ETSI TS 123 433 V18.4.0 (2024-07)

LTE;
5G;
Service Enabler Architecture Layer for Verticals (SEAL);
Data Delivery enabler for vertical applications
(3GPP TS 23.433 version 18.4.0 Release 18)

Reference
RTS/TSGS-0623433vi40

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

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

Trademarks

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

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

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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".

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].

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 signaling 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 can establish 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 can provide 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 can provide 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 can maintain 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.

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.

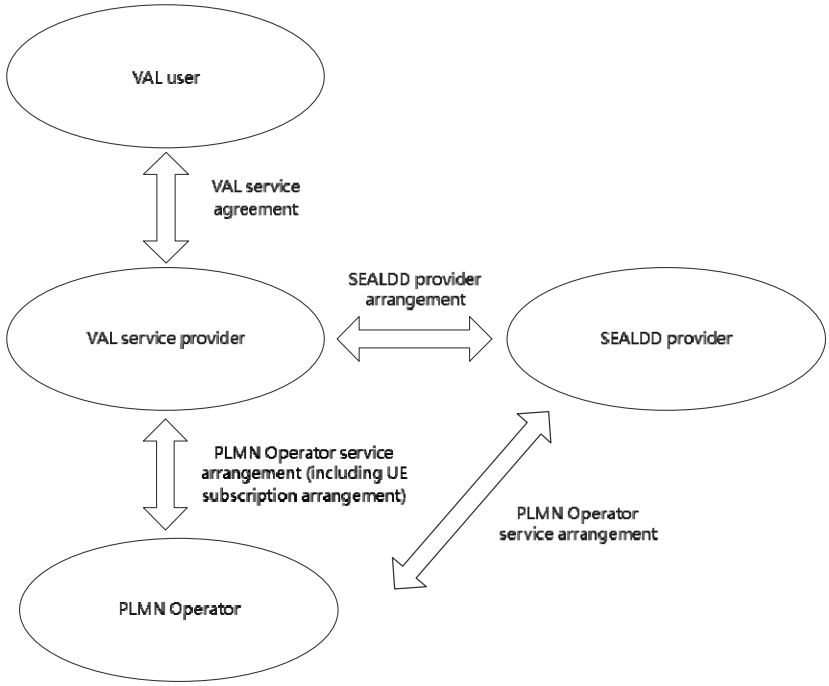

Figure 5.2-1: Business relationship option-A for VAL services

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

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

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

The PLMN operator can have PLMN operator service arrangements with multiple VAL service providers and the VAL service provider can have PLMN operator service arrangements with multiple PLMN operators. As part of the PLMN operator service arrangement between the VAL service provider and the PLMN operator, PLMN subscription arrangements can 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.

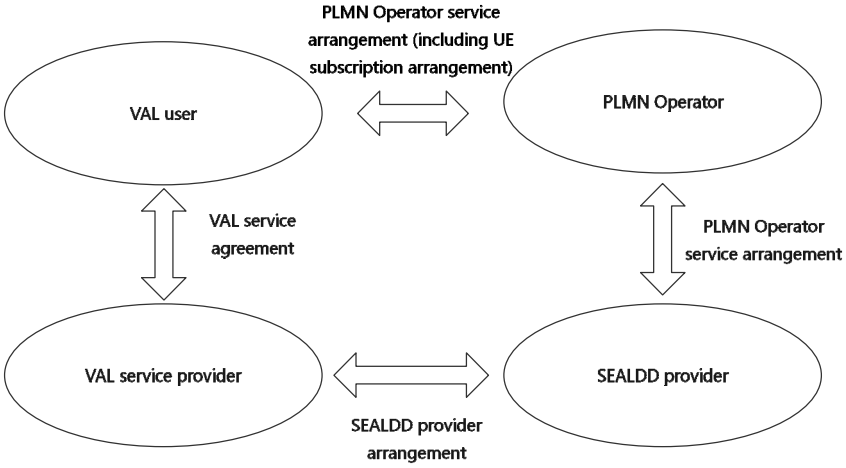

Figure 5.3-1: Business relationship option-B for VAL services

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

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

The PLMN operator can have PLMN operator service arrangements with multiple SEALDD service providers and the SEALDD service provider can have PLMN operator service arrangements with multiple PLMN operators. The SEALDD service provider and the PLMN operator can 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.

