.

When a VAL group ID or a list of VAL UE IDs or all VAL UEs indication is received in step 2, step 4 to step 11 is repeated for VAL UEs in the group/list or for all VAL UEs. The SEALDD server maps the VAL UE group ID to a list of VAL UE IDs if a VAL group ID is received. The SEALDD server identifies SEALDD connections corresponding to the desired VAL UE(s) to trigger measurement. And depending on the reporting requirement for multiple UEs, the SEALDD server collects and aggregates the needed report for the VAL server.

9.7.3 Information flows

9.7.3.1 SEALDD enabled data transmission quality measurement subscription request

Table 9.7.3.1-1 describes the information flow from the VAL server to the SEALDD server for subscribing to the data transmission measurement service.

Table 9.7.3.1-1: SEALDD transmission quality measurement subscription request

Information element	Status	Description
Application traffic identifiers	M	Identify of the application traffic (e.g. VAL server ID, VAL service ID)
Identity	O (See NOTE)	Identifier of the VAL UE or VAL user for which measurements need to be provided.
VAL UE/user group ID	O (See NOTE)	Identifier of a specific VAL UE/user group, as defined in clause 7.5 of 3GPP TS 23.434 [4].
Identity list	O (See NOTE)	Identifies a list of VAL UEs, e.g. the list of UE ID, or a list of VAL users.
All VAL UEs or VAL users Indication	O (See NOTE)	Indicates all VAL UEs or VAL users of the application identified by application traffic identifiers.
Flow(s) traffic descriptor(s)	O (See NOTE)	Indicates the flow(s) traffic descriptor(s) (Address/port or URL) for the measurement.
Crossflow measurement information	O (see NOTE)	Represents the crossflow measurement information, e.g., list of pairs traffic descriptor with traffic direction (UL or DL). Example of the crossflow measurement information: {[traffic descriptor 1, UL]; [traffic descriptor 2, DL]}.
Measurement conditions	O	Indicates the temporal and/or spatial conditions.
Transmission quality measurement requirements list	M	The measurement requirement information
> Measurement ID	M	Measurement identifiers, e.g. UL/DL/E2E latency, UL/DL bitrate, UL/DL/E2E packet loss rate, UL/DL/E2E jitter, and crossflow identifier (e.g., crossflow latency, crossflow bitrate, crossflow packet loss rate, crossflow jitter).
> Reporting frequency	O	The reporting frequency of measurement results (e.g. periodic reporting). If not present, it implies periodic reporting.
> Reporting periodicity	O	If the reporting frequency is periodic, the reporting periodicity shall be provided. For multiple UEs/users, it is recommended to give sufficient time to allow report aggregation.
> Reporting granularity	O	The reporting granularity indicates whether the measurement report is for individual VAL UE/user or for VAL UE/user group or for all VAL UEs/users, if VAL UE/user group or all VAL UEs/users is the measurement target.
> Measurement period window	O	Indicates the measurement period window for transmission quality measurements
> Measurement expiration time	O	Indicates the measurement expiration time
> Reporting criteria	O	Indicates the criteria for reporting measurement results, e.g. if the latency or bitrate reaches below or above a certain value. It also includes a unique identifier for each criteria of more than one criteria is specified.
NOTE: One of them shall be present as the measurement target UE or traffic descriptor.		

9.7.3.2 SEALDD enabled data transmission quality measurement subscription response

Table 9.7.3.2-1 describes the information flow from the SEALDD server to the VAL server for responding to the transmission quality measurement subscription request.

Table 9.7.3.2-1: SEALDD transmission quality measurement subscription response

Information element	Status	Description
Result	M	Success or failure.
Subscription ID	O	Subscription identifier corresponding to the subscription. Applicable for successful result.
Expiration time	O	Indicates the expiration time of the subscription. Applicable for successful result.

9.7.3.3 SEALDD enabled data transmission quality measurement notification

Table 9.7.3.3-1 describes the information flow from the SEALDD server to the VAL server for notifying the transmission quality measurement reports.

Table 9.7.3.3-1: SEALDD transmission quality measurement notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Transmission quality measurement reports list	M	The generated transmission quality results in SEALDD server or SEALDD client, as specified in Table 9.7.3.3-2.

Table 9.7.3.3-2 describes the information elements for the transmission quality measurement reports list, provided by the SEALDD server after performing transmission quality measurement.

Table 9.7.3.3-2: SEALDD transmission quality measurement reports list

Information element	Status	Description
> Measurement ID	M	Measurement identifiers, (e.g. UL/DL/E2E latency, UL/DL bitrate, UL/DL/E2E packet loss rate, UL/DL/E2E jitter) and crossflow identifiers (e.g., crossflow latency, crossflow bitrate, crossflow packet loss rate, crossflow jitter).
> VAL UE/user ID(s) or flow(s)traffic descriptor(s)	O (see NOTE)	It indicates the VAL UE(s) or VAL user(s) under SEALDD measurement. For a single VAL UE/user or flow(s)traffic descriptor(s), it can be omitted and the associated measurement values are for the single VAL UE/user. For multiple VAL UEs/users or flow(s)traffic descriptor(s) with reporting granularity set to individual UE/user or flow traffic descriptor, the associated measurement values are for individual VAL UE/user or flow traffic descriptor as indicated in this IE. For multiple VAL UEs/users with reporting granularity set to VAL UE/user group/list or all VAL UEs/users, the associated measurement values are aggregation for all VAL UEs/users or the VAL UE/user group/list and this IE includes the measured VAL UEs/users.
> Crossflow measurement information	O (see NOTE)	Represents the crossflow measurement information, e.g., list of pairs traffic descriptor with traffic direction (UL or DL). Example of the crossflow measurement information: {[traffic descriptor 1, UL]; [traffic descriptor 2, DL]}.
> Average measurement value	O	The average measurement value of measurement results
> Minimum measurement value	O	The minimum measurement value of measurement results
> maximum measurement value	O	The maximum measurement value of measurement results
> Standard deviation measurement value	O	Standard deviation measurement value of measurement results
> kPercentile measurement value	O	Indicates the kpercentile measurement value of measurement results
> Measurement period	O	Indicates the measurement period
> Timestamp	O	Indicates the timestamp of measurement results
NOTE: These IEs are mutually exclusive.		

9.7.3.4 SEALDD enabled data transmission quality query request

Table 9.7.3.4-1 describes the information flow from the other consumers (e.g. SEALDD server, NSCE server, ADAE server) to the SEALDD server for querying the data transmission quality measurement result.

Table 9.7.3.4-1: SEALDD transmission quality query request

Information element	Status	Description
Application traffic identifiers	M	Identify of the application traffic (e.g. VAL server ID, VAL service ID)
VAL UE/user ID(s) or flow(s) traffic descriptor(s)	O (see NOTE)	Identifier of VAL UE(s), VAL user(s), or flow(s) traffic descriptor(s) need to be queried, e.g. single VAL UE/user, multiple VAL UEs/users, flow(s) traffic descriptor(s), or VAL UE/user group
Crossflow measurement information	O (see NOTE)	Represents the crossflow measurement information, e.g., list of pairs traffic descriptor and traffic direction (UL or DL). Example of the crossflow measurement information: {[traffic descriptor 1, UL]; [traffic descriptor 2, DL]}.
NOTE: These IEs are mutually exclusive.		

9.7.3.5 SEALDD enabled data transmission quality query response

Table 9.7.3.5-1 describes the information flow from the SEALDD server to the other consumers (e.g. SEALDD server, NSCE server, etc) for returning the data transmission quality reports.

Table 9.7.3.5-1: SEALDD transmission quality query response

Information element	Status	Description
Result	M	Success or failure.
Transmission quality measurement reports list	M	The generated transmission quality results in SEALDD server, as specified in Table 9.7.3.3-2.

9.7.3.6 Transmission quality measurement subscription request

Table 9.7.3.6-1 describes the information flow from the SEALDD server to the SEALDD client for data transmission measurement subscription.

Table 9.7.3.6-1: Transmission quality measurement subscription request

Information element	Status	Description
SEALDD-UU flow ID	O (see NOTE)	Identifier of the SEALDD-UU flow.
Multi-modal SEALDD flow ID	O (see NOTE)	Identity of the multi-modal SEALDD flows associated with the SEALDD multi-modal connection for the measurement.
Measurement conditions	O	Indicates the temporal and/or spatial conditions.
Transmission quality measurement requirements list	M	The measurement requirement information
> Measurement ID	M	Measurement identifiers, e.g. latency, bitrate, jitter, signal strength (e.g. RSSI)
> Reporting frequency	O	The reporting frequency of measurement results (e.g. periodic reporting). If not present, it implies periodic reporting.
> Reporting periodicity	O	If the reporting frequency is periodic, the reporting periodicity shall be provided.
> Measurement period window	O	Indicates the measurement period window for transmission quality measurements
> Measurement expiration time	O	Indicates the measurement expiration time
> Reporting criteria	O	Indicates the criteria for reporting measurement results, e.g. if the latency or bitrate reaches below or above a certain value. It also includes a unique identifier for each criteria if more than one criteria is specified.
> Delay difference indicator	O	Indicates the delay difference needs to be measured.
> Flow alignment reporting criteria	O	Indicates the criteria for reporting flow alignment measurement results, e.g. if the flow alignment buffering reaches below or above a certain value for a certain amount of time. It also includes a unique identifier for each criteria if more than one criteria is specified.
> SEALDD policy	O	Specifies quality guarantee policies associated with the SEALDD connection
>> Quality guarantee policy	M	Indicates the event (e.g. measurement threshold) to be measured for, the quality guarantee.
>> Non-3GPP access measurement information	O	Indicates the non-3GPP access(like WLAN) measurement policy (e.g. WLAN SSIDs, BSSID, location-based measurement)
NOTE: Only one of the information element is present.		

9.7.3.7 Transmission quality measurement subscription response

Table 9.7.3.7-1 describes the information flow from the SEALDD client to the SEALDD server for responding to the transmission quality measurement subscription request.

Table 9.7.3.7-1: Transmission quality measurement subscription response

Information element	Status	Description
Result	M	Success or failure.
Expiration time	O	Indicates the expiration time of the subscription. Applicable for successful result.

9.7.3.8 Transmission quality measurement notification

Table 9.7.3.8-1 describes the information flow from the SEALDD client to the SEALDD server for notifying the transmission quality measurement reports.

Table 9.7.3.8-1: Transmission quality measurement notification

Information element	Status	Description
Transmission quality measurement reports list	M	The generated transmission quality results in SEALDD server
> Measurement ID	M	Measurement identifiers, e.g. latency, bitrate, jitter, delay difference, flow alignment measurement, signal strength (e.g., RSSI)
> Measurement range	O	Indicates the range of the measurement, e.g., end to end measurement, tethering link measurement etc.
> Average measurement value	O	The average measurement value of measurement results
> Minimum measurement value	O	The minimum measurement value of measurement results
> maximum measurement value	O	The maximum measurement value of measurement results
> Standard deviation measurement value	O	Standard deviation measurement value of measurement results
> kPercentile measurement value	O	Indicates the kpercentile measurement value of measurement results
> Measurement period	O	Indicates the measurement period
> Timestamp	O	Indicates the timestamp of measurement results
> Non-3GPP access measurement information	O	Indicates the non-3GPP access measurement information report.
> Measured non-3GPP access	O	List of measured non-3GPP access (e.g., WLAN SSID(s)/BSSID(s) or location information).
>> Signal strength value(s)	M	List of signal strength values (e.g., RSSI) for the measured non-3GPP access.

9.7.3.9 SEALDD enabled data transmission quality measurement subscription update request

Table 9.7.3.9-1 describes the information flow from the VAL server to the SEALDD server for updating the data transmission measurement subscription service.

Table 9.7.3.9-1: SEALDD transmission quality measurement subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the updated subscription.
Updated transmission quality measurement information	O (see NOTE)	The updated transmission quality measurement information, as described in Table 9.7.3.1-1.
NOTE: At least one of these IEs in Table 9.7.3.1-1 is present.		

9.7.3.10 SEALDD enabled data transmission quality measurement subscription update response

Table 9.7.3.10-1 describes the information flow from the SEALDD server to the VAL server for responding to the transmission quality measurement subscription update request.

Table 9.7.3.10-1: SEALDD transmission quality measurement subscription update response

Information element	Status	Description
Result	M	Success or failure.
Expiration time	O	Indicates the expiration time of the subscription. Applicable for successful result.

9.7.3.11 SEALDD enabled data transmission quality measurement unsubscribe request

Table 9.7.3.11-1 describes the information flow from the VAL server to the SEALDD server for unsubscribing to the data transmission measurement service.

Table 9.7.3.11-1: SEALDD transmission quality measurement unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the unsubscription.

9.7.3.12 SEALDD enabled data transmission quality measurement unsubscribe response

Table 9.7.3.12-1 describes the information flow from the SEALDD server to the VAL server for responding to the transmission quality measurement unsubscribe request.

Table 9.7.3.12-1: SEALDD transmission quality measurement unsubscribe response

Information element	Status	Description
Result	M	Success or failure.

9.7.4 APIs

9.7.4.1 General

Table 9.7.4.1-1 illustrates the APIs exposed by SEALDD server for data transmission quality measurement.

Table 9.7.4.1-1: List of SEALDD server APIs for transmission quality measurement

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_TransmissionQuality Measurement	Subscribe	Subscribe/Notify	VAL server, SEALDD server
	Update	Subscribe/Notify	VAL server, SEALDD server
	Unsubscribe	Subscribe/Notify	VAL server, SEALDD server
	Notify	Subscribe/notify	VAL server, SEALDD server
	Query	Request/Response	VAL server, SEALDD server, NSCE server, ADAE server

9.7.4.2 Sdd_TransmissionQualityMeasurement_Subscribe operation

API operation name: Sdd_TransmissionQualityMeasurement_subscription Request

Description: The consumer requests for subscribing transmission quality measurement service.

Inputs: See clause 9.7.3.1.

Outputs: See clause 9.7.3.2

See clause 9.7.2.1 and clause 9.7.2.3 for details of usage of this operation.

9.7.4.3 Sdd_TransmissionQualityMeasurement_Notify operation

API operation name: Sdd_TransmissionQualityMeasurement_notify

Description: The consumer is notified with the transmission quality measurement reports.

Inputs: See clause 9.7.3.3.

Outputs: None.

See clause 9.7.2.1 and clause 9.7.2.3 for details of usage of this operation.

9.7.4.4 Sdd_TransmissionQualityMeasurement_Query operation

API operation name: Sdd_TransmissionQualityMeasurement_Query Request

Description: The consumer requests for one time for transmission quality query.

Inputs: See clause 9.7.3.4.

Outputs: See clause 9.7.3.5.

See clause 9.7.2.2 for details of usage of this operation.

9.7.4.5 Sdd_TransmissionQualityMeasurement_Update operation

API operation name: Sdd_TransmissionQualityMeasurement_Update

Description: The consumer requests for updating transmission quality measurement service.

Inputs: See clause 9.7.3.9.

Outputs: See clause 9.7.3.10

See clause 9.7.2.1 and clause 9.7.2.3 for details of usage of this operation.

9.7.4.6 Sdd_TransmissionQualityMeasurement_Unsubscribe operation

API operation name: Sdd_TransmissionQualityMeasurement_Unsubscribe

Description: The consumer requests for unsubscribing transmission quality measurement service.

Inputs: See clause 9.7.3.11.

Outputs: See clause 9.7.3.12.

See clause 9.7.2.1 for details of usage of this operation.

9.8 SEALDD enabled rate control for VAL applications

9.8.1 General

The following clauses specify procedures, information flows and APIs for SEALDD enabled rate control transmission.

NOTE: In clause 9.8, the terms bandwidth control and data transmission rate control are interchangeable.

9.8.2 Procedures

9.8.2.1 SEALDD enabled bandwidth control for different VAL users

The SEALDD layer provides the differentiated data delivery service with different bandwidth experience for VAL users, where the VAL server provides the bandwidth limit (i.e., minimum bandwidth requirement and maximum bandwidth limit) for VAL users. Figure 9.8.2.1-1 illustrates the procedure for bandwidth control for different VAL users.

Pre-conditions:

1. The VAL server has discovered and selected the SEALDD server by CAPIF functions as specified in clause 9.4.2.

2. The SEALDD server has subscribed to 5GC for QoS monitoring of the specific UE related to the VAL user, as defined in clause 5.2.6.9 in 3GPP TS 23.502 [6].

3. The SEALDD policy (i.e, the bandwidth control policy) has been configured in SEALDD server, as described in clause 9.10.

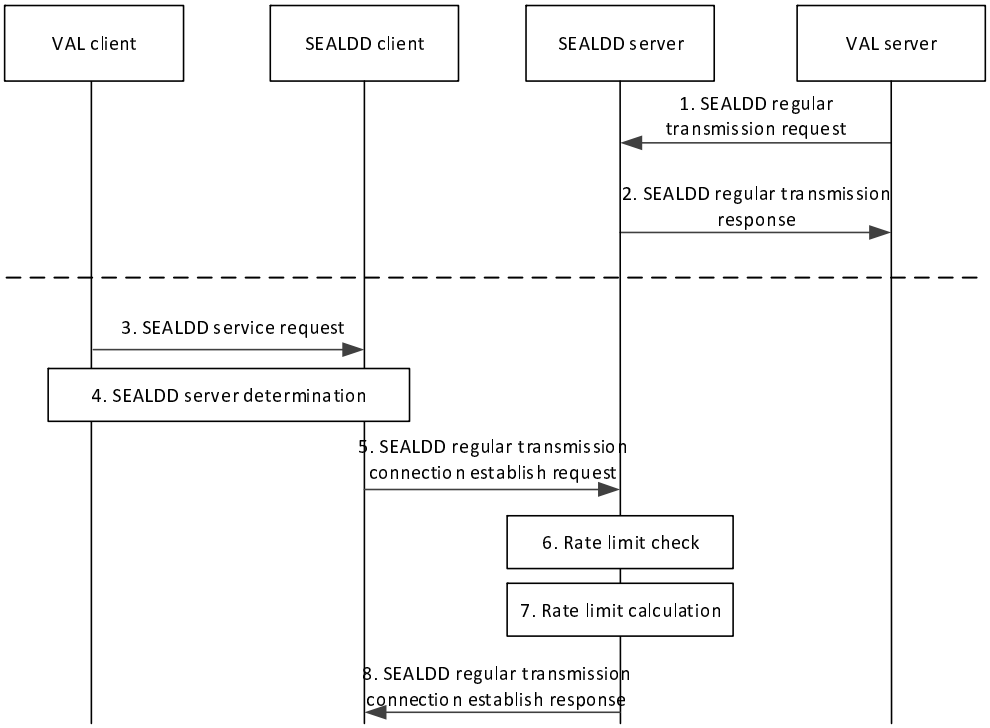

Figure 9.8.2.1-1: SEALDD enabled bandwidth control transmission procedure

1. The VAL server sends a Sdd_regularTransmission request to the SEALDD server. The request includes the identifiers of the application traffic (e.g. VAL service ID, VAL server ID), the VAL server's total bandwidth limit and the bandwidth limits (i.e. minimum bandwidth requirement and maximum bandwidth limit) for VAL users.

2. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, the SEALDD server sends a response to the VAL server.

3. The VAL client sends a SEALDD service request to SEALDD client.

4. The VAL/SEALDD client discover and select the proper SEALDD server for the VAL application. After this step, the VAL server is discovered and selected along with the associated SEALDD server, the SEALDD client gets the SEALDD server's address.

5. The SEALDD client sends Sdd_RegularTransmissionConnection_Establish request to SEALDD server with the SEALDD client ID, the VAL user or UE identity, XR application device capability information as per Table 9.2.3.3-1.

6. The SEALDD server performs bandwidth limit check according to the VAL user's bandwidth limit, the current SEALDD traffic delivery status, the VAL server's total bandwidth limit and/or the related UE's current network status (i.e. via QoS monitoring report from the 5GC). If the available bandwidth (i.e. the remaining bandwidth that is used for the VAL user without exceeding the VAL server's total bandwidth limit) fails to meet the VAL user's minimum bandwidth requirement, the SEALDD server will reject the SEALDD client's connection establishment request.

7. When the available bandwidth meets the VAL user's requirement, the SEALDD client establishes the SEALDD connection with the SEALDD server. The SEALDD server calculates the suggested traffic transmission bandwidth to the SEALDD client according to the VAL user's bandwidth limit and the related UE's current network status (i.e. via QoS monitoring report or ECN marking for L4S report from the 5GC) and XR application device capability information.

8. If the bandwidth limit check is failed (i.e., the available bandwidth fails to meet the VAL user's minimum bandwidth requirement) in step 6, the SEALDD server sends Sdd_RegularTransmissionConnection_Establish response with the failed result (i.e., reject the connection establishment) and the pending timer to trigger the re-connection from SEALDD client. If the bandwidth limit check is successful (i.e., the available bandwidth meets the VAL user's requirement) in step 6, the SEALDD server sends

Sdd_RegularTransmissionConnection_Establish response with the successful result and/or the suggested traffic transmission bandwidth.

NOTE: The SEALDD server can re-allocate the available bandwidth resource to different VAL users according to the configured bandwidth control policy, as described in clause 9.10.

If the connection establishment is rejected, the SEALDD client re-establishes SEALDD connection by performing steps 5-8, when the pending timer is expired.

For the uplink application traffic, the SEALDD client buffers or drops some packets when the uplink traffic from VAL client exceeds the suggested traffic transmission bandwidth. Similarly, for the downlink application traffic, the SEALDD server buffers or drops some packets when the downlink traffic from VAL server exceeds the suggested traffic transmission bandwidth.

9.8.2.2 SEALDD enabled congestion control for VAL applications

Based on the congestion information exposed by 5GS (i.e., by using ECN marking for L4S), the SEALDD server performs the differentiated congestion control for multiple VAL applications, after receiving the L4S feedback from the SEALDD client. Figure 9.8.2.2-1 illustrates the procedure for SEALDD enabled congestion control for VAL applications.

Pre-conditions:

1. The VAL server has discovered and selected the SEALDD server by CAPIF functions as specified in clause 9.4.2.

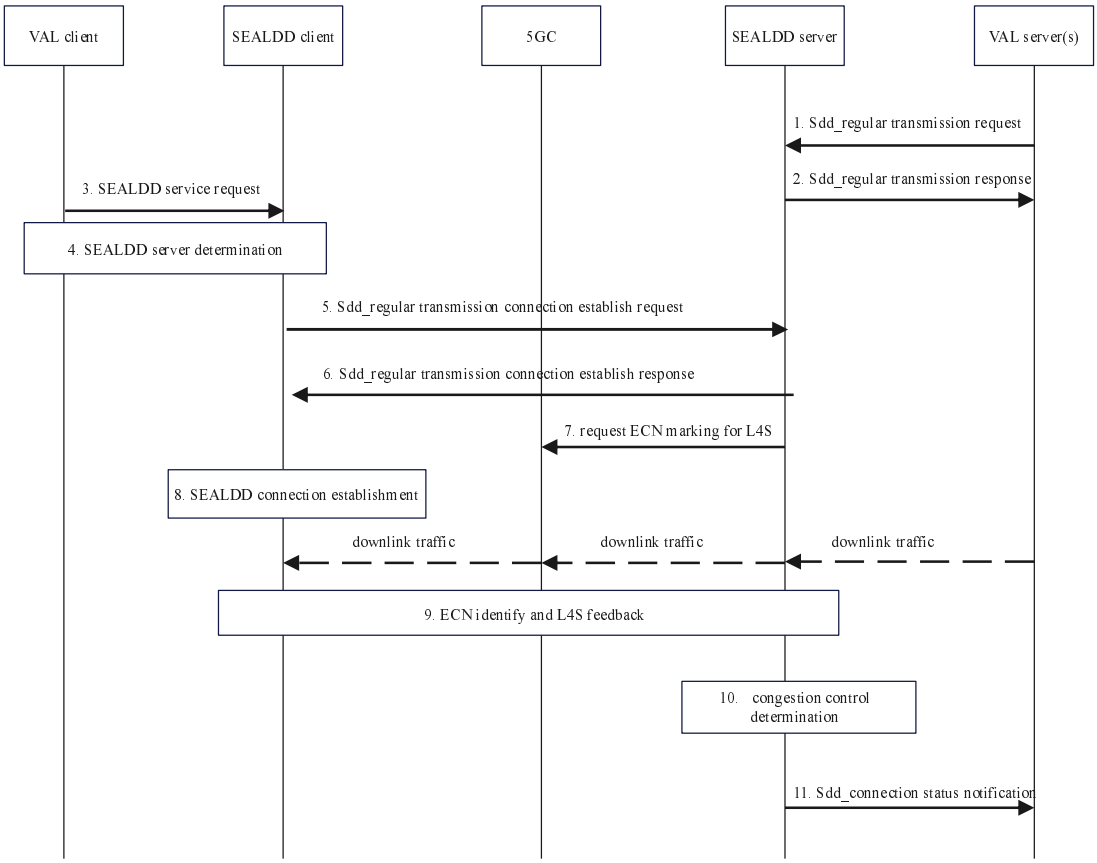

Figure 9.8.2.2-1: SEALDD enabled congestion control procedure

1-6. Same as clause 9.2.2.2 step 1 to step 7 with difference that in step 5 the SEALDD client includes also L4S feedback capability in Sdd_RegularTransmissionConnection_Establish request.

7. If the L4S feedback capability is received in step 5, the SEALDD server requests 5GC to perform the ECN marking for L4S for the required VAL applications by utilizing the AF session with required QoS procedure in clause 4.15.6.6 of 3GPP TS 23.502 [6].

8. Same as step 9 of clause 9.2.2.2.

9. For downlink traffic, if ECN marking is identified, the L4S feedback is performed in transport layer.

10. After receiving the L4S feedback in step 9, the SEALDD server may perform the congestion mitigation for downlink traffics from multiple VAL applications. For the same UE, the SEALDD server determines differentiated congestion control/rate control with the calculated congestion level or the calculated transmission rate for multiple VAL applications based on internal policy considering the received QoS requirements of different VAL applications identified by VAL service ID in step 1.

11. [Optional] The SEALDD server sends Sdd_connection status notification to VAL server with the calculated congestion level for the VAL service.

NOTE 1: According to the congestion level provided by SEALDD server, the VAL server supporting media can perform congestion control, e.g. by adjusting the encoding scheme, and rendering scheme, etc.

NOTE 2: Step 11 is performed if the SEALDD server cannot perform transmission rate adaptation to mitigate the congestion by itself.

9.8.3 Information flows

See clause 9.2.3 for the details of information flow.

9.8.4 APIs

See clause 9.2.4 for the details of API.

9.9 SEALDD enabled data transmission quality guarantee

9.9.1 General

The following clauses specify procedures, information flows and APIs for SEALDD enabled data transmission quality guarantee.

9.9.2 Procedures

9.9.2.1 SEALDD enabled data transmission quality guarantee by switching SEALDD server

Figure 9.9.2.1-1 illustrate the procedure for data transmission quality guarantee based on transmission quality report from SEALDD server and QoS monitoring from 5GS. The procedure is applicable to the scenario where there is a single path between UE and SEALDD server.

Pre-conditions:

1. The VAL server discovers and selects the SEALDD server by CAPIF functions.

2. The VAL server has requested the transmission quality measurement to the SEALDD server by invoking the Sdd_TransmissionQualityMeasurement_subscription API in clause 9.7.4.2.

3. A SEALDD service policy (i.e., the necessary SEALDD layer actions for meeting the service policy requirements) has been configured in SEALDD server and shared with the SEALDD client.

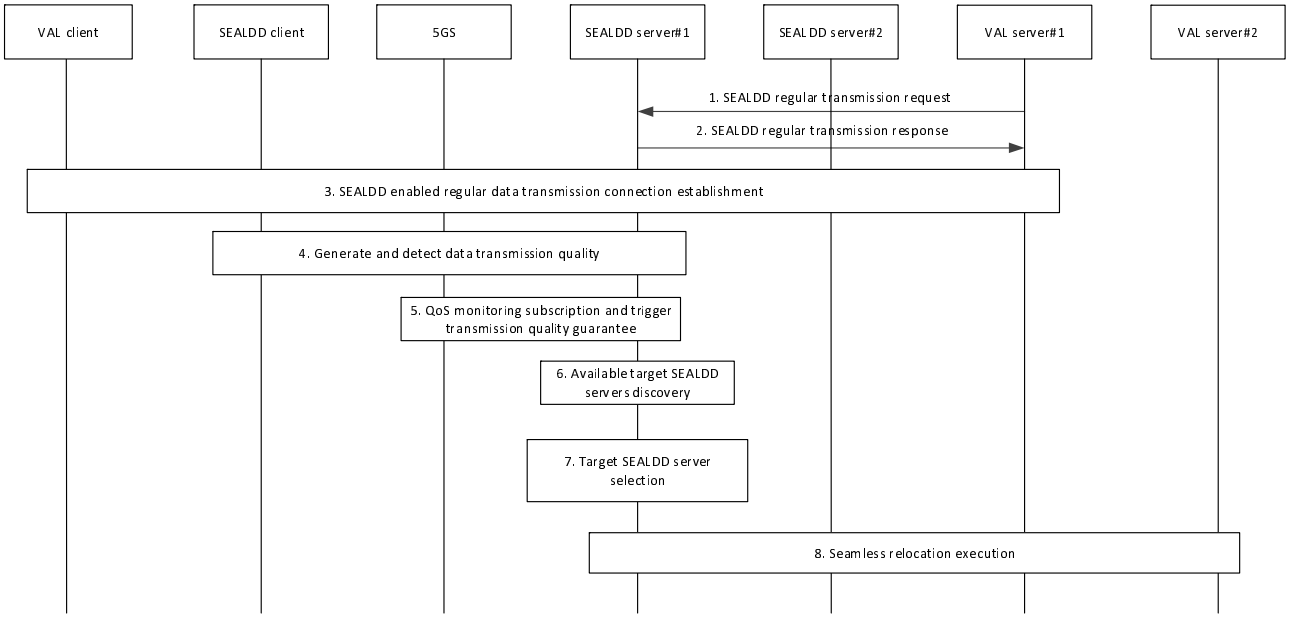

Figure 9.9.2.1-1: SEALDD enabled data transmission quality guarantee procedure by switching SEALDD server

1. The VAL server sends a Sdd_RegularTransmission request to the SEALDD server, as specified in clause 9.2.2.2. The request includes the identifiers of the application traffic (e.g. VAL service ID, VAL server ID), and optionally, the QoS information for the application traffic, e.g. QoS requirements.

2. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, the SEALDD server sends a response to the VAL server. The QoS information may be allocated by SEALDD server according to VAL service ID for different service type of application traffic if the QoS information is not provided by VAL server.

3. The regular data transmission connection is established according to clause 9.2.2.2.

4. The S-SEALDD server (i.e., SEALDD server#1) generates the transmission quality measurement report according to the SEALDD enabled transmission quality measurement procedure in clause 9.7.2.1, and detects whether the current transmission quality satisfies the QoS requirements of VAL application.

5. The S-SEALDD server subscribes to 5GC for QoS monitoring of the specific UE related to the VAL user, as defined in clause 5.2.6.9 in 3GPP TS 23.502 6]. If the S-SEALDD server diagnoses that QoS deterioration is caused by N6/SEALDD overload (i.e., based on QoS monitoring between UE and UPF, and the E2E transmission quality measurement). The S-SEALDD server determines to trigger the data transmission quality guarantee procedure (i.e., switching the connected SEALDD server according to SEALDD service policy) based on the QoS monitoring and E2E transmission quality measurement.

NOTE 1: The QoS monitoring subscription request may be triggered after step 4 when the current transmission quality cannot satisfy the QoS requirements of VAL application.

NOTE 2: This procedure cannot solve the QoS deterioration issue caused by NG-RAN (e.g. RAN congestion).

6. The S-SEALDD server performs target SEALDD server discovery procedure by using EEL, as specified in clause 9.4.

7. The S-SEALDD server selects the T-SEALDD server (i.e., SEALDD server #2) based on N6 traffic and/or SEALDD server load from performance of the available target SEALDD servers in step 6.

8. The SEALDD relocation procedure is performed for the switched SEALDD servers and the switched VAL servers, as specified in clause 9.6.2.2.

   After the SEALDD relocation procedure, the SEALDD client connects to the selected T-SEALDD server to obtain the data transmission quality guarantee service (i.e. the QoS requirements of VAL application is satisfied).

9.9.2.2 SEALDD enabled data transmission quality guarantee with redundant transport

Figure 9.9.2.2-1 illustrates the procedure of using redundant transmission as the action to meet connection reliability requirements specified by a SEALDD service policy.

Pre-conditions:

1. A SEALDD policy, which includes Quality guarantee policy, is available to SEALDD server. The policy is used to configure measurements and determine the necessary SEALDD layer actions for meeting the service policy requirements.

2. The SEALDD Client is authorized to request redundant transport services on behalf of the VAL client.

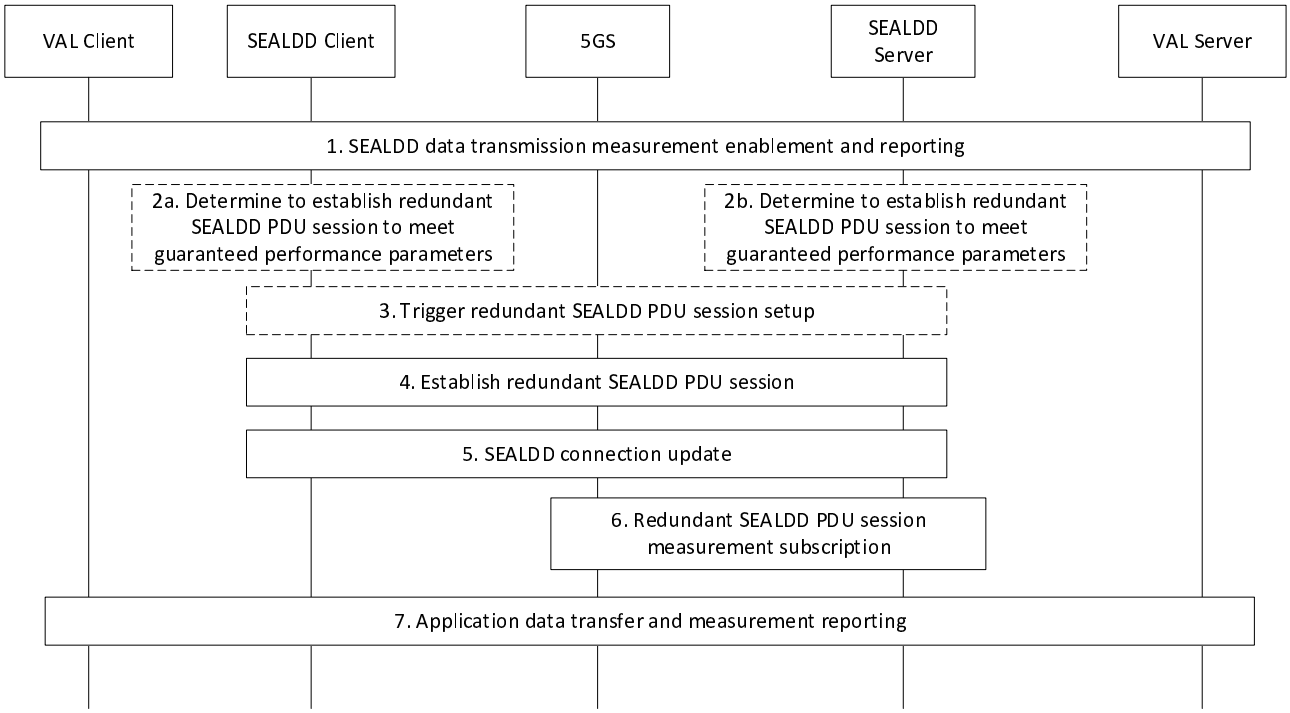

Figure 9.9.2.2-1: SEALDD data transmission quality guarantee with redundant transmission

1. A VAL client and server establish a SEALDD connection to transport the application data. As part of the connection establishment, the SEALDD policy in precondition 1 is shared so that it is available to both the SEALDD client and the SEALDD Server, as defined in clause 9.10.2.4. The SEALDD Server may use the Quality guarantee policy in SEALDD policy in conjunction with other local policies pre-provisioned at the SEALDD server. The SEALDD server determines whether to start data transmission quality measurement by itself or by the SEALDD client. As a result, SEALDD measurements (e.g. packet loss rate, latency) are configured either at the SEALDD client as described in clause 9.7.2.3 or at the SEALDD server as described in clause 9.7.2.1 and started accordingly. Then either the SEALDD client or server receives measurement reports.

2. Based on measurement reports and the SEALDD policy, depending on which entity started the measurement, either the SEALDD client or server determines to perform an action so that the data transmission quality requirements of the policy are met.

3. Specifically, if the measurement was started by the SEALDD client, the SEALDD client triggers the establishment of redundant transmission services. If the measurement was started by the SEALDD server, the SEALDD server triggers the establishment of redundant transmission services by sending a Transmission quality management request to the SEALDD client requesting to establish redundant transmission path.

NOTE: The request can be sent to SEALDD client via Application Triggering (specified in clause 4.13.2 of 3GPP TS 23.502 [6]) with payload indicating a trigger of a redundant connection setup for SEALDD packet transmission.

4. The SEALDD client uses steps 6 to 9 of the procedure in clause 9.3.2.1 to request the use of redundant transmission service from the SEALDD server. As part of this step, the UE may end the initial PDU session and establish redundant PDU sessions.

5. The SEALDD client updates the SEALDD connection with the redundant transmission information, i.e., the UE addresses and ports for the redundant PDU sessions, the SEALDD-UU flow identifier, and the application traffic descriptors. The SEALDD client or server also configures the parameters for enabling any necessary SEALDD measurements for the new SEALDD-UU flow.

6. The SEALDD server may subscribe to receive notifications from the 5G network for user plane measurements (e.g., the network latency requirements specified in 3GPP TS 28.541 [12]), network analytics (as specified in 3GPP TS 28.104 [11], etc.).

7. The SEALDD client and server handle data duplication and elimination of application traffic on the redundant SEALDD-UU flows and the necessary measurements are collected by the SEALDD client or server.

When the SEALDD measurement results indicating that the SEALDD data transmission has good performance according to threshold in Quality guarantee policy, if the measurement was started by the SEALDD client, the SEALDD client may release one transmission path and return back to single SEALDD connection mode, otherwise the SEALDD server may send a Transmission quality management request to the SEALDD client requesting to use single transmission, then the SEALDD client releases one transmission path and returns to single SEALDD connection mode.

9.9.2.3 SEALDD enabled data transmission quality guarantee with BAT and periodicity adaptation

Figure 9.9.2.3-1 illustrates the procedure of using 3GPP CN (5GS) capability for BAT and periodicity report and application layer adjustment in SEALDD layer for data transmission.

Precondition:

- SEALDD layer connection needs to be established as described in clause 9.2 and clause 9.3.
- In policy driven SEALDD connection management, the VAL server has indicated quality optimization policy during SEALDD policy configuration procedure as described in clause 9.10.

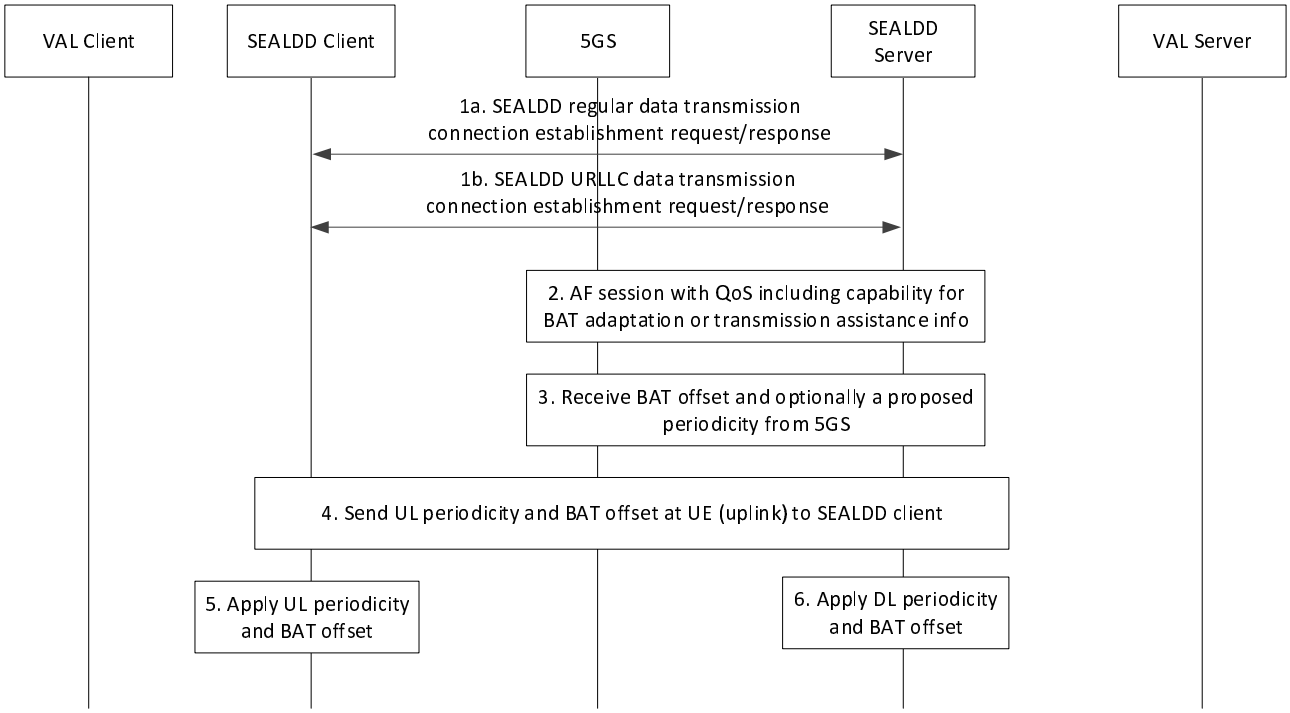

Figure 9.9.2.3-1: SEALDD data transmission quality guarantee with BAT and periodicity adaptation

1. A VAL client and server establish a SEALDD regular or redundant connection to transport the application data as described in clause 9.2 or clause 9.3. The connection establishment may be triggered by either SEALDD

server or SEALDD client. During the connection establishment, the SEALDD client includes an indication for data transmission adjustment request as part of the connection establishment over SEALDD-UU reference point.

In SEALDD-UU connection establishment, the SEALDD client also includes its capability for BAT and periodicity adaptation, or transmission assistance info to the SEALDD server in the connection establishment request (SEALDD client triggered establishment) or response (SEALDD server triggered establishment).

2. The SEALDD server, based on received data transmission adjustment request from VAL server or SEALDD client, its own capability and/or received capability from SEALDD client for BAT and periodicity adaptation, and its own DL transmission assistance info and/or received transmission assistance info from SEALDD client, subscribes to 5GS AF session with QoS service with capability for BAT adaptation or transmission assistance info as described in clause 4.15.6.6 and 4.16.6.4 of 3GPP TS 23.502 [6].
3. The SEALDD server receives BAT offset and optionally a proposed periodicity (which was adjusted in 5GS) in AF session with QoS notification from 5GS.
4. If the SEALDD client indicated its BAT and periodicity adaptation capability in step 1 during SEALDD connection establishment, the SEALDD server sends UL periodicity and BAT window to the SEALDD client in Transmission quality management request with transmission parameter adjustment action.
5. The SEALDD client applies UL periodicity and BAT offset for uplink SEALDD data.
6. The SEALDD server locally applies DL periodicity and BAT offset for downlink SEALDD data.

NOTE: Step 6 can happen before step 5, and step 3 to 6 can be repeated.

9.9.2.4 SEALDD enabled data transmission quality guarantee using Non-3GPP access

Figure 9.9.2.4-1 illustrates the procedure of using non-3gpp access for SEALDD enabled data transmission quality guarantee.

Pre-conditions:

1. The SEALDD Client is authorized to use non-3GPP access on behalf of the VAL client.

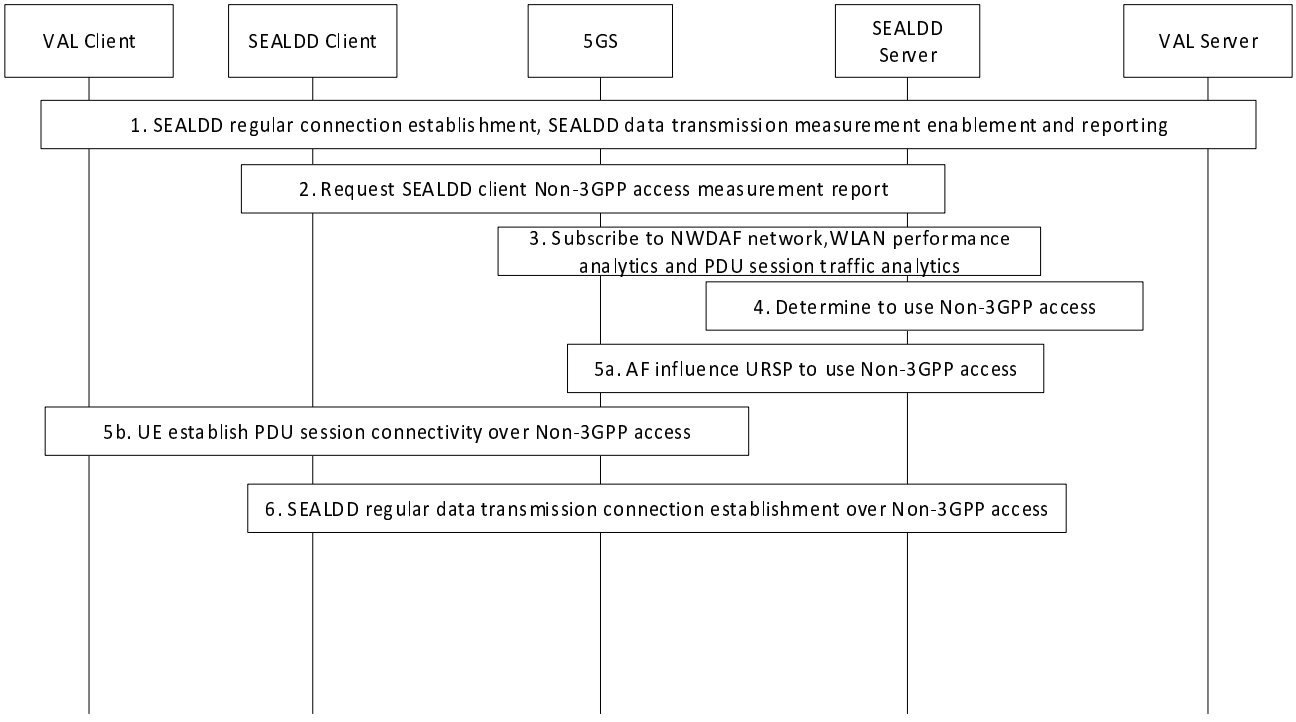

Figure 9.9.2.4-1: SEALDD enabled data transmission quality guarantee using Non-3GPP access

1. A regular data transmission connection is established according to clause 9.2.2.2 or via clause 9.3.2.3 and SEALDD data transmission measurement reporting as per clause 9.7.2.1 or clause 9.7.2.2 to get the data transmission quality.