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].

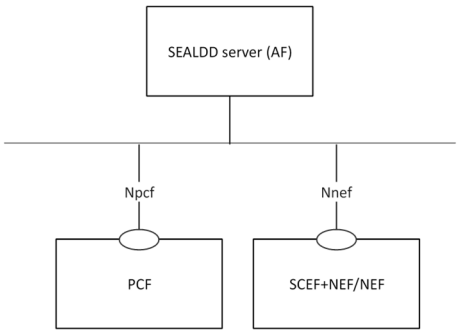

Figure 7.2-1: Utilization of 5GS network services based on the 5GS SBA – service based representation

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.

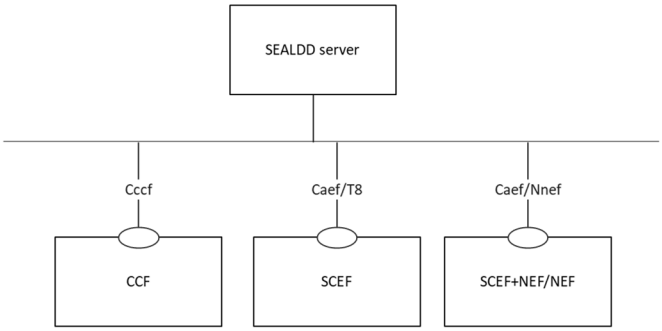

Figure 7.2-2: Utilization of Core Network Northbound APIs via CAPIF – service based representation

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.

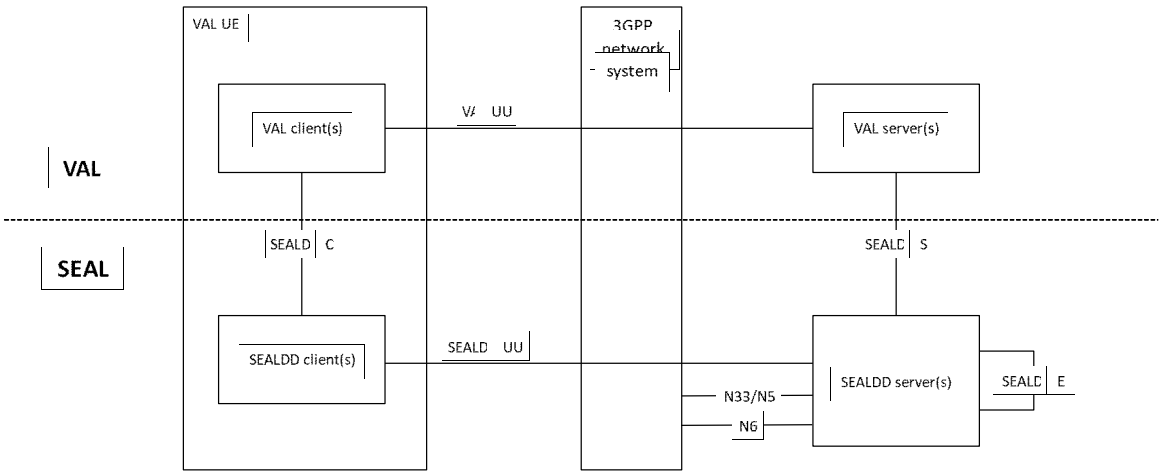

Figure 7.2-3 Architecture for SEAL Data Delivery Service

The SEALDD server can communicate 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.

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).