2. If Non-3GPP access measurement policy is available in the SEALDD server, the SEALDD server requests the SEALDD client to report the latest Non-3GPP access measurements(like RSSI for the WLAN SSIDs) as per steps 3-4 of the procedure defined in clause 9.2.2.6.

   If Non-3GPP access measurement policy is not available, the SEALDD server fetches the UE location using the SEAL location service defined in 3GPP TS 23.434 [4] clause 9.3.12 and requests the SEALDD client to report the latest Non-3GPP access measurements of the nearby WLAN SSIDs. The SEALDD server uses the steps 3-4 of the procedure defined in clause 9.2.2.6 to get the report from the SEALDD client.

   If the Non-3GPP access measurement values in the data transmission quality report or SEALDD connection status report defined in clause 9.2.2.6 are above the Signal strength thresholds mentioned in SEALDD Non-3GPP access measurement policy then the SEALDD server offloads the SEALDD-UU connection from 3GPP access to Non-3GPP access(WLAN) using steps 5-6.

3. The SEALDD server subscribes to NWDAF analytics service for subscription to network performance analytics with Analytics ID as Network Performance using the procedure described in clause 6.6.4 3GPP TS 23.288 [19]. It also subscribes to PDU Session traffic analytics service using the procedure defined in clause 6.20 3GPP TS 23.288 [19].

   The SEALDD server subscribes to WLAN performance analytics using the procedure defined in clause 6.11 3GPP TS 23.288 [19]. The SEALDD server uses the SEALDD Non-3GPP access measurement policy information or information received in step 2 for subscription to WLAN performance analytics.

4. Based on SEALDD client Non-3GPP access measurement reports, NWDAF analytics measurement reports(including predicted values), and data transmission quality measurement reports, the SEALDD server detects the 3GPP RAN congestion and determines to use non-3GPP access to meet the data transmission quality requirements.

5. The SEALDD server requests 5GS to create or update URSP rules using clause 4.15.6.10 of 3GPP TS 23.502 [6] to establish a PDU session connection over Non-3GPP access. The SEALDD server creates a URSP rule with Access Type Route selection descriptors as non-3GPP to establish PDU session. The request may include the UE ID and application traffic descriptor containing the addresses or ports allocated by SEALDD server.

6. The UE receives the new or updated URSP rules from the 5G core network. Based on the URSP rules, the UE establishes a PDU session connectivity over non-3GPP access with the 5GS.

7. On the successful establishment of PDU session connection over Non-3GPP access, the SEALDD client updates the SEALDD data transmission connection with the updated SEALDD client IP address as per steps 7-8 mentioned in clause 9.3.2.2.

Based on continuous monitoring and measurement reports, the SEALDD server decides to switch back to 3GPP access and use the SEALDD-UU connection over 3GPP access for data transmission.

9.9.2.5 SEALDD enabled data transmission quality guarantee to support the user group level QoS

Figure 9.9.2.5-1 illustrates the procedure to support the user group level QoS guarantee. The user group level QoS guarantee provides different QoS for different users in single service(e.g., XR service).

Pre-conditions:

1. The SEALDD server acts as NSaaS provider, and is authorized to get network slice related information and capabilities in Network Slice ServiceProfile (3GPP TS 28.541 [12]) from NSCE server as defined in 3GPP TS 23.435 [21].

2. The SEALDD policy for a group of users has been configured, by providing the VAL UE group ID (as defined in clause 7.5 of 3GPP TS 23.434 [4]), VAL UE identity list, or slice identifier in the SEALDD policy configuration request.

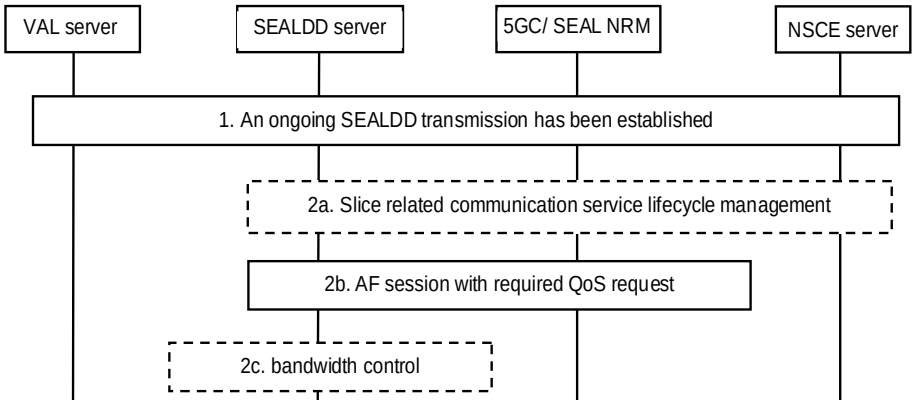

Figure 9.9.2.5-1: procedure of supporting the user group level QoS guarantee

1. The regular data transmission connection is established according to clause 9.2.2.2.

2a. Based on the configured SEALDD policy and network slice related information received from NSCE, the SEALDD server determines whether the slice related communication service lifecycle management is needed, based on Network slice information, e.g., Slice Coverage Area, Latency, and, Data volume, which specify the Network Slice characteristics, as specified in clause of ServiceProfile in 3GPP TS 28.541 [12]. If the performance of network slice identified by the provided Slice identifier is not satisfying, the SEALDD server could trigger slice related communication service Reconfiguration.

If the network slice related information of network slice identified by the provided Slice identifier is not received from NSCE before, the SEALDD server obtains the Network slice information by invoking the Network Slice Information delivery as defined in 3GPP TS 23.435 [21], clause 9.17.

Before triggering the network slice management service, to determine the target UE of network slice(s), the SEALDD server acting as AF, may receive a UE location report or a monitoring event report from 5GC (assuming that SEALDD server has subscribed to consume 5GC services like LCS or NEF monitoring events related to UE actual location, or UE mobility analytics from NWDAF) or Location service from SEAL.

2b. Based on the configured SEALDD policy, the SEALDD server initiates AF session with required QoS as defined in 3GPP TS 23.502 [6], clause 4.15.6.6a, or Multi-member AF session with required QoS as defined in 3GPP TS 23.502 [6], clause 4.16.5.3, or QoS/resource management capability provided by SEAL NRM as defined in 3GPP TS 23.434 [4], clause 14.3.5.2.

2c. Based on the configured SEALDD policy, the SEALDD server determines whether the SEALDD enabled bandwidth control is needed. If needed(e.g., multiple user groups have different bandwidth requirements), the SEALDD server may initiate the SEALDD enabled bandwidth control for different VAL users as defined in 3GPP TS23.433, clause 9.8.2.

9.9.3 Information flows

9.9.3.1 Transmission quality management request

Table 9.9.3.1-1 describes the information flow from the SEALDD server to the SEALDD client for requesting data transmission quality management.

Table 9.9.3.1-1: Transmission quality management request

Information element	Status	Description
SEALDD-UU flow ID	M	Identifier of the SEALDD-UU flow.
Transmission quality management action	M	Indicates the data transmission quality guarantee action (e.g. redundant transmission path, re-establish transmission path, switch to backup transmission path) or optimization action (back to single transmission path, transmission parameter adjustment) that triggering by event (e.g. measurement threshold).
UL periodicity (NOTE)	O	Uplink periodicity.
BAT offset for UL (NOTE)	O	BAT offset for Uplink data.
NOTE: The IE is applicable for transmission parameter adjustment.		

NOTE: The triggering event (e.g. measurement threshold) is changeable with the transmission quality guarantee event.

9.9.3.2 Transmission quality management response

Table 9.9.3.2-1 describes the information flow from the SEALDD client to the SEALDD server for responding to the transmission quality management request.

Table 9.9.3.2-1: Transmission quality management response

Information element	Status	Description
Result	M	Success or failure.

9.9.4 APIs

9.9.4.1 General

Table 9.9.4.1-1 illustrates the APIs exposed by SEALDD client for data transmission quality management.

Table 9.9.4.1-1: API list for transmission quality management

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_TransmissionQuality Management	Request	Request/Response	SEALDD server

9.9.4.2 Sdd_TransmissionQualityManagement Request operation

API operation name: Sdd_TransmissionQualityManagement Request

Description: The consumer requests for one time for transmission quality management.

Inputs: See clause 9.9.3.1.

Outputs: See clause 9.9.3.2

See clause 9.9.2.2 for details of usage of this operation.

9.10 SEALDD policy configuration

9.10.1 General

The following clauses specify procedures, information flow for SEALDD policy configuration. In clause 9.10, the VAL server is a specific server for configurating SEALDD policy, and is different from the VAL server used for VAL application processing in other clauses.

Depending on the configuration, a SEALDD policy may apply to individual SEALDD flows or to multi-modal SEALDD flows.

9.10.2 Procedures

9.10.2.1 SEALDD policy configuration

Figure 9.10.2.1-1 illustrates the procedure for SEALDD policy configuration from the VAL server used for SEALDD policy configuration to the SEALDD server.

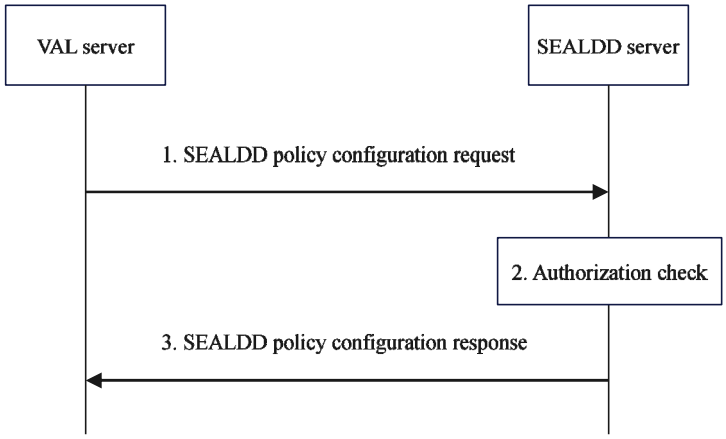

Figure 9.10.2.1-1: SEALDD policy configuration

1. The VAL server sends the SEALDD policy configuration request to the SEALDD server. The request includes the identifiers of the application traffic (e.g. VAL service ID, VAL server ID), VAL UE identify, and the SEALDD policy.
2. The SEALDD server performs authorization check to verify whether the VAL server is accepted/authorized to configure the SEALDD policy.
3. Upon successful authorization, the SEALDD server stores the SEALDD policy for later use (e.g. for bandwidth control, transmission quality guarantee) and replies to the VAL server with the SEALDD policy configuration response.

9.10.2.2 SEALDD policy configuration update

Figure 9.10.2.2-1 illustrates the procedure for SEALDD policy configuration update from the VAL server used for SEALDD policy configuration to the SEALDD server.

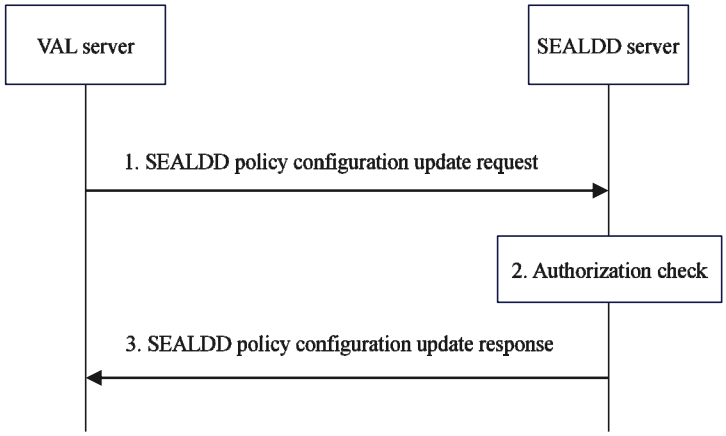

Figure 9.10.2.2-1: SEALDD policy configuration update

1. The VAL server used for SEALDD policy configuration determines that the existing SEALDD policy needs to be updated, the VAL server sends the SEALDD policy configuration update request to the SEALDD server.
2. The SEALDD server performs authorization check to verify whether the VAL server is accepted/authorized to update the SEALDD policy configuration.
3. Upon successful authorization, the SEALDD server updates the SEALDD policy configuration and replies to the VAL server with the SEALDD policy configuration update response.

9.10.2.3 SEALDD policy configuration delete

Figure 9.10.2.3-1 illustrates the procedure for SEALDD policy configuration delete from the VAL server used for SEALDD policy configuration to the SEALDD server.

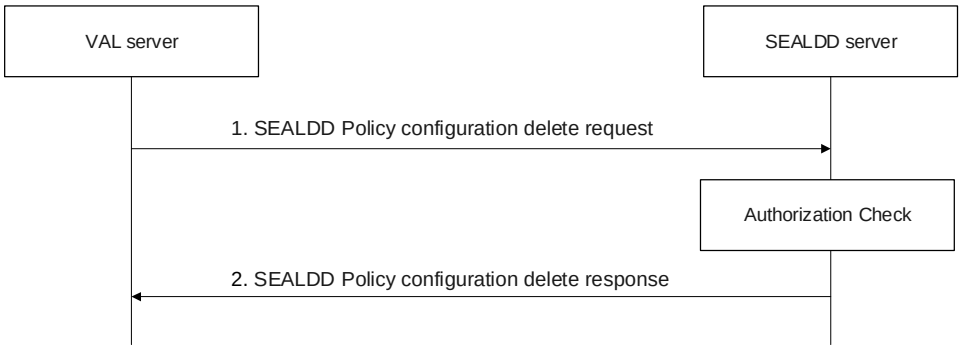

Figure 9.10.2.3-1: SEALDD policy configuration delete

1. The VAL server used for SEALDD policy configuration determines that the existing SEALDD policy needs to be deleted, the VAL server sends the SEALDD policy configuration delete request to the SEALDD server.
2. The SEALDD server performs authorization check to verify whether the VAL server is accepted/authorized to delete the SEALDD policy configuration.

3. Upon successful authorization, the SEALDD server deletes the SEALDD policy configuration and replies to the VAL server with the SEALDD policy configuration update response.

9.10.2.4 SEALDD client policy configuration request

Figure 9.10.2.4-1 illustrates the procedure for SEALDD client policy configuration request from the SEALDD server to the SEALDD client.

Pre-condition:

1. The SEALDD connectivity has been established between the SEALDD client and SEALDD server.

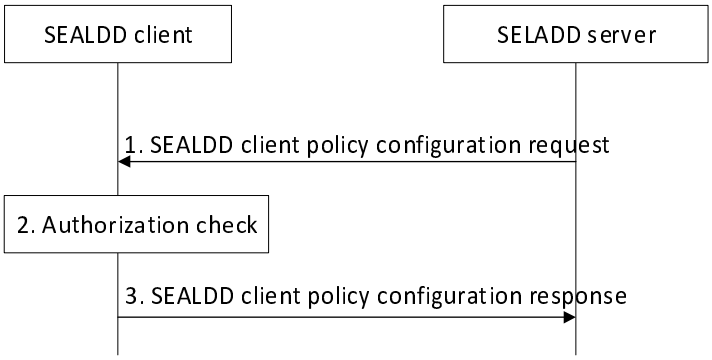

Figure 9.10.2.4-1: SEALDD client policy configuration request

1. Based on policy received from the VAL server(e.g., Multi-modal flows alignment policy), or SEALDD server determines that the policy needs to be configured to the SEALDD client, the SEALDD server sends the SEALDD client policy configuration request to the SEALDD client.
2. The SEALDD client performs authorization check to verify whether the SEALDD server is authorized to configure the SEALDD client policy.
3. Upon successful authorization, the SEALDD server stores the SEALDD client policy for later use (e.g. for multi-modal flows alignment) and replies to the SEALDD server with the SEALDD client policy configuration response.

9.10.2.5 SEALDD client policy configuration update request

Figure 9.10.2.5-1 illustrates the procedure for SEALDD client policy configuration update request from the SEALDD server to the SEALDD client.

Pre-condition:

1. The SEALDD connectivity has been established between the SEALDD client and SEALDD server.

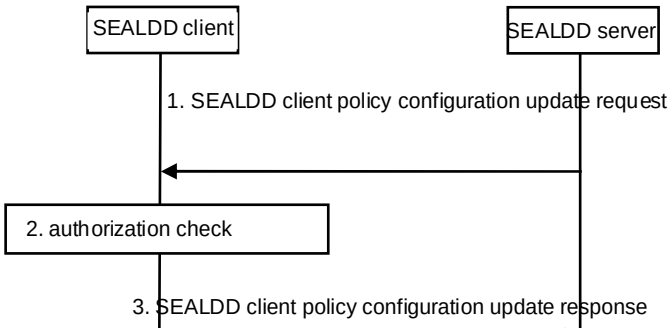

Figure 9.10.2.5-1: SEALDD client policy configuration update request

1. Based on policy received from the VAL server, or SEALDD server determines that the policy needs to be updated to the SEALDD client, the SEALDD server sends the SEALDD client policy configuration update request to the SEALDD client.
2. The SEALDD client performs authorization check to verify whether the SEALDD server can be authorized to update the SEALDD client policy.
3. Upon successful authorization, the SEALDD client updates the SEALDD client policy and replies to the SEALDD server with the SEALDD client policy configuration update response.

9.10.2.6 SEALDD client policy configuration delete request

Figure 9.10.2.6-1 illustrates the procedure for SEALDD client policy configuration delete request from the SEALDD server to the SEALDD client.

Pre-condition:

1. The SEALDD connectivity has been established between the SEALDD client and SEALDD server.

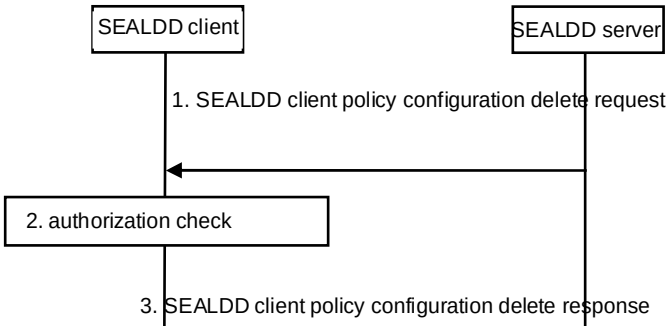

Figure 9.10.2.6-1: SEALDD client policy configuration delete request

1. Based on request received from the VAL server, or SEALDD server determines that the policy needs to be deleted, the SEALDD server sends the SEALDD client policy configuration delete request to the SEALDD client.
2. The SEALDD client performs authorization check to verify whether the SEALDD server can be authorized to delete the SEALDD client policy.
3. Upon successful authorization, the SEALDD client deletes the SEALDD client policy and replies to the SEALDD server with the SEALDD client policy configuration delete response.

9.10.3 Information flows

9.10.3.1 SEALDD policy configuration request

Table 9.10.3.1-1 describes the information flow from the VAL server to the SEALDD server for requesting the SEALDD policy configuration.

Table 9.10.3.1-1: SEALDD policy configuration request

Information element	Status	Description
Application traffic identifiers	M	Identify of the application traffic (e.g. VAL server ID, VAL service ID).
Identities	O	Identifier of the VAL UEs or VAL users, or VAL UE group ID(as defined in clause 7.5 of 3GPP TS 23.434 [4]), or VAL UE identity list for which SEALDD policy applies.
Slice identifier	O	The slice identifier (S-NSSAI) for which SEALDD policy applies.
SEALDD policy	O (See NOTE 4)	The SEALDD policy associated with application traffic identifiers, VAL UE identity.
> Quality guarantee policy	O (See NOTE 1)	Indicates the event (e.g. measurement threshold) to be measured for the quality guarantee
> Quality optimization policy	O (See NOTE 1)	Indicates the data transmission adjustment policy (e.g., adjustment need) to be performed in SEALDD layer.
> Bandwidth control policy	O (See NOTE 2)	Indicate the bandwidth control preference, e.g. re-allocating the bandwidth limit between different VAL users, including UL/DL.
> Geofence policy	O (See NOTE 3)	Indicates the geofence policy per VAL service.
>> Geofence location	O (See NOTE 3)	Indicates the geofence location information for the mentioned VAL service.
>>Geofence policy action	O (See NOTE 3)	Indicates the policy action like allowed or blocked.
> temporal policy	O (See NOTE 3)	Indicates the time period for which the sealdd traffic is allowed.
> policy expiration time	O	Indicates the validity of the policy.
> Non-3GPP access measurement policy	O	Indicates the non-3GPP access (like WLAN) measurement policy (e.g. WLAN SSIDs/BSSID, signal strength thresholds(high/low), time-based threshold for offload to WLAN).
Multi-modal SEALDD policy	O (See NOTE 4)	Multi-modal SEALDD policy associated with set of individual SEALDD flows.
> Synchronization policy	O	Indicates the synchronization threshold for multi-modal application, as specified in 3GPP TS 22.261 [2].
> Multi-modal flows alignment policy	O	Indicates the information to do the multi-modal flows alignment, e.g., Multi-modal Service ID, maximum acceptable duration for traffic flow alignment.
> Policy expiration time	O	Indicates the validity period of the policy.
> UE-to-UE policy	O	Specifies UE-to-UE direct communication policy including proximity threshold, QoS threshold (e.g. bitrate, latency and jitter, PLR, PER) or QoE threshold (e.g. MOS as specified in ITU-T P.1203.3 [18]) for entering direct communication mode, and proximity threshold, QoS threshold or QoE threshold for leaving direct communication mode.
NOTE 1: This IE is used for the SEALDD enabled transmission quality guarantee, as specified in clause 9.9. NOTE 2: This IE is used for the SEALDD enabled bandwidth control, as specified in clause 9.8. NOTE 3: This IE is used for the SEALDD connection establishment and data delivery, as specified in clause 9.2 NOTE 4: At least one of these IEs shall be present.		

9.10.3.2 SEALDD policy configuration response

Table 9.10.3.2-1 describes the information flow from the SEALDD server to the VAL server for responding to the SEALDD policy configuration.

Table 9.10.3.2-1: SEALDD policy configuration response

Information element	Status	Description
Result	M	Success or failure.
> Configuration ID	O (See NOTE)	Identifier of the SEALDD policy configuration.
> Expiration time	O (See NOTE)	Indicates the expiration time of the configured SEALDD policy
NOTE: These IEs are used for the successful case for SEALDD policy configuration request.		

9.10.3.3 SEALDD policy configuration update request

Table 9.10.3.3-1 describes the information flow from the VAL server to the SEALDD server for requesting the SEALDD policy configuration update.

Table 9.10.3.3-1: SEALDD policy configuration update request

Information element	Status	Description
Configuration ID	M	Identifier of the SEALDD policy configuration.
Updated SEALDD policy	O	The updated SEALDD policy as described in Table 9.10.3.1-1.

9.10.3.4 SEALDD policy configuration update response

Table 9.10.3.4-1 describes the information flow from the SEALDD server to the VAL server for responding to the SEALDD policy configuration update.

Table 9.10.3.4-1: SEALDD policy configuration update response

Information element	Status	Description
Result	M	Success or failure.
> Expiration time	O (See NOTE)	Indicates the expiration time of the configured SEALDD policy
NOTE: This IEs is used for the successful case for SEALDD policy configuration update request.		

9.10.3.5 SEALDD policy configuration delete request

Table 9.10.3.5-1 describes the information flow from the VAL server to the SEALDD server for requesting the SEALDD policy configuration delete.

Table 9.10.3.5-1: SEALDD policy configuration delete request

Information element	Status	Description
Configuration ID	M	Identifier of the SEALDD policy configuration.

9.10.3.6 SEALDD policy configuration delete response

Table 9.10.3.6-1 describes the information flow from the SEALDD server to the VAL server for responding to the SEALDD policy configuration delete.

Table 9.10.3.6-1: SEALDD policy configuration delete response

Information element	Status	Description
Result	M	Success or failure.

9.10.3.7 SEALDD client policy configuration request

Table 9.10.3.7-1 describes the information flow from the SEALDD server to the SEALDD client for requesting SEALDD client policy configuration.

Table 9.10.3.7-1: SEALDD client policy configuration request

Information element	Status	Description
Requestor ID	M	Identity of the requestor
SEALDD-UU flow list	O (NOTE)	Indicates the list of SEALDD-UU flows.
> SEALDD-UU flow ID	O	Identity of the SEALDD-UU flow.
Multi-modal SEALDD flow ID	O (NOTE)	Identity of the multi-modal SEALDD flows associated with the SEALDD multi-modal connection
VAL service ID	M	Identity of the VAL service
UE ID	O	Identifier of specific UE or VAL user
>Configuration ID	M	Identifier of the SEALDD policy configuration.
Multi-modal flows alignment policy	O	Multi-modal flows alignment Policy
>Multi-modal Service ID	O	Identifier of Multi-modal Service
>Flows transmission requirement	O	Flows transmission requirement including the delay requirement, maximum acceptable duration for traffic flow alignment. Maximum acceptable time duration for traffic flow alignment is used to limit the maximum waiting time. for the associated flow
SEALDD UE-to-UE policy	O	Specifies UE-to-UE direct communication policy including, QoS threshold (e.g. bitrate, latency and jitter, PLR, PER) for entering direct communication mode, and QoS threshold for leaving direct communication mode.
NOTE: At least one of these IEs shall be present in the message.		

9.10.3.8 SEALDD client policy configuration response

Table 9.10.3.8-1 describes the information flow from the SEALDD server to the VAL server for response SEALDD client policy configuration.

Table 9.10.3.8-1: SEALDD client policy configuration response

Information element	Status	Description
Result	M	Success or failure of the request.
Configuration ID	M	Identifier of the SEALDD client policy.

9.10.3.9 SEALDD client policy configuration update request

Table 9.10.3.9-1 describes the information flow from the SEALDD server to the SEALDD client for requesting SEALDD client policy configuration update.

Table 9.10.3.9-1: SEALDD client policy configuration update request

Information element	Status	Description
Configuration ID	M	Identifier of the SEALDD client policy.
Updated SEALDD client policy	O	The updated SEALDD client policy.

9.10.3.10 SEALDD client policy configuration update response

Table 9.10.3.10-1 describes the information flow from the SEALDD server to the VAL server for response SEALDD client configuration policy update.

Table 9.10.3.10-1: SEALDD client policy configuration update response

Information element	Status	Description
Result	M	Success or failure of the request.
Configuration ID	M	Identifier of the SEALDD client policy.

9.10.3.11 SEALDD client policy configuration delete request

Table 9.10.3.11-1 describes the information flow from the SEALDD server to the SEALDD client for requesting SEALDD client policy configuration delete.

Table 9.10.3.11-1: SEALDD client policy configuration delete request

Information element	Status	Description
Configuration ID	M	Identity of the SEALDD client policy.

9.10.3.12 SEALDD client policy configuration delete response

Table 9.10.3.12-1 describes the information flow from the SEALDD server to the VAL server for response SEALDD client policy Configuration delete.

Table 9.10.3.12-1: SEALDD client policy configuration delete response

Information element	Status	Description
Result	M	Success or failure of the request.
Configuration ID	M	Identifier of the SEALDD client policy.

9.10.4 APIs

9.10.4.1 General

Table 9.10.4.1-1 illustrates the APIs exposed by SEALDD server for SEALDD policy configuration.

Table 9.10.4.1-1: List of SEALDD server APIs for policy configuration

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_PolicyConfiguration	Request	Request/Response	VAL server
	Update		
	Delete		
Sdd_ClientPolicyConfiguration	Request	Request/Response	SEALDD server
	Update		
	Delete		

9.10.4.2 Sdd_PolicyConfiguration operation

API operation name: Sdd_PolicyConfiguration_Request

Description: The consumer requests for one time for SEALDD policy configuration.

Inputs: See clause 9.10.3.1.

Outputs: See clause 9.10.3.2.

See clause 9.10.2.1 for details of usage of this operation.

9.10.4.3 Sdd_PolicyConfiguration update operation

API operation name: Sdd_PolicyConfiguration_Update

Description: The consumer requests for one time for SEALDD policy configuration update.

Inputs: See clause 9.10.3.3.

Outputs: See clause 9.10.3.4.

See clause 9.10.2.2 for details of usage of this operation.

9.10.4.4 Sdd_PolicyConfiguration delete operation

API operation name: Sdd_PolicyConfiguration_Delete

Description: The consumer requests for one time for SEALDD policy configuration deletion.

Inputs: See clause 9.10.3.5.

Outputs: See clause 9.10.3.6.

See clause 9.10.2.3 for details of the usage of this operation.

9.10.4.5 Sdd_ClientPolicyConfiguration operation

API operation name: Sdd_ClientPolicyConfiguration_Request

Description: The consumer requests for one time for SEALDD Client policy configuration.

Inputs: See clause 9.10.3.7.

Outputs: See clause 9.10.3.8.

See clause 9.10.2.4 for details of the usage of this operation.

9.10.4.6 Sdd_ClientPolicyConfiguration_Update operation

API operation name: Sdd_ClientPolicyConfiguration_Update

Description: The consumer requests for SEALDD Client policy configuration update.

Inputs: See clause 9.10.3.9.

Outputs: See clause 9.10.3.10.

See clause 9.10.2.5 for details of the usage of this operation.

9.10.4.7 Sdd_ClientPolicyConfiguration_Delete operation

API operation name: Sdd_ClientPolicyConfiguration_Delete

Description: The consumer requests for SEALDD Client policy configuration delete.

Inputs: See clause 9.10.3.11.

Outputs: See clause 9.10.3.12.

See clause 9.10.2.6 for details of the usage of this operation.

9.11 SEALDD Background data transfer

9.11.1 General

The following clauses specify procedures and information flow for SEALDD Background data transfer (BDT). The SEALDD supports BDT in downlink (DL) centric direction, e.g., streaming a video clip to the VAL client, and in uplink (UL) centric direction, e.g., uploading drone captured data to the VAL server.

9.11.2 Procedures

9.11.2.1 SEALDD background data transfer subscription

Figure 9.11.2.1-1 illustrates the procedure for SEALDD background data transfer subscription.

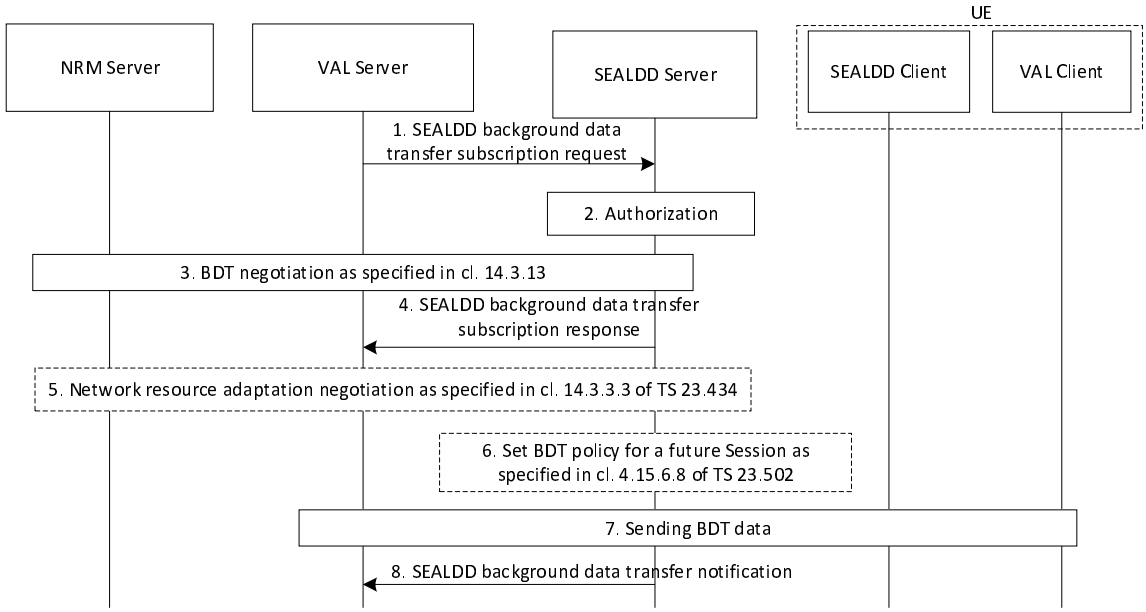

Figure 9.11.2.1-1: SEALDD background data transfer

1. The VAL server sends a SEALDD background data transfer subscription request to the SEALDD server. The request includes the VAL service ID, a list of VAL UE IDs or VAL group ID, the data volume per UE and may also include the desired time window, the desired area information (e.g., when a UE enters a geographical area), Policy Selection Guidance.

2. The SEALDD server authorizes the request from the VAL server.

3. The SEALDD server starts the BDT configuration negotiation with the SEAL NRM server as described in clause 14.3.13 of 3GPP TS 23.434 [4].

NOTE: If the NRM server is an external control plane functionality for the SEALDD server, then the SEALDD server uses step 3, otherwise SEALDD server can use procedure defined in 3GPP TS 23.502 [6] clause 4.16.7.2.

4. The SEALDD server sends the SEALDD background data transfer subscription response, containing the result of the operation which includes the result and may include the BDT subscription identifier.

5. If the SEALDD server determines that the negotiated BDT policy applies to ongoing sessions, the SEALDD server performs Network resource adaptation negotiation with the SEAL NRM server as described in clause 14.3.3.3 of 3GPP TS 23.434 [4]. Policies are set for the BDT data transfer using the previously negotiated BDT Reference ID. This step may be performed simultaneously with step 7.

6. If the SEALDD server determines that the negotiated BDT policy applies to future sessions, the SEALDD server performs the Set BDT policy for future sessions as specified in clause 4.15.6.8 of 3GPP TS 23.502 [6].

7. The VAL server uses clause 9.5.2 procedure to send the BDT data to the SEALDD server for DL centric direction. During the negotiated transmission time window, the SEALDD server sends the BDT data to SEALDD client(s) and monitors the quality, e.g., latency, jitter, bitrate, packet loss rate, of the transmission. The SEALDD client forwards the BDT data received to the VAL client.

   Equivalently, for UL centric direction, during the negotiated transmission window, the SEALDD client(s) sends the BDT data to the SEALDD server. The SEALDD server forwards the BDT data received to the VAL server.

8. The SEALDD server may notify the VAL server about:

i. the delivery result, by sending the SEALDD background data transfer notification including the BDT subscription identifier and optionally the list of VAL UEs which received/sent the BDT data, the executed time window and quality of the BDT data transmission based on the measurements in step 5; or.

ii. the renogiated granted time window or the removal of BDT policy, if there is any change in the network impacting the current BDT policy and the SEAL NRM server performs BDT policy re-selection as described in clause 14.3.13.3 of 3GPP TS 23.434 [4].

9.11.2.2 SEALDD background data transfer subscription update

Figure 9.11.2.2-1 illustrates the procedure for SEALDD background data transfer subscription update from VAL server to the SEALDD server.

Pre-condition:

- The SEALDD background data transfer subscription procedure has been performed.

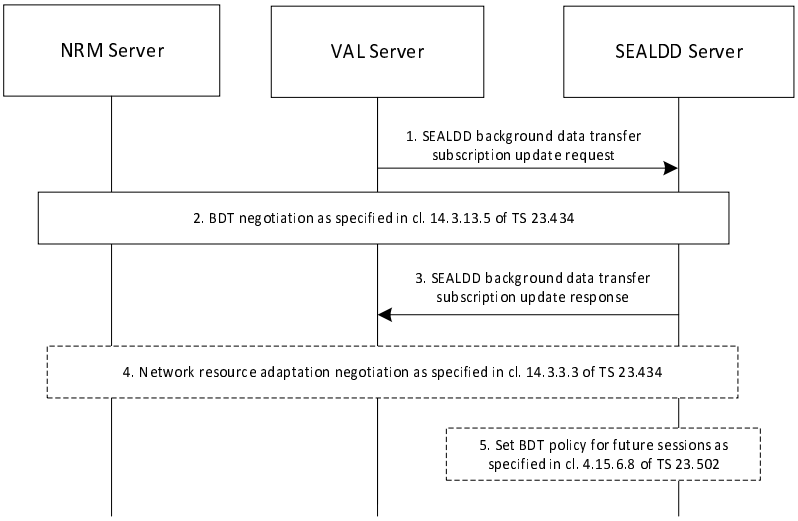

Figure 9.11.2.2-1: SEALDD background data transfer subscription update

1. The VAL server initiates a BDT update by sending a SEALDD background data transfer subscription update request. The request contains BDT subscription identifier and may contain e.g. updated desired time window, desired area information, Policy Selection Guidance, updated data volume per UE.

2. The SEALDD server starts a new BDT configuration negotiation with the SEAL NRM server as described in clause 14.3.13.5 of 3GPP TS 23.434 [4].

NOTE: If the NRM server is an external control plane functionality for the SEALDD server, then the SEALDD server uses step 3 otherwise SEALDD server can directly use procedure defined in 3GPP TS 23.502 [6] clause 4.16.7.2

3. The SEALDD server sends the SEALDD background data transfer subscription update response to the VAL server, containing result and the BDT subscription identifier, and, if updated, the granted time window.

4. If the SEALDD server determines that the negotiated BDT policy applies to ongoing sessions, the SEALDD may perform Network resource adaptation negotiation with the SEAL NRM server as described in clause 14.3.3.3 of 3GPP TS 23.434 [4] for the updated BDT subscription. This step may occur simultaneously with the delivery of the BDT data.

5. If the SEALDD server determines that the negotiated BDT policy applies to future sessions, the SEALDD server may perform the Set BDT policy for future sessions as specified in clause 4.15.6.8 of 3GPP TS 23.502 [6].

9.11.2.3 SEALDD background data transfer unsubscribe

Figure 9.11.2.3-1 illustrates the procedure for SEALDD background data transfer unsubscription from the VAL server to the SEALDD server.

Pre-condition:

- The SEALDD background data transfer subscription procedure has been performed.

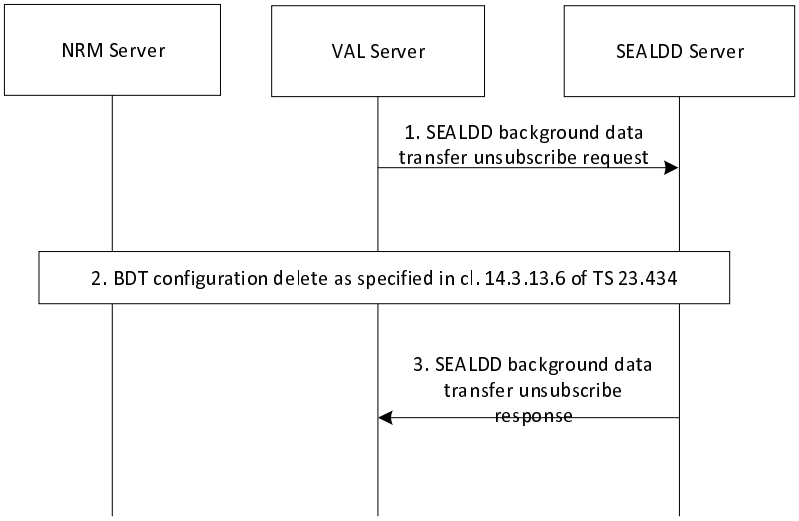

Figure 9.11.2.3-1: SEALDD background data transfer unsubscribe

1. The VAL server may trigger a BDT deletion by sending a SEALDD background data transfer unsubscribe request to the SEALDD server. The request contains the BDT subscription identifier.
2. The SEALDD server requests the deletion of the BDT configuration to the SEAL NRM server as described in clause 14.3.13.6 of TS 23.434 [4] and deletes any stored application data related to the BDT subscription identifier.
3. The SEALDD server sends the SEALDD background data transfer unsubscribe response to the VAL server, containing result of the operation.

9.11.3 Information flows

9.11.3.1 SEALDD background data transfer subscription request

Table 9.11.3.1-1 describes the information flow from the VAL server to the SEALDD server for requesting the SEALDD background data transfer request.

Table 9.11.3.1-1: SEALDD background data transfer subscription request

Information element	Status	Description
VAL service ID	M	Identity of the VAL service for which the background data transfer is requested.
List of VAL UE IDs	O (See NOTE)	List of VAL UE IDs for which the transfer policy applies.
VAL group ID	O (See NOTE)	VAL group ID for which the transfer policy applies.
Desired time window	O	Desired time window for the background data transfer.
Data volume per UE	M	Expected data volume for the background data transfer.
Desired area information	O	Desired geographical area for the background data transfer.
Policy Selection Guidance	O	List that includes guidance 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, local and ASP-provided policies decide one among multiple transfer policies.
NOTE: One of these IEs shall be present in the message.		

9.11.3.2 SEALDD background data transfer subscription response

Table 9.11.3.2-1 describes the information flow from the SEALDD server to the VAL server.

Table 9.11.3.2-1: SEALDD background data transfer subscription response

Information element	Status	Description
Result	M	The result indicates success or failure.
subscription identifier	O	Indicates the background data transfer subscription identifier. Applicable for successful result.
Granted time window	O	Granted time window for the background data transfer. Applicable for successful result.

9.11.3.3 SEALDD background data transfer notification

Table 9.11.3.2-1 describes the information flow from the SEALDD server to the VAL server.

Table 9.11.3.3-1: SEALDD background data transfer notification

Information element	Status	Description
subscription identifier	M	Indicates the background data transfer subscription identifier
List of VAL UE IDs	O	List of VAL UE IDs or VAL group ID.
Executed time window	O	The actual time window the BDT data was transferred.
Granted time window	O	If BDT renegotiation takes place, and the previously provided granted time window changed, the current granted time window for the background data transfer.
BDT transmission quality	O	Indicates the transmission quality (e.g., QoE) when transferring the BDT data between SEALDD client and SEALDD server.

9.11.3.4 SEALDD background data transfer update subscription request

Table 9.11.3.4-1 describes the information flow from the VAL server to the SEALDD server for sending the SEALDD background data transfer update subscription request.

Table 9.11.3.4-1: SEALDD background data transfer update subscription request

Information element	Status	Description
subscription identifier	M	Indicates the background data transfer subscription identifier.
Desired time window	O (See NOTE)	Desired time window for the background data transfer.
Desired area information	O (See NOTE)	Desired geographical area for the background data transfer.
Policy Selection Guidance	O (See NOTE)	List that includes guidance in selecting from multiple transfer policies provided by underlying network. Possible values include: ”lowest cost”, “highest throughput given maximum cost of X”, etc.
Data volume per UE	O (See NOTE)	Updated expected data volume for the background data transfer.
NOTE: At least one of these IEs shall be present in the message.		

9.11.3.5 SEALDD background data transfer update subscription response

Table 9.11.3.5-1 describes the information flow from the SEALDD server to the VAL server for responding to the SEALDD background data transfer update subscription request.

Table 9.11.3.5-1: SEALDD background data transfer update subscription response

Information element	Status	Description
Result	M	The result indicates success or failure.
Subscription identifier	O	Indicates the background data transfer subscription identifier. Applicable for successful result.
Granted time window	O	Granted time window for the background data transfer. Applicable for successful result.

9.11.3.6 SEALDD background data transfer unsubscribe request

Table 9.11.3.6-1 describes the information flow from the VAL server to the SEALDD server for requesting the SEALDD background data transfer unsubscribe request.

Table 9.11.3.6-1: SEALDD background data transfer unsubscribe request

Information element	Status	Description
subscription identifier	M	Indicates the background data transfer subscription identifier.

9.11.3.7 SEALDD background data transfer unsubscribe response

Table 9.11.3.7-1 describes the information flow from the SEALDD server to the VAL server for responding to the SEALDD background data transfer unsubscribe response.

Table 9.11.3.7-1: SEALDD background data transfer unsubscribe response

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

9.11.4 APIs

9.11.4.1 General

Table 9.11.4.1-1 illustrates the APIs exposed by SEALDD server for background data transfer.

Table 9.11.4.1-1: List of SEALDD server APIs for background data transfer

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_BDT	Subscribe	Subscribe/Notify	VAL server
	Notify	Subscribe/Notify	VAL server
	Update	Subscribe/Notify	VAL server
	Unsubscribe	Subscribe/Notify	VAL server

9.11.4.2 Sdd_BDT_Subscribe operation

API operation name: Sdd_BDT_Subscribe

Description: The consumer requests for a background data transfer service.

Inputs: See clause 9.11.3.1.

Outputs: See clause 9.11.3.2.

See clause 9.11.2.1 for details of usage of this operation.

9.11.4.3 Sdd_BDT_Notify operation

API operation name: Sdd_BDT_Notify

Description: The consumer is notified with background data transfer result.

Inputs: See clause 9.11.3.3.

Outputs: None.

See clause 9.11.2.1 for details of usage of this operation.

9.11.4.4 Sdd_BDT_Update operation

API operation name: Sdd_BDT_Update

Description: The consumer requests to update the SEALDD background data transfer service.

Inputs: See clause 9.11.3.4.

Outputs: See clause 9.11.3.5.

See clause 9.11.2.2 for details of usage of this operation.

9.11.4.5 Sdd_BDT_Unsubscribe operation

API operation name: Sdd_BDT_Unsubscribe

Description: The consumer requests to unsubscribe the SEALDD background data transfer service.

Inputs: See clause 9.11.3.6.

Outputs: See clause 9.11.3.7.

See clause 9.11.2.3 for details of usage of this operation.

9.12 SEALDD enabled transmission for XR application

9.12.1 General

This clause provides the services to support the transmission for XR application based on SEALDD capabilities.

9.12.2 Procedures

9.12.2.1 SEALDD enabled multi-modal data transmission service for multi-modal application

9.12.2.1.1 General

The following clauses specify procedures, information flows and APIs about SEALDD enabled data transmission for multi-modal application, including the SEALDD facilate PDU set handling.

9.12.2.1.2 SEALDD enabled multi-modal data transmission establishment

Figure 9.12.2.1.2-1 illustrate the procedure for establishing multi-modal data transmission connection, and the SEALDD facilitates the multi-modal application to transmit its data between the VAL client and VAL server with RTP packetilization and PDU set inclusion.

Pre-condition:

- The VAL server has discovered and selected the SEALDD server by CAPIF functions.