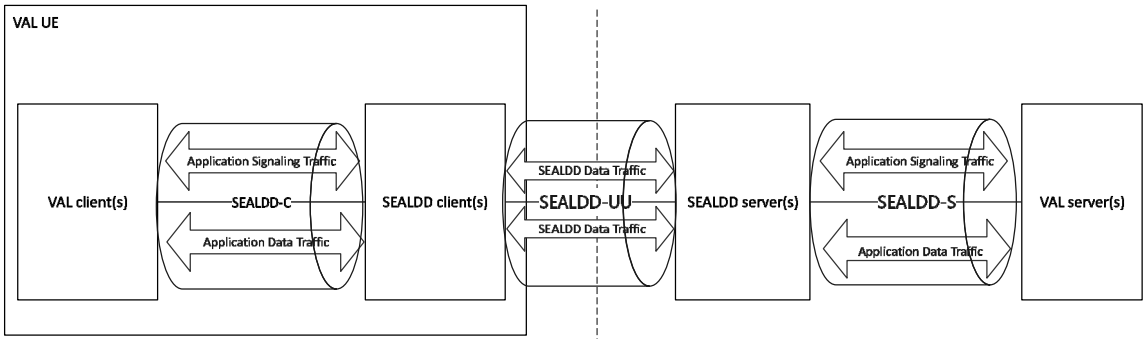

Figure 7.2-4: Architecture for application traffic transfer

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.

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) Supporting the transmission for application signalling data and application media/data, by using 3GPP network.

b) Providing the application data/media handling capabilities (e.g. storage, management, transmission).

c) 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.

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) Supporting the transmission for application signalling data and application media/data, by using 3GPP network.

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

Reference point between SEALDD client and SEALDD server used to transfer data content and exchange 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.

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

7.4.4 SEALDD-S

Reference point between SEALDD server and VAL server to enable northbound server side API exposed by SEALDD server to VAL server for data delivery and SEALDD service provisioning, control, reporting etc.

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.

7.5 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.

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 flow ID

The SEALDD flow ID is used by the SEALDD client and SEALDD server to identify different VAL application traffic.

9 Procedures and information flows

9.1 General

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

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

For the uplink traffic transmission, the SEALDD server can 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 can pull the data/content of VAL application from the SEALDD server.
- Uplink push mode: the SEALDD server can push the data/content of VAL application to the address provided by the VAL server (i.e. data/content address in VAL server, 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 flow) is uniquely identified in the SEALDD layer by the SEALDD flow ID. The specific procedures detailed in the subsequent clauses are for cases in which the SEALDD regular connection is used respectively for application signaling, application data delivery initiated by VAL server, and application data delivery initiated based on DD policy.

NOTE: 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.

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 can discover and select the SEALDD server by CAPIF functions.