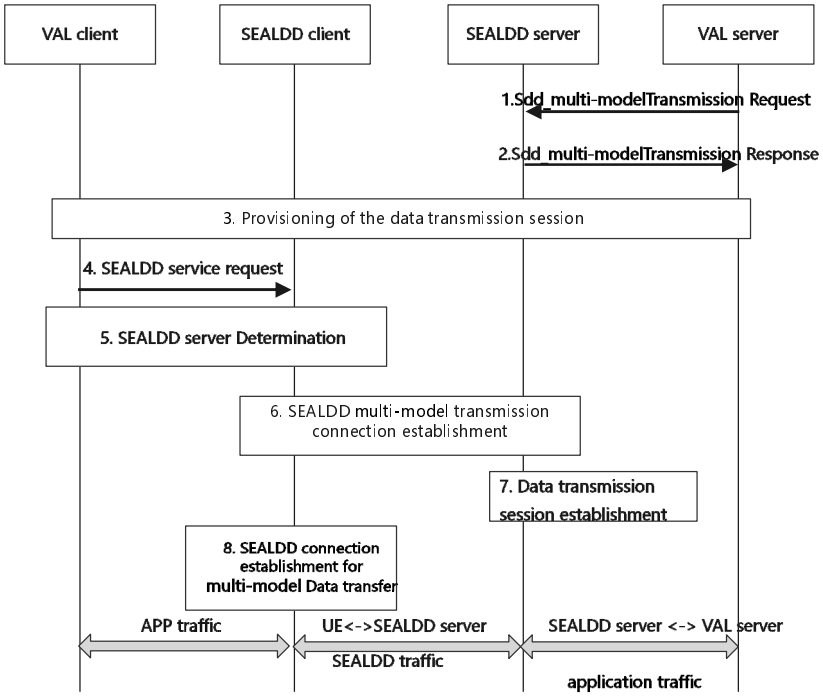

Figure 9.12.2.1.2-1: SEALDD enabled multi-modal ata transmission connection establishment procedure

1. The VAL server decides to use SEALDD service for multi-modal traffic transfer and allocates address/port as SEALDD-S Data transmission connection information for receiving the data packets from SEALDD server. The VAL server sends Sdd_multi-modalTransmission request to the SEALDD server discovered by CAPIF. The service request includes UE ID/address, VAL server ID, VAL service ID, list of requested flows, including SEALDD-S Data transmission connection information of the VAL server side, and optionally, the protocol

description, the QoS information for the application traffic, e.g. QoS requirements. As one of key parameters for multi-modal application, Crossflow measurement can be measured as procedure in clause 9.7.2.2 step 1.

2. Same as step 2 of clause 9.2.2.2. For application multi-modal service, the SEALDD server derives PDU Set related assistance information based on received VAL service ID and/or VAL server ID, and protocol description for interacting with NEF/PCF. The SEALDD server may send the AF request to provide the required QoS information to 5GC via N33/N5 for each requested flow provided in step 1. The AF request may also include the Multi-modal Service ID, which could be determined by the SEALDD server according to VAL service ID and/or VAL server ID.

3-5. Same as step 3-5 of clause 9.2.2.2.

6. The SEALDD client establishes multi-modal transmission connection with the SEALDD server. The request includes the SEALDD client ID, VAL user/UE ID, VAL server ID, VAL service ID, SEALDD-UU flow IDs, and traffic descriptors for the multiple flows from the SEALDD client side. The SEALDD server sends the SEALDD traffic descriptors for multiple flows from SEALDD server side (e.g. address/port for multiple SEALDD-UU flow) to the SEALDD client, and may send the protocol description (UL related info) received from the VAL server to the SEALDD client in the multi-modal transmission connection response. The response also includes a multi-modal SEALDD flow ID which the SEALDD server allocates. And the SEALDD client policy may also be included in its response. The SEALDD client shall then perform authorization checks and reply with a policy configuration response as specified in clause 9.10.2.4.

7-8. Same as step 8-9 of clause 9.2.2.2.

NOTE : If multiple requested flows are provided in step 1, the SEALDD client repeats steps 6-8 for each requested flow provided in step 1.

The multi-modal application traffic is exchanged between VAL client and VAL server via SEALDD layer as described in clause 9.2.2.2. If packetization indication indicates that SEALDD layer needs to perform packetization, the SEALDD server performs packetization and sends streaming data (e.g. RTP packet) via SEALDD-UU user plane (e.g. SEALDD/UDP/IP) to the SEALDD client for downlink application traffic. Similarly, the SEALDD client performs packetization and sends streaming data (e.g. RTP packet) via SEALDD-UU user plane (e.g. SEALDD/UDP/IP) to the SEALDD server for uplink application traffic. The SEALDD server and client also perform PDU Set inclusion (e.g. in RTP extension as defined in 3GPP TS 26.522 [TS26522]), and if needed, stream session and transport management (e.g. RTCP, RTSP).

9.12.2.2 SEALDD enabled multi-modal flow synchronization

9.12.2.2.1 General

The following clauses specify procedures, information flows and APIs about SEALDD enabled data transmission for XR application, including SEALDD enabled multi-modal flow synchronization.

9.12.2.2.2 SEALDD enabled multi-modal flow synchronization

Figure 9.12.2.2.2-1 illustrate the procedure for SEALDD enabled multi-modal flow synchronization, the SEALDD server determines/updates the required QoS information for multi-modal flow(s), and further interacts with 5G network.

Pre-condition:

- The VAL server has discovered and selected the SEALDD server by CAPIF functions.
- The SEALDD server has been provisioned with a multi-modal SEALDD policy including the synchronization threshold, as specified in clause 9.10.3.1.
- The SEALDD client has been provisioned with a multi-modal SEALDD policy, as specified in clause 9.10.2.4.

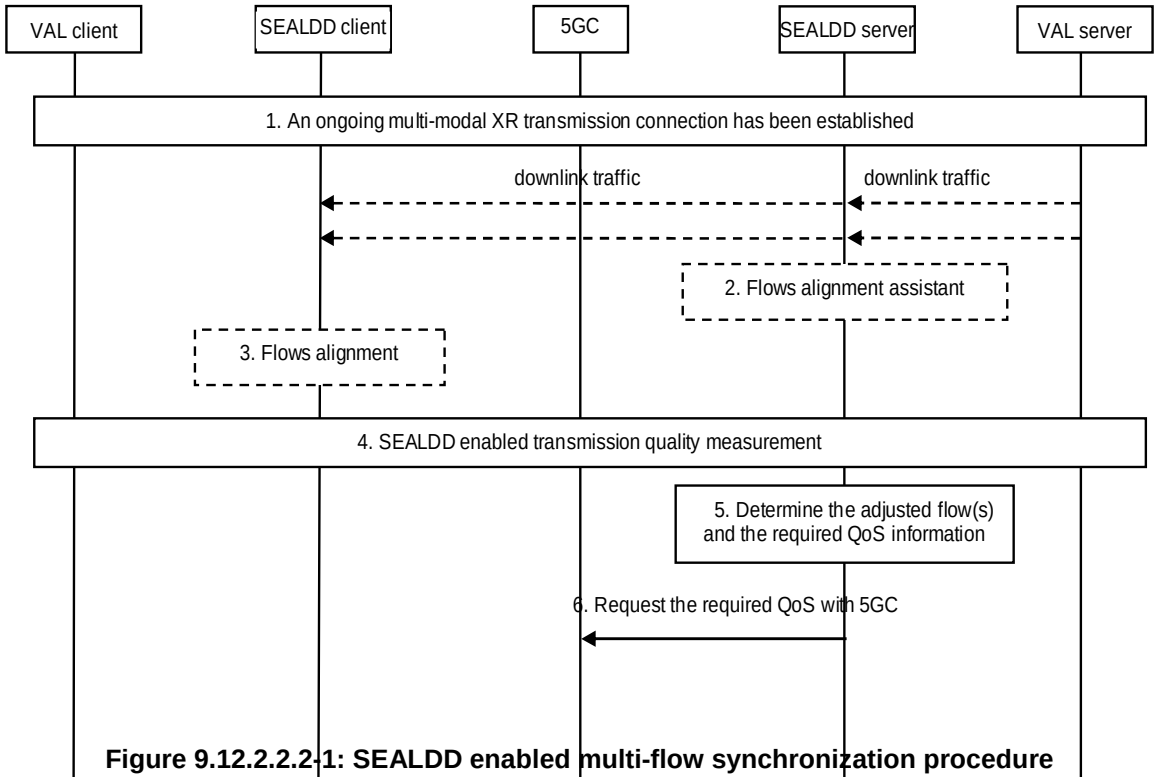

Figure 9.12.2.2.2-1: SEALDD enabled multi-flow synchronization procedure

1. An on-going multi-modal data transmission connection is established according to the steps 1-8 of clause 9.12.2.1.2.

2. Upon the multi-modal flows alignment policy triggered, the SEALDD server may help to provide the flows alignment assistance information (e.g. timestamp in the RTP header, RTCP) to the SEALDD client. If the maximum acceptable duration for traffic flow alignment is not provided, then the SEALDD server may determine the maximum acceptable duration for traffic flow alignment based on VAL service ID, flows transmission requirement, transmission quality, and the synchronization threshold. The server may translate the traffic descriptor into multi-modal SEALDD flow ID.

   The SEALDD server may communicate with the 5GS to get the analytics and prediction for the RAN congestion as per clause 6.6, clause 6.7, and clause 6.8 3GPP TS 23.288 [19]. Based on the RAN congestion analytics and prediction information, synchronization threshold and/or multi-modal flow alignment policy, the SEALDD server derives the delay introduced by the RAN and adjusts the flow alignment assistance information like DL/UL transmission timing advance or delay period. In case flow alignment is required, the flow alignment assistance information may contain UL/DL transmission timing advance period, UL/DL transmission timing delay period and the associated flow IDs in the multi-modal flows. The UL flow alignment assistance information may be sent to the SEALDD client in the Transmission quality management request specified in clause 9.9.3.1.

NOTE 1: The flow alignment assistance information can be obtained by SEALDD server based on SEALDD policy.

NOTE 2: The SEALDD client performs the caching and transmission to align multi-modal flows based on the flow alignments assistance information and maximum acceptable time duration.

NOTE 3: The NTP timestamp and RTP timestamp in RTCP sender report (SR) can be used to identify the associated packets among multi-modal flow, and further be used to perform alignment in SEALDD client.

NOTE 4: The option to rely on UE congestion analytics and RAN congestion analytics, as exposed by the 5GC via NWDAF has a margin of error, as with any predictions. To handle the real-time/near real-time constraint of these predictions, these UE congestion analytics can be requested ahead of time from the 5GC/NWDAF, e.g., once the XR session is started by the UE.

3. Upon the multi-modal flows alignment policy triggered, the SEALDD client initiates the multi-modal flows alignment based on the policy. The flows need to be aligned are identified by the VAL service ID, multi-modal SEALDD flow ID, and flow alignment assistance information.

If the flow alignment assistance information is provided, the SEALDD client identifies the associated packets (e.g., those with the same RTP timestamp) in the multi-modal flows. After all associated packets in the multi-modal flows have arrived, the SEALDD client sends the associated packets to the application client. If the maximum acceptable time duration is provided, once this maximum acceptable time is reached, the SEALDD client will no longer wait for the associated packets in multi-modal flows, even if they have not arrived yet.

For the UL synchronization, the SEALDD client sends the UL packets as per the flow alignment assistance information. The UL transmission timing advance period indicates SEALDD client to advance the UL packet transmission by advance period. The UL transmission timing delay period correction mode indicates SEALDD client to delay the transmission of the UL packet by UL delay period units. After all associated packets in the multi-modal flow have arrived at the SEALDD server, then the SEALDD server sends the associated UL packets to the VAL server.

4. The SEALDD server performs data transmission quality measurement, as defined in clause 9.7.2.1 or clause 9.7.2.3, in SEALDD-UU interface based on the mapping information for multiple flow association information between SEALDD-S interface and SEALDD-UU interface. Upon receiving the packets from multiple associated flows in SEALDD-S interface, the SEALDD server performs the packet encapsulation with sending timestamp information in the corresponding SEALDD-UU interface, and calculates the transmission delay measurement result of multiple associated flows after obtaining the receiving timestamp from the SEALDD client. As one of key parameters for XR application, delay difference can be measured as procedure in clause 9.7.2.3 step 10.

5. Based on the data transmission quality measurement results obtained for multiple associated flow over SEALDD-UU interface in step 4, and the synchronization threshold for multi-modal application as described in pre-condition, the SEALDD server determines the service flow(s) (i.e. address/port for SEALDD-UU flow) that needs to be adjusted among the multiple associated flows in SEALDD-UU interface, and the corresponding required QoS information (i.e. transmission delay). E.g., the SEALDD server evaluates whether the difference of the packet delay measurements for the flows that need to be in synchrony is above the synchronization threshold, and if it is so, the SEALDD server takes the corresponding corrective actions. The SEALDD server may advance or delay the transmission of the DL packets according to the flow assistance information to maintain the synchronization of DL flows. The DL transmission timing advance period correction mode indicates SEALDD server to advance the DL packet transmission by advance period. The DL transmission timing delay period correction mode indicates SEALDD server to delay the transmission of the DL packet by DL delay period units.

   The SEALDD server may further update the flow alignment assistance information like DL/UL transmission timing advance or delay period to fine-tune as per the data transmission quality measurement results.

6. The SEALDD server sends the AF request to 5GC via N33/N5 with the SEALDD traffic descriptor of the adjusted flow(s) (i.e. address/port for the adjusted SEALDD-UU flow) and the corresponding required QoS information determined in step 5, by utilizing the AF session with required QoS procedure in clause 4.15.6.6 of TS 23.502 [6]. The SEALDD traffic descriptor of the adjusted flow(s) contains the address or port in SEALDD server side, and/or SEALDD client side.

NOTE 5: This procedure is applicable for both downlink and uplink synchronization of multi-modal flow. For downlink and/or uplink, the step 5 is determined according to the measured downlink and/or uplink data transmission quality measurements in step 4. For uplink synchronization, the SEALDD server performs the caching and transmission to align multi-modal flows based on the flow alignment assistance information before sending the associated packets to the VAL server.

After requesting the transmission quality optimization on 5G network with the required QoS for the adjusted flow(s), the multi-flow synchronization of multi-modal application is satisfied.

9.12.2.3 Tethering link measurement and provisioning

9.12.2.3.1 General

The following clauses specify procedures, information flows and APIs about SEALDD enabled Tethering link measurement and provisioning for XR application.

9.12.2.3.2 SEALDD and VAL coordination measurement based on PIN

Figure 9.12.2.3.2-1 illustrates the procedure of SEALDD and VAL coordination Tethering link measurement based on PIN.

Pre-conditions:

1. The UE or PINE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;
2. The UE or PINE has already been registered in PIN server;
3. The PEMC on the 3GPP device has already obtained the tethered device information from PIN server;
4. There is business agreement between the VAL provider and the SEALDD provider, which requests the VAL client to respond to ICMP Ping packet.

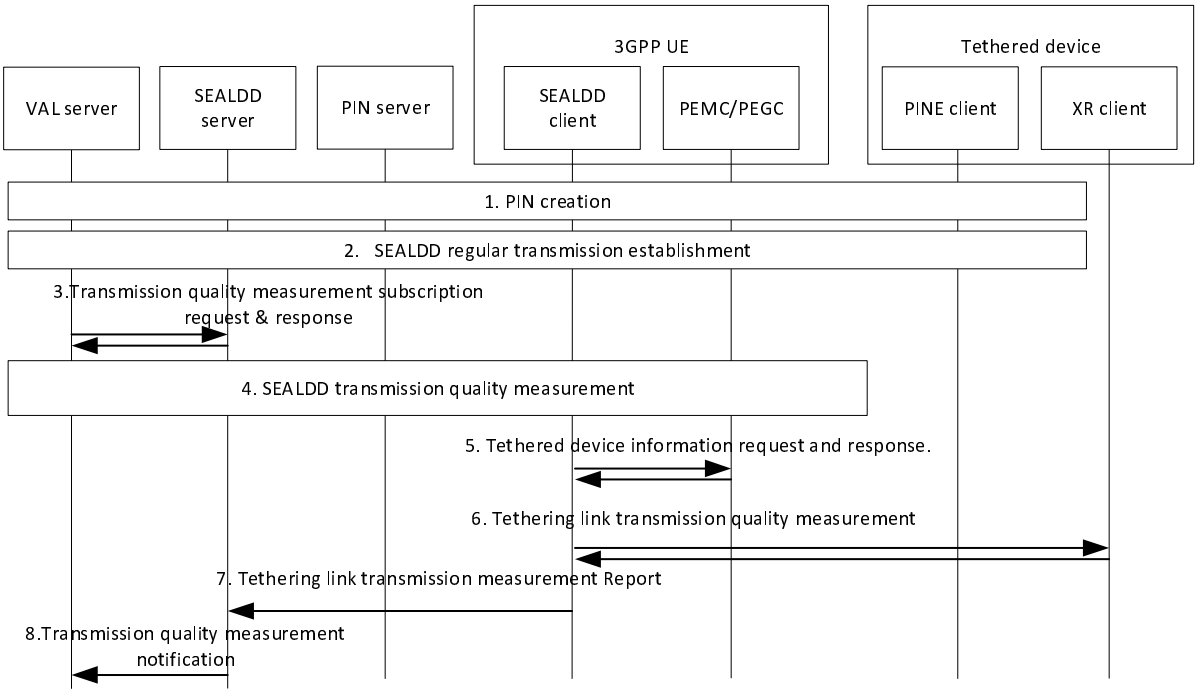

Figure 9.12.2.3.2-1: SEALDD and VAL coordination measurement based on PIN procedure

1. The PIN is successfully created and in use. The 3GPP UE acts as PEGC and PEMC, and the Tethered XR devices acts as a PINE. During the PIN creation, the detailed information of the tethered device has been provided to PEMC on 3GPP UE from PINAPP server as defined in clause 8.5.2, 3GPP TS 23.542 [23].
2. The regular data transmission connection is established, with the information received in step1.

   The connection between the SEALDD server and 3GPP UE is established as defined in clause 9.2.2.2.
3. The VAL server sends a SEALDD transmission quality measurement subscription request to the SEALDD server as defined in clause 9.7. If authorization is successful, the SEALDD server sends a response to the VAL server with the subscription ID, expiration time.
4. The SEALDD server starts the transmission quality measurement as defined in clause 9.7.2.3. The SEALDD server sends a SEALDD transmission quality measurement subscription request to the SEALDD client and the SEALDD client responds to the SEALDD server.
5. The SEALDD client, acting as a PINE, gets the information of the tethered device from the PEMC over PIN-1, as defined in the clause 8.5.8 of 3GPP TS 23.542 [23], to identify the tethering link.
6. The SEALDD client on the 3GPP UE interacts with XR client on the tethered UE to do the measurement based on ICMP ping protocol.

7. The SEALDD client sends the report to the SEALDD server using the transmission quality measurement notification.

8. The SEALDD server reports the data transmission quality measurement results to the VAL server via the notification message.

9.12.2.3.3 SEALDD measurement based on PIN

Figure 9.12.2.3.3-1 illustrates the procedures of SEALDD measurement based on PIN.

Pre-conditions:

1. The UE or PINE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The UE or PINE has already been registered in PIN server;

3. The PEMC on the 3GPP device has already obtained the tethered device information from PIN server;

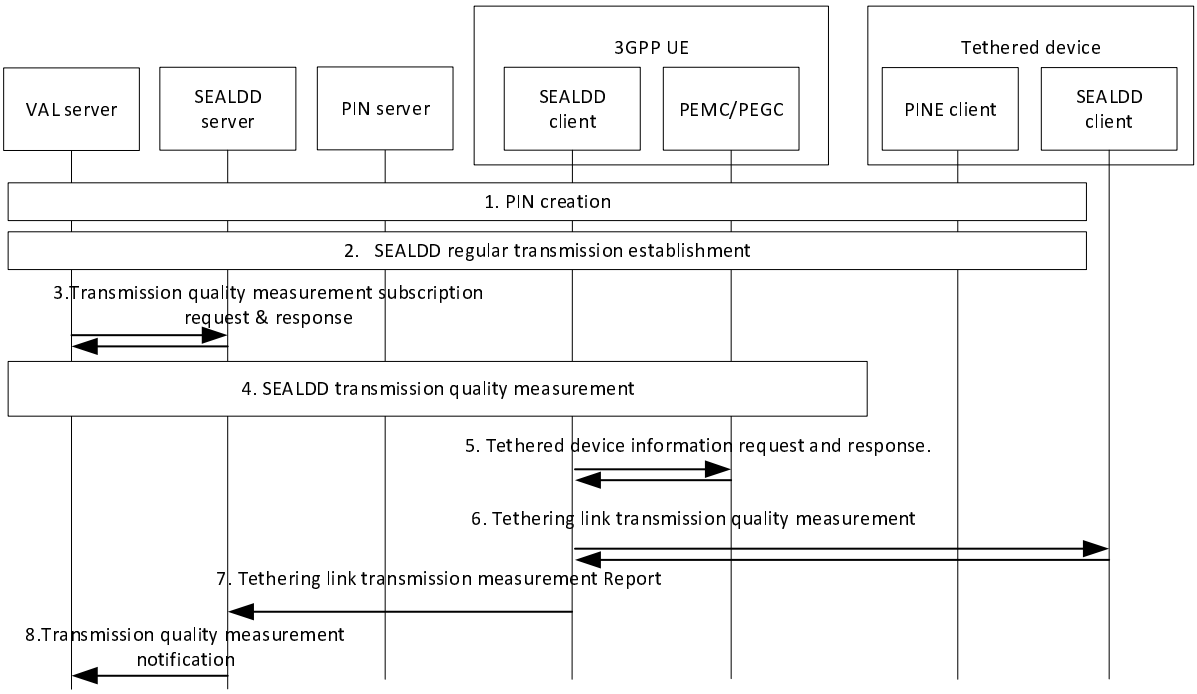

Figure 9.12.2.3.3-1: SEALDD measurement based on PIN procedure

1. The PIN is successfully created and in use. The 3GPP UE acts as PEGC and PEMC, and the Tethered XR devices act as a PINE. During the PIN creation, the detailed information of the tethered device has been provided to PEMC on 3GPP UE from PINAPP server as defined in clause 8.5.2, 3GPP TS 23.542 [23].

2. The regular data transmission connection is established, with the information received in step1.

   The connection between the SEALDD server and 3GPP UE is established as defined in clause 9.2.2.2.

   Optionally, the SEALDD client gets the tethered device information form PEMC(e.g., the MAC address, PINE Address, Port number.) and sends the direct data transmission connection request to the tethered UE using the information form PEMC to establish a SEALDD-UUc connection between the 3GPP UE and tethered device as defined in clause 9.12.2.3.4.

3. The VAL server sends a SEALDD transmission quality measurement subscription request to the SEALDD server as defined in clause 9.7. If authorization is successful, the SEALDD server sends a response to the VAL server with the subscription ID, expiration time.

4. The SEALDD transmission quality measurement is defined in clause 9.7.2.3. The SEALDD server sends a SEALDD transmission quality measurement subscription request to the SEALDD client and the SEALDD client responds to the SEALDD server.

5. The SEALDD client gets the information of the tethered device from the PEMC over PIN-1, as defined in the clause 8.5.8 of 3GPP TS 23.542 [23], to identify the tethering link.

6. The SEALDD client on the 3GPP UE interacts with SEALDD client on the tethered UE to do the measurement based on ICMP ping protocol, or uses monitoring packet in established tethering link SEALDD connection.

7. The SEALDD client sends the report to the SEALDD server using the transmission quality measurement notification.

8. The SEALDD server sends the data transmission quality measurement results (e.g. latency, jitter, bitrate, packet loss rate) to the VAL server via the SEALDD enabled data transmission quality measurement notification as defined in clause 9.7.3.3.