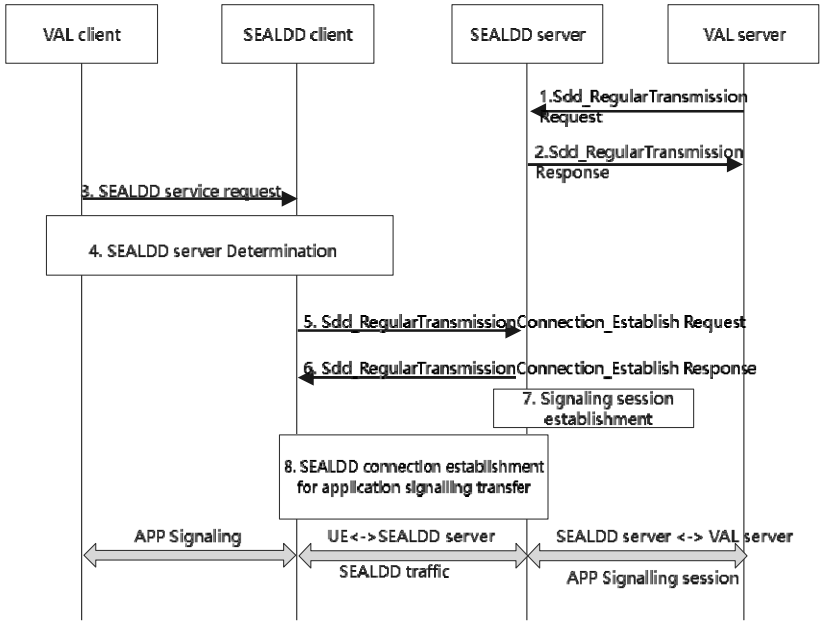

Figure 9.2.2.1-1: SEALDD signalling transmission connection establishment procedure

1. The VAL server decides to use SEALDD service for application signalling transfer and allocates address/port as SEALDD-S Data transmission connection information for receiving the application signalling packets 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 traffic, the 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, the SEALDD server allocates a specific address or port used for SEALDD traffic transfer with the incoming SEALDD client(s) for the VAL server and responds with a SEALDD service response.

NOTE 1: The SEALDD server does not allocate address/port in this step and VAL server treats the SEALDD-S Data transmission connection information as wildcard endpoint 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, the SEALDD client can get the SEALDD server's address.

5. The SEALDD client allocates a SEALDD flow ID mapping to application traffic for application signalling transmission. The SEALDD client sends Sdd_RegularTransmissionConnection_Establish request to SEALDD server with the SEALDD client ID, the SEALDD flow ID, VAL server ID, VAL service ID and the SEALDD traffic descriptor of the SEALDD client side (the address/port of the SEALDD client for receiving the downlink SEALDD traffic). The request message also contains the selected VAL server endpoint information.

NOTE 2: The SEALDD flow ID is used by the SEALDD client and SEALDD server to identify different application 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. address/port allocated in step 2, transport layer protocol) mapping to the application traffic.

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

8. The SEALDD client uses the SEALDD traffic descriptor of SEALDD server side for SEALDD 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 address/port 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 UE's address/port and SEALDD server's address/port for the SEALDD traffic transmission). The SEALDD client gets the mapping information (i.e. SEALDD flow ID for the application signalling transfer). The SEALDD server gets the mapping information between the SEALDD 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 flow ID. The SEALDD server sends the recovered 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 can respond to the source address/port (SEALDD-S address/port 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 can map the downlink application signalling traffic to the related SEALDD client ID and SEALDD 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 can communicate 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 can discover and select the SEALDD server by CAPIF functions.

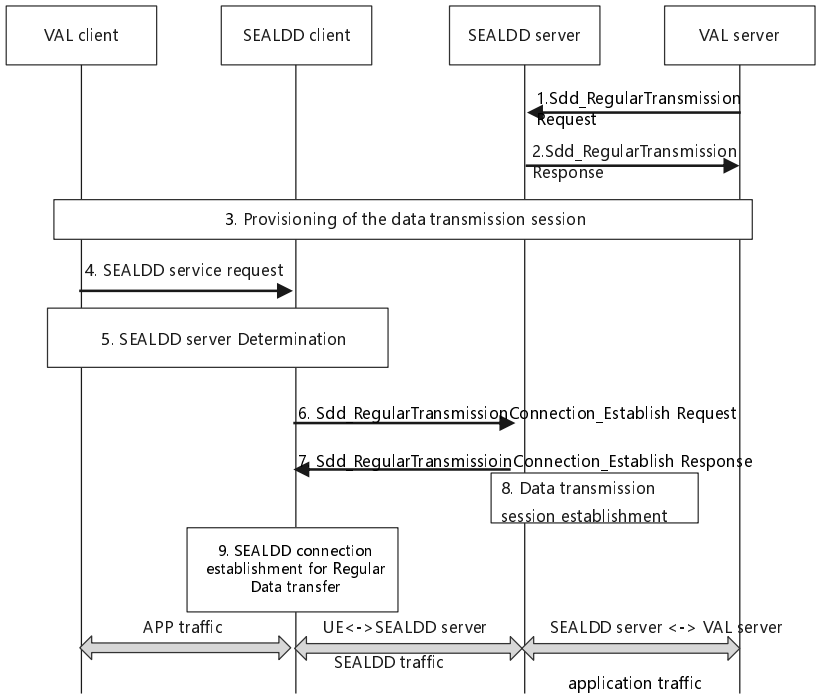

Figure 9.2.2.2-1: SEALDD enabled regular data transmission connection establishment procedure

1. The VAL server decides to use SEALDD service for application 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_RegularTransmission 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, 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 address/port 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 allocates a specific address or port used for SEALDD traffic transfer with the specific UE for the VAL server and responds with a SEALDD service response (including SEALDD-S data transmission connection information of the SEALDD server side). The VAL server and SEALDD server can use SEALDD-S data transmission 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 address or ports 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 data transmission 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.

NOTE 2: 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. The response indicates that whether the SEALDD service request is successful or not.

5. 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 can get the SEALDD server's address.

6. The SEALDD client allocates a SEALDD flow ID 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 flow ID, the SEALDD traffic descriptor of the SEALDD client side (the address/port 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.

NOTE 3: 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 4: The SEALDD flow ID is used by the SEALDD client and SEALDD server to identify different VAL application traffic of the same SEALDD client. The SEALDD 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/port allocated in step 2, transport layer protocol) mapping to the application 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 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/port and SEALDD server's address/port for the SEALDD traffic transmission).

After the negotiation and establishment of the connections, the SEALDD client gets the mapping information between application traffic and SEALDD flow ID. The SEALDD server gets the mapping information between the SEALDD flow ID and the SEALDD-S connection. Upon receiving application 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 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.

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.