9.12.2.3.4 SEALDD-UUc connection establishment between the SEALDD client on 3GPP UE and tethered device

Depicted in figure 9.12.2.3.4-1 is the procedure for establishment of SEALDD-UUc connection between the SEALDD client on 3GPP UE and tethered device.

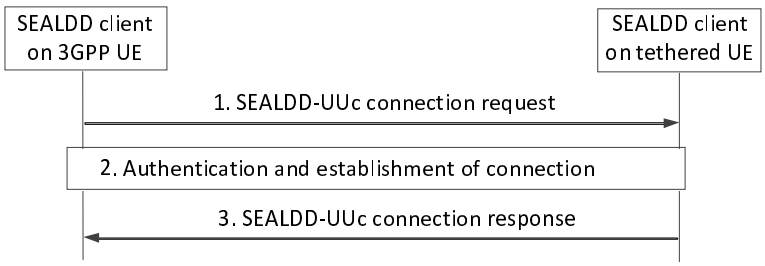

Figure 9.12.2.3.4-1: Establishment of SEALDD-UUc connection between the SEALDD client on 3GPP UE and tethered device

1. SEALDD client on 3GPP UE sends a SEALDD-UUc connection request to SEALDD client on tethered UE. This message includes the UE identity, SEALDD-UUc data transmission connection information(e.g., address/port allocated).

2. SEALDD client on Tethered UE initiates the procedure for mutual authentication. The successful completion of the authentication procedure completes the establishment of the SEALDD-UUc connection.

3. SEALDD client on tethered UE sends a SEALDD-UUc connection response to SEALDD client on 3GPP UE.

9.12.2.4 SEALDD enabled UE-to-UE communication based on policy

9.12.2.4.1 General

When two VAL UEs need to communicate with each other for exchanging gaming/interactive data in XR service, they use servers in the DN as data relay or communicate with each other directly.

NOTE 1: This solution is only applicable for the XR transmission scenario without involvement of VAL server. As an example, XR gaming application client can support LAN-type of multi-player game mode without involvement of XR gaming server to process run-time game data.

In order to improve service experience (esp. for reducing service latency), SEALDD server monitors distance of UEs involved in the XR communication. When SEALDD server finds that the two UEs are within direct communication range, the SEALDD server instructs the SEALDD clients to switch to direct communication mode. Such mode switch decision needs to take E2E communication performance into consideration.

If the UE-to-UE application performance analytics result from ADAE shows the quality in off-network mode will be degraded and the quality in on-network mode is estimated to be good, or vice versa, the mode switch is done in SEALDD layer.

NOTE 2: For the same XR application service, all XR traffic flows are transmitted via either off-network or on-network between UEs.

9.12.2.4.2 SEALDD enabled UE-to-UE communication

The SEALDD servers has Data Delivery (DD) policy being provisioned for UE-to-UE communication. The DD policy is enforced by the SEALDD server to switch the SEALDD connection for UE-to-UE communication (either direct or indirect).

Pre-conditions:

1. The SEALDD server has DD policies available.
2. The SEALDD clients in UE1 and UE2 has discovered the same SEALDD server.
3. The SEALDD clients in UE1 and UE2 have the ProSe application capabilities.
4. SEALDD UE-to-UE policy has been provided to SEALDD client.

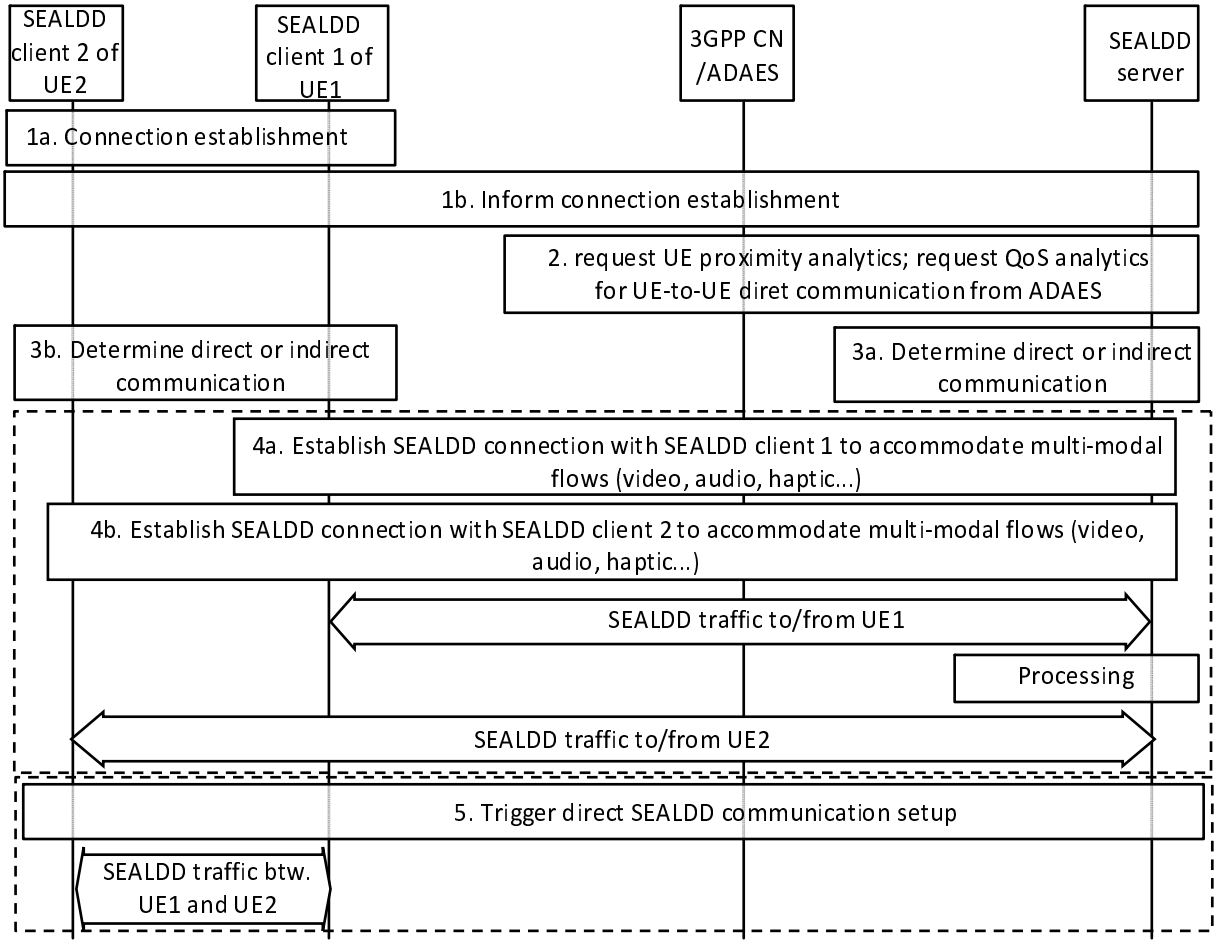

Figure 9.12.2.4.2-1: Policy enforced by SEALDD server for connectivity between two UEs

1a. The UE-to-UE communication is established between UE 1 and UE 2 via SEALDD client as specified in clause 6.4.3.1 3GPP TS 23.304 [17].

1b. The SEALDD client in UE1/2 informs the SEALDD server about the establishment of direct SEALDD communication with Sdd_XRTransmissionConnnection_Inform operation.

2. Based on SEALDD UE-to-UE policy, the SEALDD server requests 3GPP CN (NWDAF/NEF) for UE relative proximity analytics for UE1 and UE2, requests 3GPP CN (GMLC/NEF) for SL/Ranging service exposure about the relative locations or distances and directions related to the UE1 and UE2, and requests ADAES for UE-to-UE application performance analytics as described in 3GPP TS 23.436 [13] clause 8.4, requests NWDAF/NEF for QoS Sustainability Analytics and Service Experience Analytics for UEs and/or requests PCF/NEF for QoS monitoring.

Editor's note: Whether SA2 provided services can support UE-to-UE communication analytics is FFS. Whether ADAES supports off-network communication analytics is FFS.

3a. According to the SEALDD UE-to-UE policy, if relative proximity analytics result shows that both UEs are not in vicinity to each other (distance between UEs > proximity threshold in UE-to-UE policy), and/or the QoS/QoE for UE-to-UE direct communication analytics result is no so good (e.g. PLR in analytics report > PLR threshold in UE-to-UE policy), the SEALDD continues with step 4 for indirect communication preparation; otherwise, the SEALDD keeps monitoring (as described in step 2) for the two UEs.

3b. According to the SEALDD UE-to-UE policy, if the ProSe discovery result shows that both UEs are not in vicinity to each other(e.g., no discovery response received), and/or the UE-to-UE application performance result(collected as defined in 3GPP TS 23.436 [13] clause 8.4 step 5) is not so good(latency in application performance result > latency in UE-to-UE policy), the SEALDD client(s) on either or both of the two UEs decides to perform path switching and continues with step 4 for indirect communication preparation.4. After establishment of SEALDD connections for UE1 and UE2, the SEALDD traffic carrying XR flows are processed in the SEALDD server. The SEALDD server forwards traffic between UE1 and UE2, and may buffer data burst from originating UE and send it to destination UE smoothly.

5. If later on, both UEs are in proximity which is capable of direct communication and the QoS/QoE analytics result from ADAES for UE-to-UE direct communication shows good quality, the SEALDD server helps to establish direct SEALDD communication by informing the SEALDD client of any of the two UEs with Sdd_XRTransmissionConnnection_Trigger operation including the information of its peer SEALDD client (of UE1 or UE2). Then the SEALDD client 1 or 2 establishes SEALDD connection towards the peer SEALDD client via SEALDD-PC5 and the SEALDD traffic carrying XR flows are exchanged directly between UE1 and UE2 via SEALDD-PC5.

Based on the monitoring and analytics result (as requested in step 2), and SEALDD UE-to-UE policy:

- if the current UE1-UE2 communication mode is direct and SEALDD server decides to switch to indirect communication mode, the SEALDD server establishes SEALDD connections with SEALDD client 1 and SEALDD client 2 as described in step 4, then triggers direct SEALDD communication release using Sdd_XRTransmissionConnnection_Trigger operation towards the SEALDD client which received establishment request in step 5 and the SEALDD client further releases the direct SEALDD connection towards its peer SEALDD client via SEALDD-PC5.

- if the current UE1-UE2 communication mode is indirect and SEALDD server decides to switch to direct communication mode, the SEALDD server triggers direct SEALDD communication setup as described in step 5 and releases SEALDD connections towards SEALDD client 1 and SEALDD client 2.

9.12.3 Information flows

Editor's note: Whether SEALDD enabled XR data transmission establishment service and SEALDD enabled multi-modal flow synchronization service can use the same API is FFS.

9.12.3.1 SEALDD enabled multi-modal transmission request

Table 9.12.3.1-1 describes the information flow from the VAL server to the SEALDD server for requesting multi-modal transmission service.

Table 9.12.3.1-1: SEALDD enabled multi-modal transmission request

Information element	Status	Description
VAL server ID	M	Identity of the VAL server
VAL service ID	O	Identity of the VAL service
Identity	O	Identifier of specific UE or VAL user
List of requested flows	M	List of the requested multi-modal flows
>SEALDD-S Data transmission connection information for multi-modal XR	M	Address(s)/port(s) and/or URL(s) of the VAL server to receive the multi-flow packets from the SEALDD server (e.g. audio flow, tactile flow)
>QoS information	O	QoS information provided by VAL server
>Protocol description	O	The protocol description of VAL traffic. It includes header extension information (e.g. RTP extension with PDU set), packetization indication, payload type and format (e.g. H.264/RTP, H.265/RTP, H.264, H.265). Header extension information is only applicable when payload indicates RTP.

9.12.3.2 SEALDD enabled multi-modal transmission response

Table 9.12.3.2-1 describes the information flow from the SEALDD server to the VAL server for responding to the multi-modal transmission response.

Table 9.12.3.2-1: SEALDD enabled multi-modal transmission response

Information element	Status	Description
Result	M	Success or failure.
SEALDD-S information Data transmission connection information for multi-modal service	O	Address(s)/port(s) and/or URL(s) of the SEALDD server to receive the multi-flow packets from the VAL server for application traffic transfer (e.g. audio flow, tactile flow)
Cause	O (See NOTE)	Indicates the reason for the failure
NOTE: The IE is only present if the Result is failure.		

9.12.3.3 SEALDD multi-modal transmission connection establishment request

Table 9.12.3.3-1 describes the information flow from the SEALDD client to the SEALDD server for requesting the multi-modal transmission connection establishment.

Table 9.12.3.3-1: SEALDD multi-modal transmission connection establishment request

Information element	Status	Description
SEALDD client ID	M	Identity of the SEALDD client.
Identity	O	The VAL user ID of the VAL user or VAL UE ID
SEALDD-UU flows info	M	Information of the list of SEALDD-UU flows.
> SEALDD-UU flow ID	M	Identity of the SEALDD-UU flow.
> SEALDD traffic descriptor	M	SEALDD traffic descriptor for the flow of the SEALDD client side used to establish SEALDD multi-modal XR connection.
>> Addressing info	M	Indicates the addressing information (e.g. address, port, URL).
>> Transport layer protocol	M	Indicates the transport layer protocol.
VAL server ID	O	Identity of the VAL server.
VAL service ID	O	Identity of the VAL service.

9.12.3.4 SEALDD multi-modal transmission connection establishment response

Table 9.12.3.4-1 describes the information flow from the SEALDD server to the SEALDD client for responding to the multi-modal transmission connection establishment.

Table 9.12.3.4-1: SEALDD multi-modal transmission connection establishment response

Information element	Status	Description
Result	M	Indicates the success or failure of establishing the SEALDD connection.
Multi-modal SEALDD flow info	M	Information of the Multi-modal SEALDD-UU flow associated with the multi-modal XR connection.
> Multi-modal SEALDD flow ID	M	Identity of the Multi-modal SEALDD-UU flow associated with the multi-modal service connection.
> SEALDD-UU flows list	M	Indicates the list of SEALDD-UU flows.
>> SEALDD-UU flow ID	M	Identity of the SEALDD-UU flow.
>> SEALDD traffic descriptors	M	SEALDD traffic descriptors for the flows of the SEALDD server side used to establish SEALDD multi-modal connection.
>>> Addressing info	M	Indicates the addressing information (e.g. address, port, URL).
>>> Transport layer protocol	M	Indicates the transport layer protocol.
Protocol description	O	The protocol description of VAL traffic. It includes header extension information (e.g. RTP extension for PDU set), packetization indication, payload type and format.
>Header extension information	O	The header extension information includes the RTP header extension type and RTP header extension identity.
>Packetization indication	O	Packetization indication indicates whether the RTP header extension information is included or not.
>Payload type	O	Indicates the type of the payload (e.g., RTP, SRTP). Header extension information is only applicable when payload type indicates RTP.
>Payload format	M	Indicates the format of the payload (e.g., H.264, H.265).
Cause	O (See NOTE)	Indicates the reason for the failure
NOTE: The IE is only present if the Result is failure.		

9.12.3.5 SEALDD-UUc connection request

Table 9.12.3.5-1 describes the information flow from the SEALDD client on 3GPP UE to SEALDD client on tethered UE for SEALDD-UUc connection request.

Table 9.12.3.5-1: SEALDD-UUc connection request

Information element	Status	Description
Requestor's ID or PIN ID	M	Identity of the requestor SEALDD client on 3GPP UE, or the PIN ID of the requestor.
SEALDD-UUc data transmission connection information	M	SEALDD-UUc data transmission connection information(e.g., address/port allocated)

9.12.3.6 SEALDD-UUc connection response

Table 9.12.3.6-1 describes the information flow from the SEALDD client on 3GPP UE to SEALDD client on tethered UE for SEALDD-UUc connection response.

Table 9.12.3.6-1: SEALDD-UUc connection response

Information element	Status	Description
Result	M	Success or failure.
SEALDD-UUc data transmission connection information	O	SEALDD-UUc data transmission connection information(e.g., address/port allocated)

9.12.3.7 Inform XR transmission request

Table 9.12.3.7-1 describes the information flow from the SEALDD client to the SEALDD server to inform XR transmission connection status between two UEs.

Table 9.12.3.7-1: Inform XR transmission request

Information element	Status	Description
Requestor ID	M	Identity of the requestor (i.e. SEALDD client).
VAL service ID	O	Identity of the VAL service
Identities	M	Identifier of UEs or VAL users involved in the UE-to-UE direct communication.
Status	M	Identifies the UE-to-UE direct communication status (e.g. establishment, release).

9.12.3.8 Inform XR transmission response

Table 9.12.3.8-1 describes the information flow from the SEALDD server to the SEALDD client to acknowledge XR transmission connection status between two UEs.

Table 9.12.3.8-1: Inform XR transmission response

Information element	Status	Description
Result	M	Result of the operation.

9.12.3.9 Trigger XR transmission request

Table 9.12.3.9-1 describes the information flow from the SEALDD server to the SEALDD client to trigger XR transmission connection operation between two UEs.

Table 9.12.3.9-1: Trigger XR transmission request

Information element	Status	Description
Requestor ID	M	Identity of the requestor (i.e. SEALDD server).
VAL service ID	O	Identity of the VAL service
Identities	M	Identifier of UEs or VAL users involved in the UE-to-UE direct communication.
Operation	M	Identifies the action for UE-to-UE direct communication (e.g. establishment, release).

9.12.3.10 Trigger XR transmission response

Table 9.12.3.10-1 describes the information flow from the SEALDD client to the SEALDD server to acknowledge XR transmission connection operation between two UEs.

Table 9.12.3.10-1: Trigger XR transmission response

Information element	Status	Description
Result	M	Result of the operation.

9.12.4 APIs

9.12.4.1 General

Table 9.12.4.1-1 illustrates the APIs exposed by SEALDD server for XR transmission.

Table 9.12.4.1-1: List of SEALDD server APIs for XR transmission

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_multi-modalTransmission	Request	Request/Response	VAL server
Sdd_XRTransmissionConnnection	Establish	Request/Response	SEALDD client
	Trigger (NOTE)	Request/Response	SEALDD server
	Inform	Request/Response	SEALDD client
Sdd_SEALDD-UUcConnection	Establish	Request/Response	SEALDD client
NOTE: The Sdd_XRTransmissionConnection_Trigger API operation is exposed by the SEALDD client.			

9.12.4.2 Sdd_multi-modalTransmission Request operation

API operation name: Sdd_multi-modalTransmission Request

Description: The consumer requests for one time for multi-modal transmission service.

Inputs: See clause 9.12.3.1.

Outputs: See clause 9.12.3.2

See clause 9.12.2.1.2 and 9.12.2.2.2 for details of usage of this operation.

9.12.4.3 Sdd_XRTransmissionConnection_Establish operation

API operation name: Sdd_XRTransmissionConnection_Establish

Description: The consumer requests for multi-modal transmission connection establishment.

Inputs: See clause 9.12.3.3.

Outputs: See clause 9.12.3.4.

See clause 9.12.2.1.2 and 9.12.2.2.2 for details of usage of this operation.

9.12.4.4 Sdd_SEALDD-UUcConnectionEstablish operation

API operation name: Sdd_SEALDD-UUcConnectionEstablish

Description: The consumer requests for SEALDD-UUc connection establishment between the SEALDD client on 3GPP UE and tethered device.

Inputs: See clause 9.12.3.5.

Outputs: See clause 9.12.3.6.

See clause 9.12.2.3.4 for details of usage of this operation.

9.12.4.5 Sdd_XRTransmissionConnection_Trigger operation

API operation name: Sdd_XRTransmissionConnection_Trigger

Description: The consumer requests to trigger direct multi-modal transmission connection establishment between two UEs.

Inputs: See clause 9.12.3.7.

Outputs: See clause 9.12.3.8.

See clause 9.12.2.4 for details of usage of this operation.

9.12.4.6 Sdd_XRTransmissionConnection_Inform operation

API operation name: Sdd_XRTransmissionConnection_Inform

Description: The consumer informs direct multi-modal transmission connection establishment between two UEs.

Inputs: See clause 9.12.3.9.

Outputs: See clause 9.12.3.10.

See clause 9.12.2.4 for details of usage of this operation.

9.13 SEALDD enabled adaptive data transmission

9.13.1 General

The following clauses specify procedures, information flows and APIs about SEALDD enabled adaptive data transmission.

9.13.2 SEALDD enabled adaptive data transmission

Figure 9.13.2-1 illustrate the procedure for supporting adaptive data transmission. The SEALDD facilitates to transmit data between the VAL client and VAL server adaptively by using application enablement layer capabilities of the AIML Enablement server defined in 3GPP TS 23.482 [xx]. This procedure is used to support adaptive data transmission for XR services.

Pre-conditions:

- The AIMLE Server is known by the consumer and the SEALDD Server.
- The AI/ML services provided by the AIMLE Server is allowed for exposure to the consumer and the SEALDD Server.
- The consumer decides on the application which requires split image/video processing (distribute image/video processing tasks to multiple split endpoints for processing).
- Up to requirements of high layer application, SEALDD Server triggers interaction with AIMLE Server for assistance information.

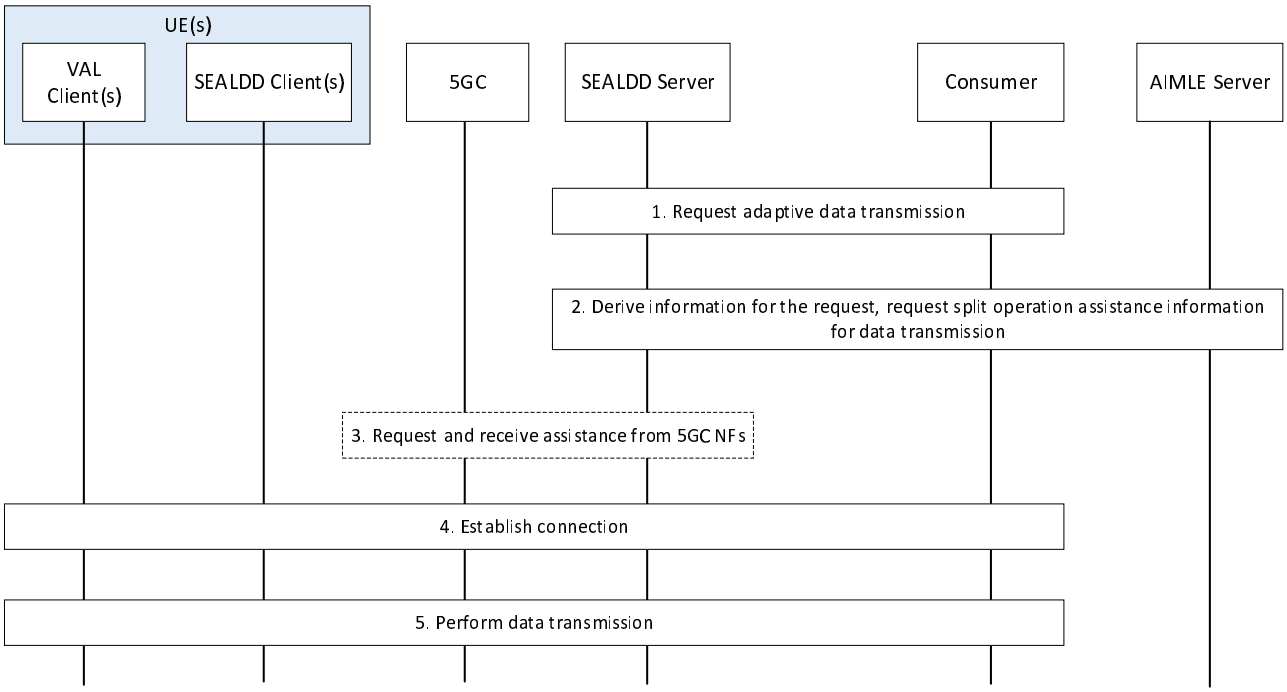

Figure 9.13.2-1: SEALDD enabled adaptive data transmission procedure

1. The consumer (e.g. VAL server, VAL client via SEALDD client) sends adaptive data transmission request to the SEALDD server (e.g. for supporting XR service to deliver/distribute data to the split AI/ML endpoints (i.e. VAL client(s))). The request message contains message as defined in table 9.13.3.1-1.

2. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, the SEALDD server responses to the VAL server. The SEALDD server derives information for the request, for example, based on the message in the request to decide whether assistance from 5GC and/or AIMLE server is needed or not, and determine downstream entities and services needed based on the information derived.

   Then the SEALDD server sends request to the AIMLE server for split operation assistance information for the data transmission. For example, for split AI/ML image/video processing, the request contains the information of split AI/ML endpoints (from the request in step 1), data information (e.g. data type, data size, range of data size) to be delivered/distributed to the split AI/ML endpoints, may contain QoS requirements on the data transmission, e.g. desired data transmission time. The information flow for the request reuses the mechanisms specified in 3GPP TS 23.482 [xx].

3. The SEALDD server may request and receive assistance from 5GC, as described in step 2, e.g. assistance information from NWDAF (or via NEF) about analytics on E2E data volume transfer time. In the request from SEALDD server to NWDAF for E2E data volume transfer time analytics, the split AI/ML endpoints information and a pre-configured data size (or data size range) may be used (the pre-configured data size may be the data size provided in step 1 or be decided by the SEALDD server according to the data size range in step 1 and based on its local policy. The data size range is provided in step 1.). The analytics subscription is modified when the actual data size changed. The actual data size may be obtained via measurement described in Sdd_TransmissionQuality Management API.

4. The SEALDD server triggers to establish connection among the consumer, SEALDD server, SEALDD client(s), and with the split AI/ML endpoints (i.e. VAL client(s)) for the data transmission. The split operation assistance information received in steps 2 and 3 is used by the SEALDD server separately or jointly based on need and local policy.

   According to the assistance information, the SEALDD server may adjust the data volume to be transmission to each of the split AI/ML endpoints (if adaptive assign of date volume to the split AI/ML endpoints is allowed), or adjust the time point/time window for data transmission to the split endpoints.

NOTE 1: Adaptive assign of date volume to split AI/ML endpoints is allowed in the scenarios when there is no dependency of data processing at different split AI/ML endpoints and no specifical requirement on data assignment to different split AI/ML endpoints for processing.

NOTE 2: The connection establishment and data transmission procedures could use the existing mechanisms in clause 9.12.2.1.2.

5. Operations are performed at the consumer, SEALDD server, SEALDD client(s), and VAL client(s) for the data transmission, e.g. image/video/multi-modal data transmission from the consumer to the split AI/ML endpoints.

9.13.3 Information flows

9.13.3.1 SEALDD adaptive data transmission request

Table 9.13.3.1-1 describes the information flow from the consumer to the SEALDD server for requesting or updating request for an adaptive data transmission.

Table 9.13.3.1-1: SEALDD adaptive data transmission request

Information element	Status	Description
Requestor ID	M (NOTE)	The identifier of the consumer (e.g. VAL server ID, SEALDD client ID, VAL client ID).
VAL service ID	O	Identity of the VAL service.
VAL UE ID(s)	O	Identifier(s) of the endpoints (i.e. VAL UE(s)).
Adaptive data assign Indicator	O	Indicate that the data can be assigned to different endpoints adaptively.
Data information	M	The information of the data needs to be delivered or distributed.
>Data type	O	The type of data, could be e.g. image, video, multi-model data (e.g. audio, video, positioning, haptic data).
>Data size information	M	The maximum/minimum/average size of the data or a range of size for the data (a pair of minimum and maximum data volumes) to be delivered/distributed.
>Time duration	M	The time duration (start and end time) expected for sending the volume of data.
QoS requirement	O	The QoS requirement, e.g. latency for data transmission.
Assistance information	O	The assistance information for deliver/distribute the data, e.g. time point/time window for the data transmission to the split AI/ML endpoints.
NOTE: This information element shall not be updated.		

9.13.3.2 SEALDD adaptive data transmission response

Table 9.13.3.2-1 describes the information from the SEALDD server to the consumer for responding to the adaptive data transmission request.

Table 9.13.3.2-1: SEALDD adaptive data transmission response

Information element	Status	Description
Result	M	The result of the request (positive or negative acknowledgement).

9.13.4 APIs

9.13.4.1 General

Table 9.13.4.1-1 illustrates the APIs exposed by SEALDD server for adaptive data transmission.

Table 9.13.4.1-1: List of SEALDD server APIs for adaptive data transmission

API Name	API Operations	Operation Semantics	Consumer(s)
Sdd_AdaptiveTransmission	Request	Request/Response	VAL server, SEALDD client

9.13.4.2 Sdd_AdaptiveTransmission Request operation

API operation name: Sdd_AdaptiveTransmission Request

Description: The consumer requests for adaptive data transmission service.

Inputs: See clause 9.13.3.1.

Outputs: See clause 9.13.3.2.

See clause 9.13.2 for details of usage of this operation.

10 SEALDD services over Satellite Access

10.1 General

This clause provides clarifications on the procedures and information flows for enabling SEALDD services using satellite access.

10.2 SEALDD enabled transmission for S&F Satellite operation

10.2.1 General

This clause provides the services to support the transmission for delivery of delay-tolerant/non-real-time satellite services (i.e. CIoT/MTC, SMS) based on SEALDD capabilities including adapt the DL data delivery according to the S&F events from the 3GPP core network.

NOTE: In Store and Forward Satellite operation, the end-to-end exchange of signalling/data traffic is handled in a sequence of steps reflecting the intermittent availability of the service link when the satellite can exchange data with the VAL UE and of the intermittent availability of the feeder (ground) link when the satellite can exchange data with the ground network (VAL server). To support Store and Forward Satellite operation, network functionality needs to be deployed on the satellite, as specified in 3GPP TS 23.401 [25].

10.2.2 Procedures

10.2.2.1 SEALDD enabled data transmission for delay-tolerant satellite services

Figure 10.2.2.1-1 illustrates the procedure for establishing S&F data transmission connection, and the SEALDD facilitates the delay-tolerant satellite services to transmit its data between the VAL client and VAL server.

Pre-condition:

- The VAL server discovers and selects the SEALDD server by CAPIF functions.

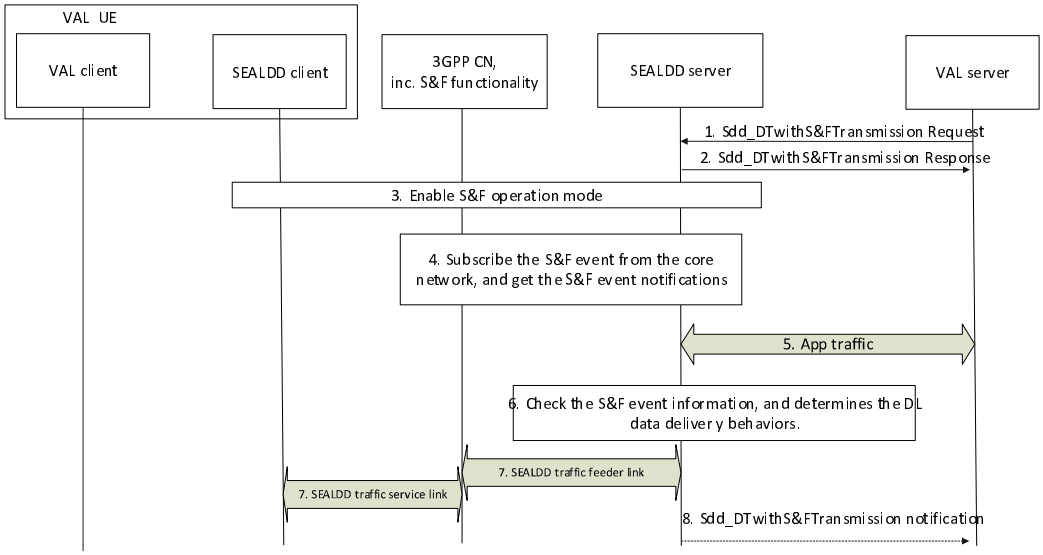

Figure 10.2.2.1-1: SEALDD enabled data transmission for delay-tolerant satellite services

1. The VAL server decides to use SEALDD service for delay-tolerant traffic transfer and allocates address/port as SEALDD-S Data transmission connection information for receiving the data packets from SEALDD server. The VAL server sends Sdd_DTwithS&FTransmission request to the SEALDD server discovered by CAPIF. The service request includes UE ID/address, VAL server ID, VAL service ID, SEALDD-S Data transmission connection information of the VAL server side.

2. Upon receiving the request, the SEALDD server performs an authorization check. If authorization is successful, SEALDD server allocates the SEALDD-S data transmission connection information (e.g., address/port) of SEALDD server side to receive the application data packets from the VAL server to be delivered to the VAL UE. The SEALDD server responds with a Sdd_DTwithS&FTransmission response.

NOTE 1: The SEALDD-S data transmission connection information of the SEALDD server side is optional, if the SEALDD server uses the downlink pull mode to fetch the application data from the address provided by the VAL server in step 1, and uses the uplink push mode to send the application data to the address provided by VAL server.

3. The SEALDD server and the SEALDD client enable S&F operation.

NOTE 2: The procedure to enable the S&F mode for the SEALDD server and SEALDD client is out of the scope of this release.

4. The SEALDD server subscribes and is notified about the store and forward satellite operation information from the 3GPP CN as specified in clause 5.6.3.10 of 3GPP TS 23.682 [24] e.g., whether the UE is registered in S&F Mode, the estimated S&F DL delivery time indicating the estimated/expected time required to deliver the data to UE from the time data has been received in the 3GPP network (i.e., SCEF or PGW), feeder link availability period. The SEALDD server stores the received S&F satellite operation information for further control the downlink application data transmission.

5. The VAL server sends downlink application data to the SEALDD server which further delivers it to the VAL UE via the S&F satellite when the feeder link is available.

NOTE 3: Based on implementation, the SEALDD server can monitor the availability of terrestrial network connectivity and hence enable connectivity before the feeder link is available.

NOTE 4: The SEALDD server may receive the DL application data from the VAL server in step 5 before S&F satellite operation information from the 3GPP CN in step 4.

6. The SEALDD server controls the downlink application data delivery to the SEALDD client based on the S&F satellite operation information, when the UE is registered in S&F mode:

- pending the DL data transmission when the Feeder Link is not available;
- (re-)transmitting the pending DL data when the Feeder Link is available.
- DL data volume to be transmitted is smaller than maximum S&F data storage quota.
- If estimated S&F DL delivery time is received from 3GPP CN, it may be used by the SEALDD server to estimate whether the transmitted DL application data is successfully delivered to the UE and its corresponding storage is available for new DL data. For each Feeder Link available period, the SEALDD server starts an estimated delivery timer based on the estimated S&F DL delivery time which is corresponding to the current feeder link. The estimated delivery timer may be greater than or equal to the estimated S&F DL delivery time. In next Feeder Link available period, the SEALDD server checks the previous estimated delivery timer is expired or not before transmitting the DL data. Also, the maximum S&F data storage quota is also considered.

    a. If the timer expires, the SEAL server sends DL data. If the maximum S&F data storage quota is configured, the SEALDD server may further calculate the volume (e.g., increasing the volume by certain data size (e.g., size of data previously delivered to the SEALDD client)) of new DL data to be sent.

    b. If the timer not expires, the SEALDD server may not send the DL data and wait until the timer expires. If the maximum S&F data storage quota is configured, the SEALDD server may further also checks the available data volume within the maximum S&F data storage quota. The SEALDD server may send DL data limited within the available data volume. If no available data volume, the SEALDD server pends the DL data transmission until the timer expires.

NOTE 5: The SEALDD server can use the estimated S&F DL delivery time as the estimated/expected time required to deliver the data to UE from the time data has been received at the SEALDD server, as the data delivery latency from the SEALDD server to the 3GPP network (i.e., the SCEF or PGW) is quite small and can be ignored compared with the estimated S&F DL delivery time from network to the UE.

NOTE 6: The maximum S&F data storage quota can be per UE, per application or per SEALDD server or any combination of them.

NOTE 7: The data forwarding based on priority policy is out of the scope of the current release.

7. The SEALDD server sends the DL data to the VAL UE via the 3GPP network and the S&F network functionality deployed in the S&F satellite.

8. Optionally, the SEALDD server may send Sdd_DTwithS&FTransmission notification to the VAL server to influence the DL application data transmission from VAL server if the VAL UE connection status changes or the DL data transmission from the VAL server needs to be adjusted.

10.2.2.2 Client initiated data transmission for delay-tolerant satellite services

Figure 10.2.2.2-1 illustrates the procedure for establishing S&F data transmission connection, and the SEALDD facilitates the delay-tolerant satellite services to transmit data initiated by the VAL client to VAL server.

Pre-condition:

- The VAL client is aware of the availability of delay-tolerant satellite services to transmit data.

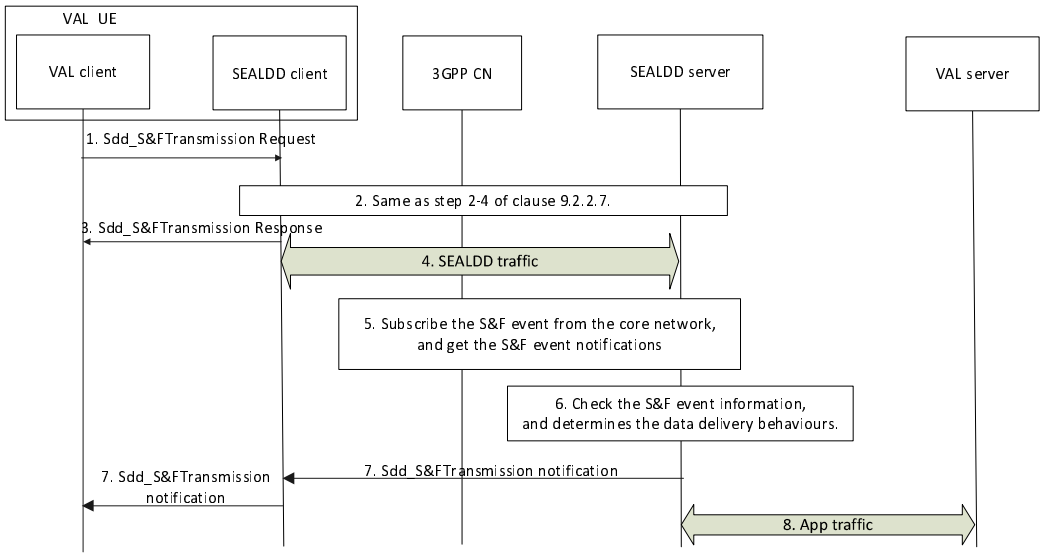

Figure 10.2.2.2-1: Client initiated data transmission for delay-tolerant satellite services

1. The VAL client decides to use SEALDD service for delay-tolerant traffic transfer.
2. Same as steps 2-4 of clause 9.2.2.7.
3. The SEALDD client provides the acknowledgment for the request made in step 1.
4. The SEALDD client sends the UL data to the SEALDD server via the 3GPP network.
5. The SEALDD server subscribes the recipient S&F satellite operation information from the 3GPP CN as specified in clause 5.6.3.10 of 3GPP TS 23.682 [24] and is notified about the recipient UE S&F satellite operation information e.g., whether UE is registered in S&F Mode, the estimated S&F DL delivery time. The SEALDD server stores the received recipient UE S&F status events information for further control the downlink application data transmission.

Editor's note: How SEALDD server knows the recipient UE information is FFS.

6. The SEALDD server controls the downlink application data delivery to the SEALDD client based on the UE S&F status events information, when the recipient UE is in S&F mode and receives the estimated S&F DL delivery time is received from 3GPP CN. If the recipient UE is not available or not registered to S&F mode, then the SEALDD server handles the DL data as per the service policy.
7. The SEALDD server sends the Sdd_S&FTransmission_notification to the SEALDD client and VAL client including the estimated S&F DL delivery time of the recipient UE.

NOTE 1: VAL client can use the estimated S&F DL delivery time of the recipient UE to control the UL application data delivery.

8. The SEALDD server sends the DL data to the VAL server.

NOTE 2: Details of step 1, step 3 and step 7 are out of scope of the current specification.

10.2.3 Information flows

10.2.3.1 SEALDD enabled DTwithS&F transmission request

Table 10.2.3.1-1 describes the information flow from the VAL server to the SEALDD server for requesting the delay-tolerant with S&F application transmission service.

Table 10.2.3.1-1: SEALDD enabled DTwithS&F transmission request

Information element	Status	Description
VAL server ID	M	Identity of the VAL server
VAL service ID	O	Identity of the VAL service
Identity	M	Identifier of specific UE or VAL user
SEALDD-S Data transmission connection information	M	Address/port and/or URL of the VAL server to receive the application packets from the SEALDD server.
DL data delivery status subscription indication	O	Indicates the VAL server expected to receive the DL delivery status notification

10.2.3.2 SEALDD enabled DTwithS&F transmission response

Table 10.2.3.2-1 describes the information flow from the SEALDD server to the VAL server for responding to the delay-tolerant with S&F application transmission.

Table 10.2.3.2-1: SEALDD enabled DTwithS&F transmission response

Information element	Status	Description
Result	M	Success or failure.
SEALDD-S information Data transmission connection information	O	Address/port and/or URL of the SEALDD server to receive the packets from the VAL server for application traffic transfer
Cause	O (see NOTE)	Indicates the reason for the failure, e.g. SEALDD policy mismatch.
NOTE: The IE is only present if the Result is failure.		

10.2.3.3 SEALDD DTwithS&F transmission notification

Table 10.2.3.3-1 describes the information flow from the SEALDD server to the VAL server to notify S&F delivery related events.

Table 10.2.3.3-1: SEALDD DL delivery notification

Information element	Status	Description
Event ID	O (see NOTE)	Identifies event SEALDD client connection status for DL data delivery e.g., reachable, unreachable, sleeping.
DL data delivery instructions	O (see NOTE)	Indicates the instructions to the VAL server regarding the DL data delivery
> Adjust DL data volume	O	Indicates adjusting DL data volume with suggested traffic volume
> Pending DL data delivery	O	Indicates pending DL data delivery due to e.g., feeder link is not available
> Resume DL data delivery	O	Indicates pending DL data delivery due to e.g., feeder link is available
Identity	M	Identifier of VAL UE or VAL user.
VAL service ID	O	Identity of the VAL service.
NOTE: Either Event ID IE or the DL data delivery instruction ID is present.		

10.2.3.4 Sdd_S&FTransmission_notification

Table 10.2.3.4-1 describes the information flow from the SEALDD server to the SEALDD Client to notify the DL estimated delivery time.

Table 10.2.3.4-1: Sdd_S&FTransmission_notification

Information element	Status	Description
VAL server ID	M	Identity of the VAL server
VAL service ID	O	Identity of the VAL service.
Identity	M	Identifier of specific UE or VAL user
Identity	M	Identifier of specific recipient UE or VAL user
> DL estimated delivery time	M	DL estimated delivery time for a recipient UE

Annex A (informative): Deployment models

The SEALDD service can be deployed as a generic SEAL service and hence the deployment models for SEALDD service utilizes the deployment models specified in clause 8 of 3GPP TS 23.434 [4]. In the context of SEALDD service the following rules apply:

- The SEAL server is the SEALDD server;
- The SEAL-S reference point is the SEALDD-S reference point; and
- The SEAL-E reference point is the SEALDD-E reference point.

Annex B (Informative): Message delivery option: Utilizing MSGin5G

B.1 General

MSGin5G provides a data delivery messaging service in 5GS especially for enabling IoT device communications. It has been specified starting with Rel-17 in 3GPP TS 23.554 [9]. SEALDD is proposed as a generic data delivery enabler layer for all the verticals utilizing SEAL. It is beneficial to deploy one unified data delivery system suitable for all kinds of terminals to reduce the complexity of vertical applications.

B.2 SEALDD utilizing MSGin5G

MSGin5G functionalities described in 3GPP TS 23.554 [9] are integrated in SEALDD enabler layer. As shown in Figure B.2-1, MSGin5G client functionality is integrated in SEALDD client, and MSGin5G server functionality is integrated in SEALDD server. SEALDD server and SEALDD client can use MSGin5G functionalities to send SEALDD traffic in MSGin5G message format.

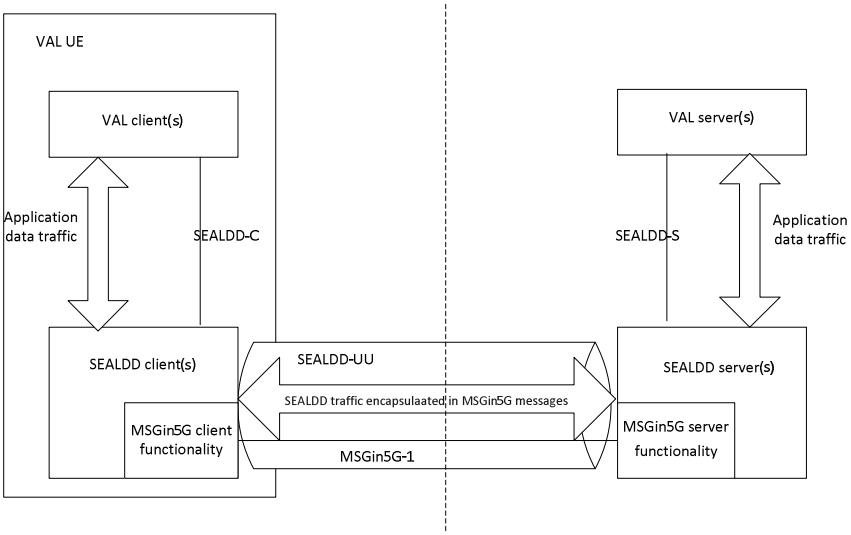

Figure B.2-1 SEALDD utilizing MSGin5G

Annex C (Informative): Overall lifecycle of SEALDD service

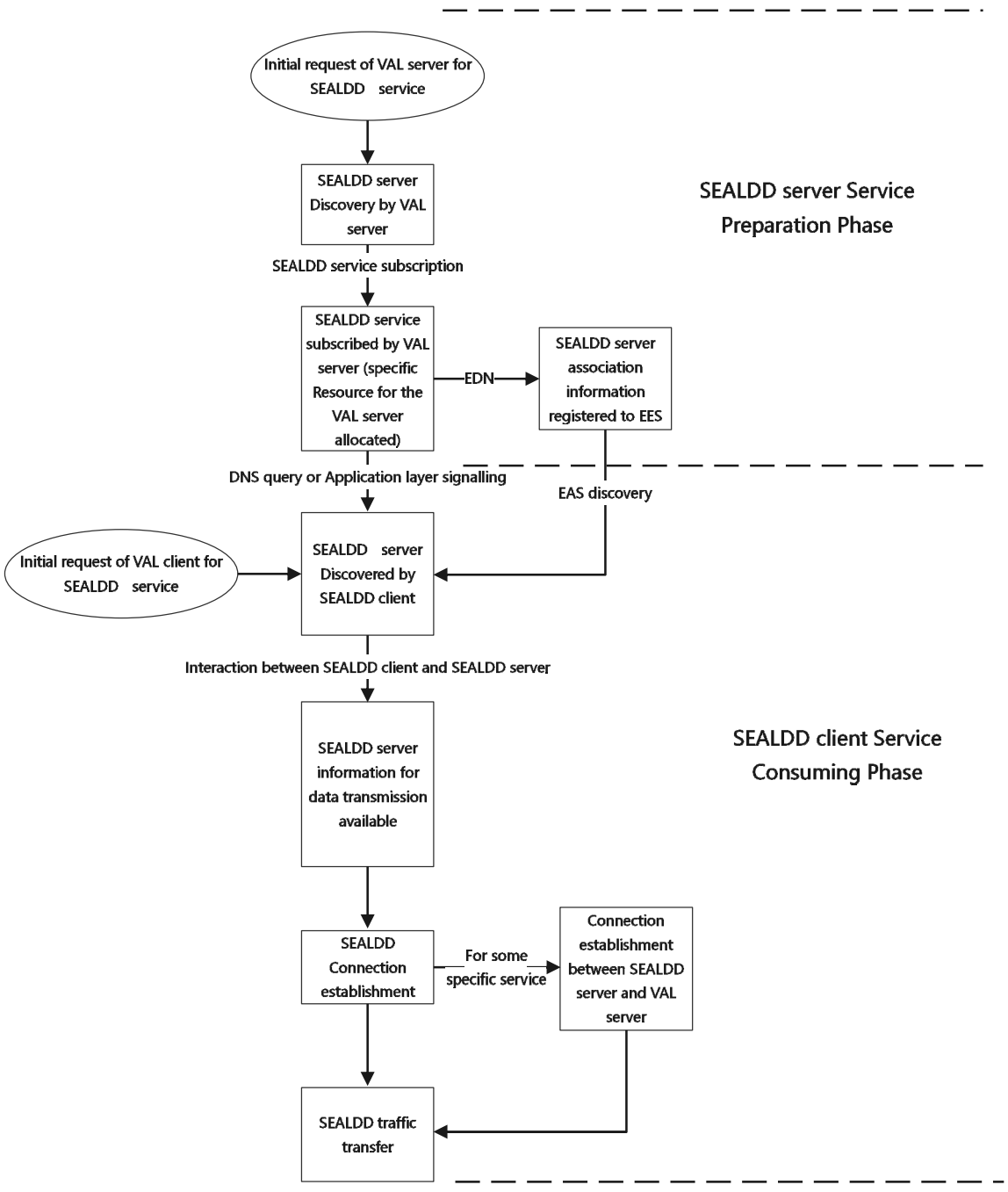

Figure C-1: Overall lifecycle of SEALDD

As shown in Figure C-1, the whole lifecycle of SEALDD to establish the SEALDD connection for the VAL client and VAL server includes two phases:

1. SEALDD server Service Preparation Phase (This Phase is used by the VAL server to get SEALDD server prepared for SEALDD client access):

(1) When the VAL server decides to use the SEALDD service for data transmission enhancement, it discovers the SEALDD server (e.g. by CAPIF).

(2) Then the VAL server triggers SEALDD service subscription procedure to the discovered SEALDD server, in that procedure, SEALDD server is associated with the VAL server, and specific SEALDD server resource (e.g. address/port of the SEALDD server for redundant transmission) is allocated for the VAL server's service to transfer SEALDD traffic.

(3) For EDN scenario, the SEALDD server or VAL server will register the association information to the EES.

2. SEALDD client Service Consuming Phase (When SEALDD server is prepared in SEALDD server Service Preparation Phase, the VAL client(s) can trigger SEALDD client to connect to specific prepared SEALDD server for SEALDD service):

(1) When VAL client request to use SEALDD service to transmit the VAL traffic to VAL server, the VAL client or SEALDD client can discover the proper SEALDD server associated with the VAL server (e.g. via EAS discovery, DNS query, pre-configuration or Application layer signalling).

(2) Then SEALDD client can interact with SEALDD server to negotiate for SEALDD data transfer. If Address/Port is allocated in SEALDD service subscription phase, it will be notified to SEALDD client in this step.

(3) Data transmission connection is established between the SEALDD client and SEALDD server for SEALDD traffic transfer.

(5) The whole configuration is accomplished and the VAL traffic is transferred via the SEALDD connection.

Annex D (Informative): Media data delivery in SEALDD

D.1 General

The SEALDD layer provides a general functionality to support data storage and data delivery by introducing 5G interaction (N5/N33 in control plane, N6 in user plane), including application data storage and management, application signalling and data transmission, E2E URLCC transmission, IoT message transmission (i.e. MSGin5G), etc.

D.2 SEALDD deployment for media delivery

For media delivery functionality in SEALDD, as shown in Figure D.2-1, the functionality/protocol defined in SA4 can be reused and further enhanced by SEALDD for supporting media type traffic, 5GMS/RTC AF and 5GMS RTC AS in 3GPP TS 26.501 [14] and 3GPP TS 26.506 [15] is utilized in SEALDD server to support the general media type delivery. The 5G transmission adaptation component is added in SEALDD, to facilitate the specific optimization for XR application provided by 5G network.

NOTE: The functionality about 5G transmission adaptation component for media type will be further detailed based on the other progresses (e.g. application enabler for XR Services).

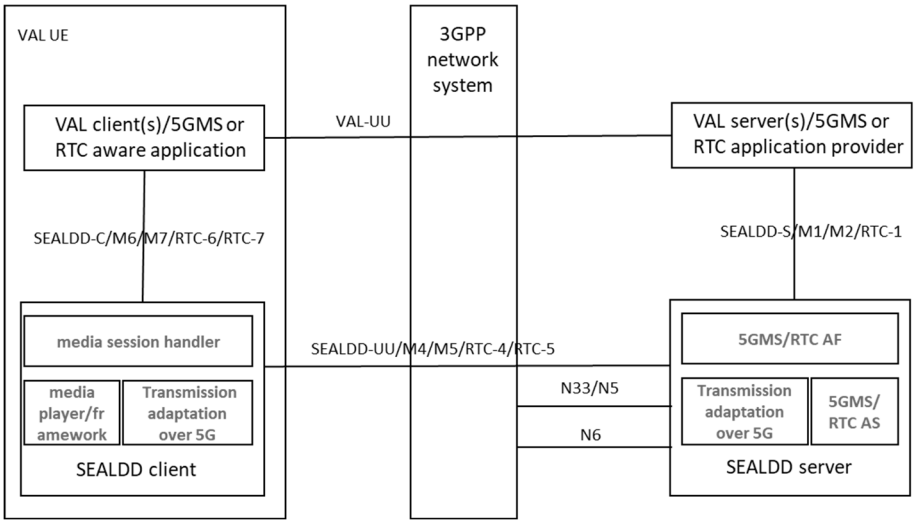

Figure D.2-1: SEALDD deployment for media delivery

When utilizing the SEALDD to deliver the media stream, the SEALDD server integrates the 5GMS/RTC AF and 5GMS/RTC AS, the SEALDD client integrates as the media session handler and the media player/framework, and follows the support the uplink media transmission and the downlink media transmission defined in 3GPP TS 26.501 [14] and 3GPP TS 26.506 [15]. The SEALDD-UU integrates the M4 and M5 interfaces of 5GMS according to 3GPP TS 26.501 [14], and the RTC-4 and RTC-5 interfaces of 5G RTC system according to 3GPP TS 26.506 [15]. The SEALDD-S integrates the M1 and M2 interfaces of 5GMS according to 3GPP TS 26.501 [14], and the RTC-1 interface of 5G RTC system according to 3GPP TS 26.506 [15].

Annex E (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-10	SA6#51-e					TS skeleton (S6-222790)	0.0.0
2022-10	SA6#51-e					Implementation of the following pCRs approved by SA6: S6-222984, S6-222986, S6-223040, S6-223041, S6-223042, S6-223043, S6-223044	0.1.0
2022-11	SA6#52					Implementation of the following pCRs approved by SA6: S6-223432, S6-223433, S6-223434, S6-223568	0.2.0
2022-12	SA#98-e	SP-221218				Submitted to SA#98-e for information	1.0.0
2023-01	SA6#52-bis-e					Implementation of the following pCRs approved by SA6: S6-230195, S6-230253, S6-230375, S6-230442, S6-230477, S6-230478, S6-230479, S6-230480, S6-230481	1.1.0
2023-03	SA6#53					Implementation of the following pCRs approved by SA6: S6-230611, S6-230725, S6-230868, S6-230869, S6-230870, S6-230871, S6-230872, S6-230873, S6-230877, S6-230879, S6-230880, S6-230881, S6-230882, S6-230883, S6-231045, S6-231046, S6-231047	1.2.0
2023-04						Moved clause 9.7.2.3 to clause 9.9.2.2 as per the approved pCR in S6-230880	1.2.1
2023-04	SA6#54-e					Implementation of the following pCRs approved by SA6: S6-231297, S6-231298, S6-231300, S6-231330, S6-231365, S6-231485, S6-231554, S6-231558, S6-231559, S6-231560, S6-231561, S6-231562, S6-231564, S6-231565, S6-231637, S6-231638, S6-231639, S6-231640	1.3.0
2023-05	SA6#55					Implementation of the following pCRs approved by SA6: S6-231881, S6-231882, S6-232041, S6-232042, S6-232043, S6-232044, S6-232045, S6-232047, S6-232048, S6-232049, S6-232050, S6-232051, S6-232052, S6-232053, S6-232063, S6-232179, S6-232209	1.4.0
2023-06	SA#100	SP-230685				Submitted to SA#100 for approval	2.0.0
2023-06	SA#100	SP-230685				MCC Editorial update for publication after TSG SA approval (SA#100)	18.0.0
2023-09	SA#101	SP-231010	0001	1	F	Introducing cause field and transfer of SEALDD server policy information in context transfer procedure	18.1.0
2023-09	SA#101	SP-231010	0002	1	F	SEALDD client initiated connection release	18.1.0
2023-09	SA#101	SP-231010	0003	1	F	Add the missing SEALDD policy delete procedure	18.1.0
2023-09	SA#101	SP-231010	0004	1	F	Correct performance info in SEALDD server discovery	18.1.0
2023-09	SA#101	SP-231010	0005	2	F	Update the SEALDD server discovery procedure	18.1.0
2023-09	SA#101	SP-231010	0006		F	Correction for regular transmission procedure	18.1.0
2023-09	SA#101	SP-231010	0007	1	F	Align the transmission quality report information	18.1.0
2023-09	SA#101	SP-231010	0009	1	F	Adding the SEALDD overall lifecycle	18.1.0
2023-12	SA#102	SP-231567	0013	1	F	Add missing information flow for transmission quality guarantee	18.2.0
2023-12	SA#102	SP-231567	0014		F	Correct message name in policy driven connection management	18.2.0
2023-12	SA#102	SP-231567	0017		F	Terminology alignment for transmission guarantee procedure	18.2.0
2023-12	SA#102	SP-231567	0018		F	Correction for E2E redundant transmission procedure	18.2.0
2023-12	SA#102	SP-231567	0019	1	F	Align the transmission quality analytics with ADAE server	18.2.0
2023-12	SA#102	SP-231567	0022		F	Correction SEALDD context pull request	18.2.0
2023-12	SA#102	SP-231567	0025	2	F	Complete information flow and API for transmission quality measurement procedure	18.2.0
2023-12	SA#102	SP-231567	0026	2	F	Adding the consumer for data transmission quality query procedure	18.2.0
2023-12	SA#102	SP-231567	0027	1	F	Clarification on SEALDD regular data transmission procedure	18.2.0
2023-12	SA#102	SP-231567	0028	2	F	Correction for quality guarantee policy	18.2.0
2023-12	SA#102	SP-231568	0015	2	B	SEALDD transmission quality guarantee with BAT and periodicity adaptation	19.0.0
2023-12	SA#102	SP-231568	0016	1	B	Policy triggered redundant connection management	19.0.0
2023-12	SA#102	SP-231568	0020	2	F	Clarification on media delivery functionality in SEALDD	19.0.0
2023-12	SA#102	SP-231568	0021	6	B	Correction on SEALDD enabled congestion control for VAL application by supporting L4S mechanism	19.0.0
2023-12	SA#102	SP-231568	0023	2	B	Provisioning a Geofence policy in the SEALDD server	19.0.0
2023-12	SA#102	SP-231568	0024	3	B	Enhancements to the SEALDD connection status procedure	19.0.0
2024-03	SA#103	SP-240316	0029	1	F	Clarification on content delivery in SEALDD-S interface	19.1.0
2024-03	SA#103	SP-240316	0030	2	F	Clarification on media delivery functionality in SEALDD	19.1.0
2024-03	SA#103	SP-240316	0032	3	B	Seamless SEALDD relocation enhancement	19.1.0
2024-03	SA#103	SP-240309	0034		A	Alignment on VAL UE identity and VAL user identity	19.1.0
2024-03	SA#103	SP-240309	0036	2	A	Complete API for regular data transmission procedure	19.1.0
2024-03	SA#103	SP-240309	0038	1	A	Complete API for stored data transfer procedure	19.1.0
2024-03	SA#103	SP-240309	0042	1	A	Add release operation for URLLC connection	19.1.0
2024-03	SA#103	SP-240309	0044	2	A	Correct NRM and SEALDD interaction	19.1.0
2024-03	SA#103	SP-240309	0046		A	Correct regular transmission procedure	19.1.0
2024-03	SA#103	SP-240309	0048		A	Correct Sdd_TransmissionQualityMeasurement API	19.1.0
2024-03	SA#103	SP-240309	0050		A	Correct URLLC transmission procedure	19.1.0

2024-03	SA#103	SP-240316	0051	3	B	SEALDD Background data transfer	19.1.0
2024-03	SA#103	SP-240316	0052		F	Correct IE presence condition	19.1.0
2024-06	SA#104	SP-240769	0055	3	F	Functional model update to introduce the SEALDD UU-U and SEALDD S-U	19.2.0
2024-06	SA#104	SP-240769	0057	1	F	Clarification on connection and flow in SEALDD	19.2.0
2024-06	SA#104	SP-240769	0059	1	F	Clarification on the identifier of stored data from multiple SEALDD servers	19.2.0
2024-06	SA#104	SP-240769	0060	1	F	Resolve Editor's notes about SEALDD query procedure	19.2.0
2024-06	SA#104	SP-240769	0061	1	F	Update SEALDD connection status procedure	19.2.0
2024-06	SA#104	SP-240763	0063	1	A	Alignment on data transmission connection establishment and release procedure re	19.2.0
2024-06	SA#104	SP-240763	0065	1	A	Correction on E2E redundant transmission procedure	19.2.0
2024-06	SA#104	SP-240763	0067	1	A	Correction on SEALDD server discovery and selection procedure	19.2.0
2024-06	SA#104	SP-240769	0068	1	F	Correct SEALDD connection status event	19.2.0
2024-06	SA#104	SP-240763	0070	2	A	Correct context IE table	19.2.0
2024-06	SA#104	SP-240769	0071	2	B	Add client-initiated SEALDD connection establishment	19.2.0
2024-06	SA#104	SP-240769	0072		F	Correct BDT IE table	19.2.0
2024-06	SA#104	SP-240769	0073		F	Correct SEALDD quality measurement subscription response	19.2.0
2024-06	SA#104	SP-240769	0074	3	F	Clarification about SEALDD enabled connection establishment based on policy	19.2.0
2024-09	SA#105	SP-241232	0075	1	B	Support of QoS measurement for Multi-Modal traffic in SEALDD layer	19.3.0
2024-09	SA#105	SP-241227	0077		F	Correction for SEALDD enabled L4S congestion control	19.3.0
2024-09	SA#105	SP-241216	0079	1	A	Correction for SEALDD server discovery for SEALDD client	19.3.0
2024-09	SA#105	SP-241232	0080	2	B	SEALDD policy configuration for multi-modal flows	19.3.0
2024-09	SA#105	SP-241232	0082	4	B	PDU set handling	19.3.0
2024-09	SA#105	SP-241227	0083	1	F	Correct API operation input output	19.3.0
2024-09	SA#105	SP-241227	0084		F	Seamless SEALDD server relocation	19.3.0
2024-12	SA#106	SP-241733	0086	3	B	Multi-modal SEALDD flow identifier	19.4.0
2024-12	SA#106	SP-241733	0087	2	B	Architecture update to support the tethered UE based on PINAPP	19.4.0
2024-12	SA#106	SP-241733	0088	3	B	Add new feature to support the tethered UE	19.4.0
2024-12	SA#106	SP-241733	0089	6	B	Add new feature to support the Multi-modal flows alignment and monitoring	19.4.0
2024-12	SA#106	SP-241729	0090		F	Correct BAT adaptation	19.4.0
2024-12	SA#106	SP-241729	0091		D	Correct SEALDD-Uu	19.4.0
2024-12	SA#106	SP-241733	0092	1	B	Support UE-to-UE communication	19.4.0
2024-12	SA#106	SP-241711	0095	1	A	Correction to APIs exposed by SEALDD client side	19.4.0
2024-12	SA#106	SP-241729	0096	1	F	Completion of SEALDD enabled URLLC transmission connection based on policy	19.4.0
2024-12	SA#106	SP-241729	0097		F	Completion of SEALDD Background data transfer	19.4.0
2024-12	SA#106	SP-241729	0098	1	F	Clarification on SEALDD server discovery and determination	19.4.0
2024-12	SA#106	SP-241729	0100		F	Correction on NOTE in clause 9.2.2.1	19.4.0
2024-12	SA#106	SP-241729	0102	1	F	Correction on SEALDD data transmission connection establishment message	19.4.0
2024-12	SA#106	SP-241729	0103	1	F	Correction on SEALDD enabled regular data transmission connection establishment procedure	19.4.0
2024-12	SA#106	SP-241729	0104	1	F	Fix the inconsistency on SEALDD enabled signalling transmission connection establishment procedure	19.4.0
2024-12	SA#106	SP-241733	0108	2	B	XR architecture based on SEALDD architecture	19.4.0
2024-12	SA#106	SP-241717	0109	4	B	SEALDD enabled S&F transmission	19.4.0
2024-12	SA#106	SP-241729	0110	1	B	SEALDD enabled data transmission quality guarantee using a Non-3GPP RAT	19.4.0
2024-12	SA#106	SP-241729	0111	1	B	XR Application Client Capability Information Request Procedure	19.4.0
2024-12	SA#106	SP-241733	0114	1	B	SEALDD-UUc Cardinality rule	19.4.0
2024-12	SA#106	SP-241733	0115	1	B	Support the user group level QoS guarantee	19.4.0
2024-12	SA#106	SP-241729	0117		F	Correction the description on clause 9.2.2.1	19.4.0
2024-12	SA#106	SP-241729	0118	1	F	Fix the inconsistency on SEALDD connection information in clause 9.3	19.4.0
2024-12	SA#106	SP-241729	0119	2	F	Fix the inconsistency on SEALDD connection information in clause 9.3	19.4.0
2024-12	SA#106	SP-241733	0120	2	B	Support for Multi-modal flows synchronization monitoring	19.4.0
2024-12	SA#106	SP-241733	0121	2	B	Adding SEALDD Adaptive XR Data Transmission Service	19.4.0
2024-12	SA#106	SP-241729	0122		F	Correction on SEALDD URLLC transmission connection establishment request	19.4.0
2024-12	SA#106	SP-241729	0123	1	F	Correction on Mode of reporting	19.4.0
2025-03	SA#107	SP-250217	0125	2	B	Address the EN in UE-to-UE communication	19.5.0
2025-03	SA#107	SP-250217	0127	1	F	Remove the EN about multi-modal flow synchronization and crossflow measurement	19.5.0
2025-03	SA#107	SP-250217	0128	1	B	Add update and delete service operation of SEALDD client policy configuration	19.5.0
2025-03	SA#107	SP-250215	0129		F	Informative wording corrections	19.5.0
2025-03	SA#107	SP-250215	0130	1	D	Corrections to 3GPP spec reference	19.5.0

2025-03	SA#107	SP-250215	0131	1	D	NOTE number correction	19.5.0
2025-03	SA#107	SP-250215	0132	1	D	Add missing figures to clause 9.12.2.3	19.5.0
2025-03	SA#107	SP-250215	0133	2	D	Message name style alignment	19.5.0
2025-03	SA#107	SP-250217	0134	1	F	Add service operation of Crossflow measurement and delay difference for XR application	19.5.0
2025-03	SA#107	SP-250217	0135	2	B	Multi-Modal traffic indication in SEALDD layer	19.5.0
2025-03	SA#107	SP-250215	0136		F	Correction on mode of reporting	19.5.0
2025-03	SA#107	SP-250215	0137		F	Corrections to non-3GPP access measurements	19.5.0
2025-03	SA#107	SP-250217	0139		F	Solving Editor's Notes on PDU set an RTT	19.5.0
2025-03	SA#107	SP-250217	0140	2	B	Completion of SEALDD-enabled flow Alignment procedure	19.5.0
2025-03	SA#107	SP-250205	0141	2	B	Client initiated data transmission	19.5.0
2025-06	SA#108	SP-250621	0142	1	F	Update SEALDD XR transmission connection establishment information flow	19.6.0
2025-06	SA#108	SP-250616	0143		F	Correction to server initiated SEALD data transmission connectivity	19.6.0
2025-06	SA#108	SP-250592	0144	5	F	Correction to SEALDD enabled S&F transmission	19.6.0
2025-06	SA#108	SP-250616	0145		F	Correction on SEALDD enabled data transmission quality guarantee with redundant transport	19.6.0
2025-06	SA#108	SP-250616	0146	1	F	Clarification on SEALDD enabled XR data transmission service for XR application	19.6.0
2025-06	SA#108	SP-250592	0147	2	F	Corrections and alignments of clause 10.2.2	19.6.0
2025-06	SA#108	SP-250616	0149	1	D	Clarification on the SEALDD client policy configuration request	19.6.0
2025-06	SA#108	SP-250616	0150	2	F	Clarification on SEALDD client policy configuration	19.6.0
2025-06	SA#108	SP-250616	0151	2	F	Alignment of the Multi-modal SEALDD flow ID and clarification of the redundant Synchronization policy	19.6.0
2025-06	SA#108	SP-250616	0152	1	F	Corrections to message names	19.6.0
2025-09	SA#109	SP-251064	0153	2	F	Add service overview on SEALDD enabled transmission for XR application	19.7.0
2025-09	SA#109	SP-251064	0155	1	F	Correction to L4S Feedback capability	19.7.0
2025-09	SA#109	SP-251064	0156		F	Clarification in SEALDD enabled bandwidth control procedure for XR application	19.7.0
2025-09	SA#109	SP-251064	0157		F	Clarification in SEALDD connection status	19.7.0
2025-09	SA#109	SP-251067	0158	1	C	Enhancements to SEALDD rate control to support rejected clients	19.7.0
2025-09	SA#109	SP-251068	0159		F	Addition of Information elements for protocol description for SEALDD XR transmission connection establishment response	19.7.0
2025-10	SA#109	SP-251067	0158	1	C	The present CR0158 rev 1 is removed from the Rel-19 as it is intended to be a Rel-20 CR	19.7.1

History

Document history		
V19.7.1	October 2025	Publication