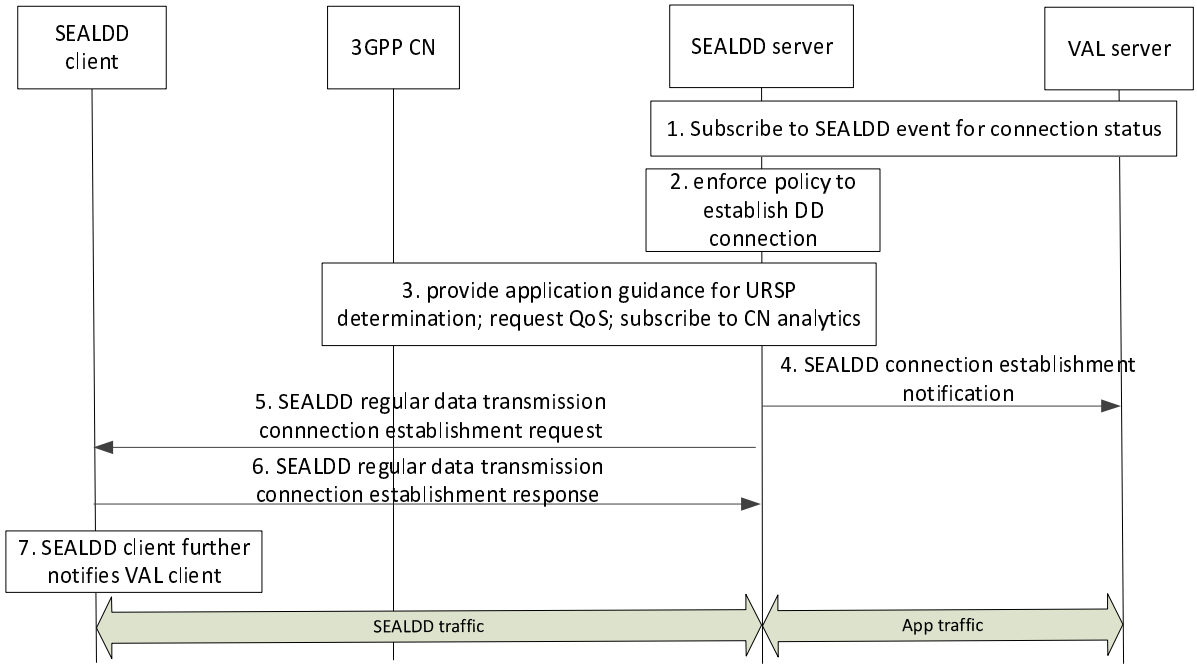

Figure 9.2.2.3-1: Policy enforced by SEALDD server for connectivity

1. The VAL server subscribes to SEALDD event exposure for connection status.

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 IP address and port.

5-6. The SEALDD server allocates an IP address and port for sending and receiving packet over SEALDD-UU reference point, then SEALDD server sends regular data transmission connection establishment request to the SEALDD client with SEALDD flow ID, VAL service ID, the IP address and port. The request is responded by the SEALDD client. 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.

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

NOTE 3: Step 5 can be sent via PDU session (if exist) or via application triggering (if no PDU session exists).

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

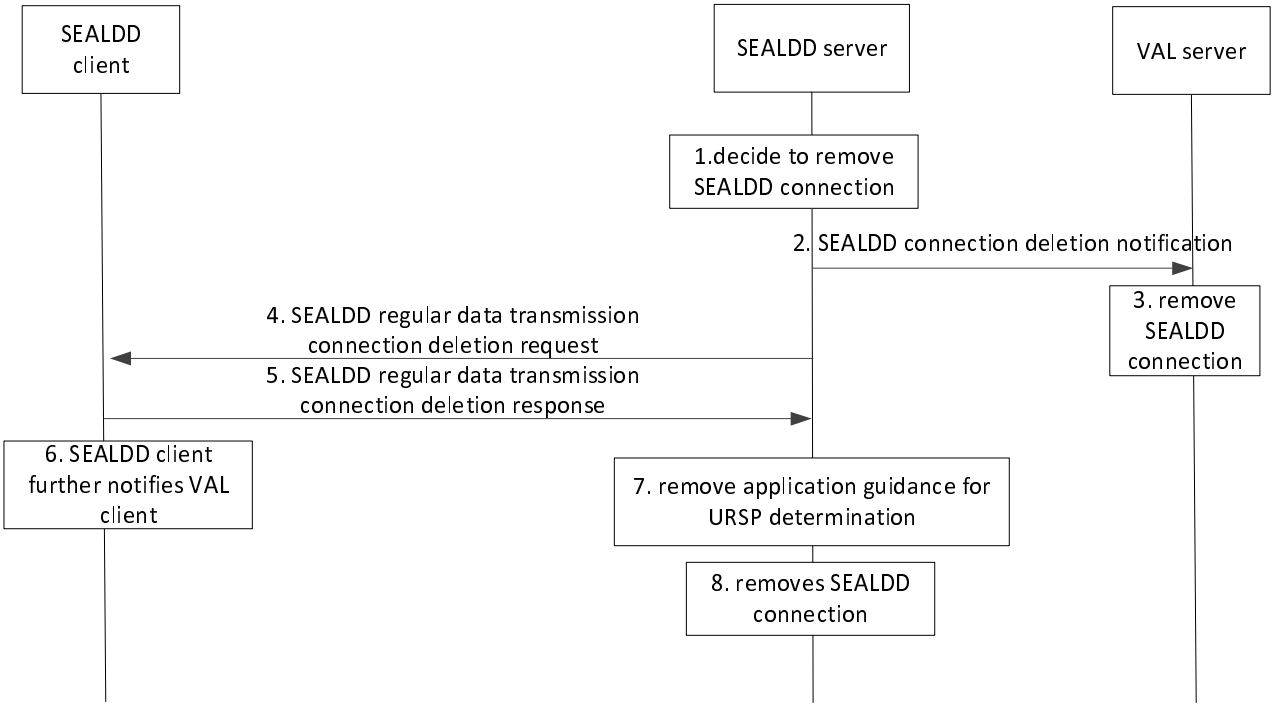

Figure 9.2.2.4-1: SEALDD enabled regular data transmission connection deletion

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 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 (i.e. SEALDD connection status notification with release event, as described in Table 9.2.3.9-1) 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.

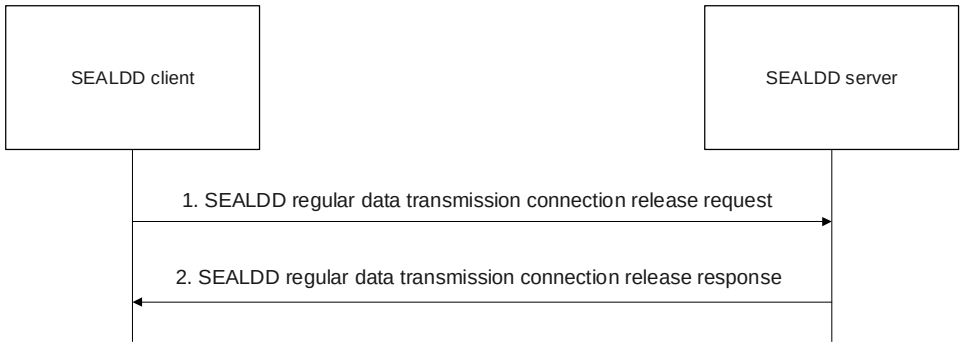

Figure 9.2.2.5-1: SEALDD client initiated connection release

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 can release the connection resources.

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 Data transmission connection information	M	Address/port and/or URL of the VAL server to receive the application packets 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 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.		

9.2.3.3 SEALDD regular transmission connection establishment request

Table 9.2.3.3-1 describes the information flow from the SEALDD client to the SEALDD server or from the SEALDD server to the SEALDD client for requesting the 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 or SEALDD server).
SEALDD flow ID	M (See NOTE)	Identity of the SEALDD 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 (for client side initiated request) or the SEALDD server side (for server side initiated request) 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, applicable for SEALDD server side initiated request.
NOTE: The SEALDD 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.		

9.2.3.4 SEALDD regular transmission connection establishment response

Table 9.2.3.4-1 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 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) or the SEALDD client side (for server side initiated request) used to establish SEALDD connection.
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 flow ID	M	Identifies the SEALDD 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.
VAL service ID	O	Identity of the VAL service
Identity	O	Identifier of VAL UE or VAL user.
SEALDD-S Data transmission connection information	M	Address/port of the VAL server to send/receive the application packets to/from the SEALDD server.

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
Identity	M	Identifier of VAL UE or VAL user.
VAL service ID	M	Identity of the VAL service.
SEALDD connection establishment data	O	Data related to SEALDD connection establishment.
> SEALDD-S Data transmission connection information	M	Address/port of the SEALDD server to send/receive the application packets to/from the VAL server.
> SEALDD communication lifetime	O	Identifies the DD communication lifetime.

9.2.3.10 SEALDD connection status subscription update request

Table 9.2.3.10-1 describes the information flow from the VAL server to SEALDD server to update subscription for SEALDD connection status information.

Table 9.2.3.10-1: SEALDD connection status subscription update request

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

9.2.3.11 SEALDD connection status subscription udpate response

Table 9.2.3.11-1 describes the information flow from the SEALDD server to VAL server for responding SEALDD connection status subscription update request.

Table 9.2.3.11-1: 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.		

9.2.3.12 SEALDD connection status unsubscribe request

Table 9.2.3.12-1 describes the information flow from the VAL server to SEALDD server to unsubscribe the SEALDD connection status information.

Table 9.2.3.12-1: SEALDD connection status unsubscribe request

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

9.2.3.13 SEALDD connection status unsubscribe response

Table 9.2.3.13-1 describes the information flow from the SEALDD server to VAL server for responding SEALDD connection status unsubscribe request.

Table 9.2.3.13-1: SEALDD connection status unsubscribe response

Information element	Status	Description
Result	M	Success or failure.

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
	Release	Request/Response	SEALDD client
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.

Outputs: See clause 9.2.3.4.

See clause 9.2.2.1 and 9.2.2.2 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 9.2.2.3 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: See clause 9.2.3.9.

See clause 9.2.2.3 and clause 9.2.2.4 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 9.2.3.10.

Outputs: See clause 9.2.3.11.

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 9.2.3.12.

Outputs: See clause 9.2.3.13.

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.

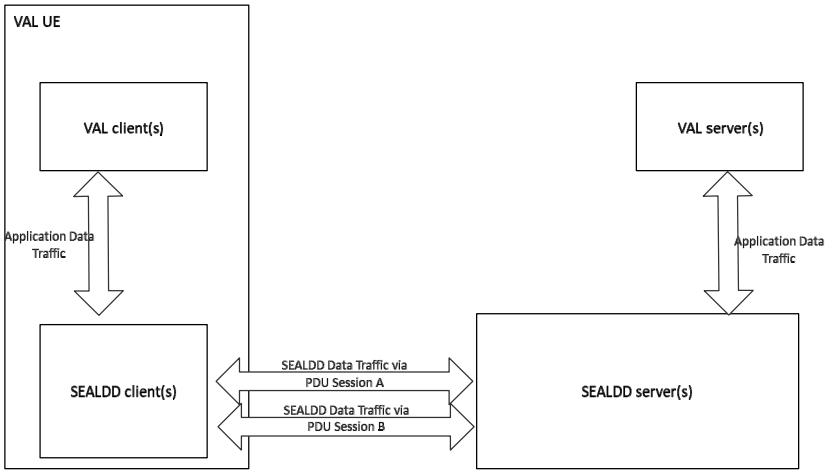

Figure 9.3.1-1: E2E redundant transmission traffic flow

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 flow IDs and SEALDD traffic descriptors to identify SEALDD traffic for different VAL servers.

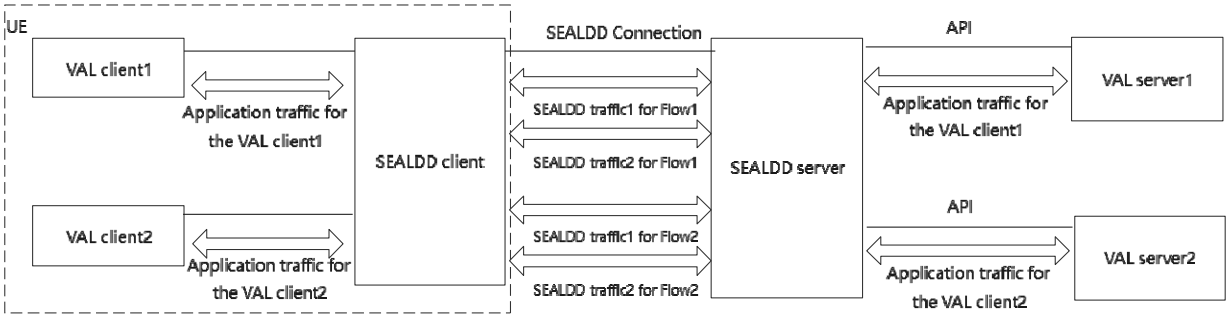

Figure 9.3.1-2: E2E redundant transmission traffic flow for multiple VAL servers

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 same Flow ID). Then according to the

SEALDD traffic descriptors of the SEALDD 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 Flow. 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 can 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.

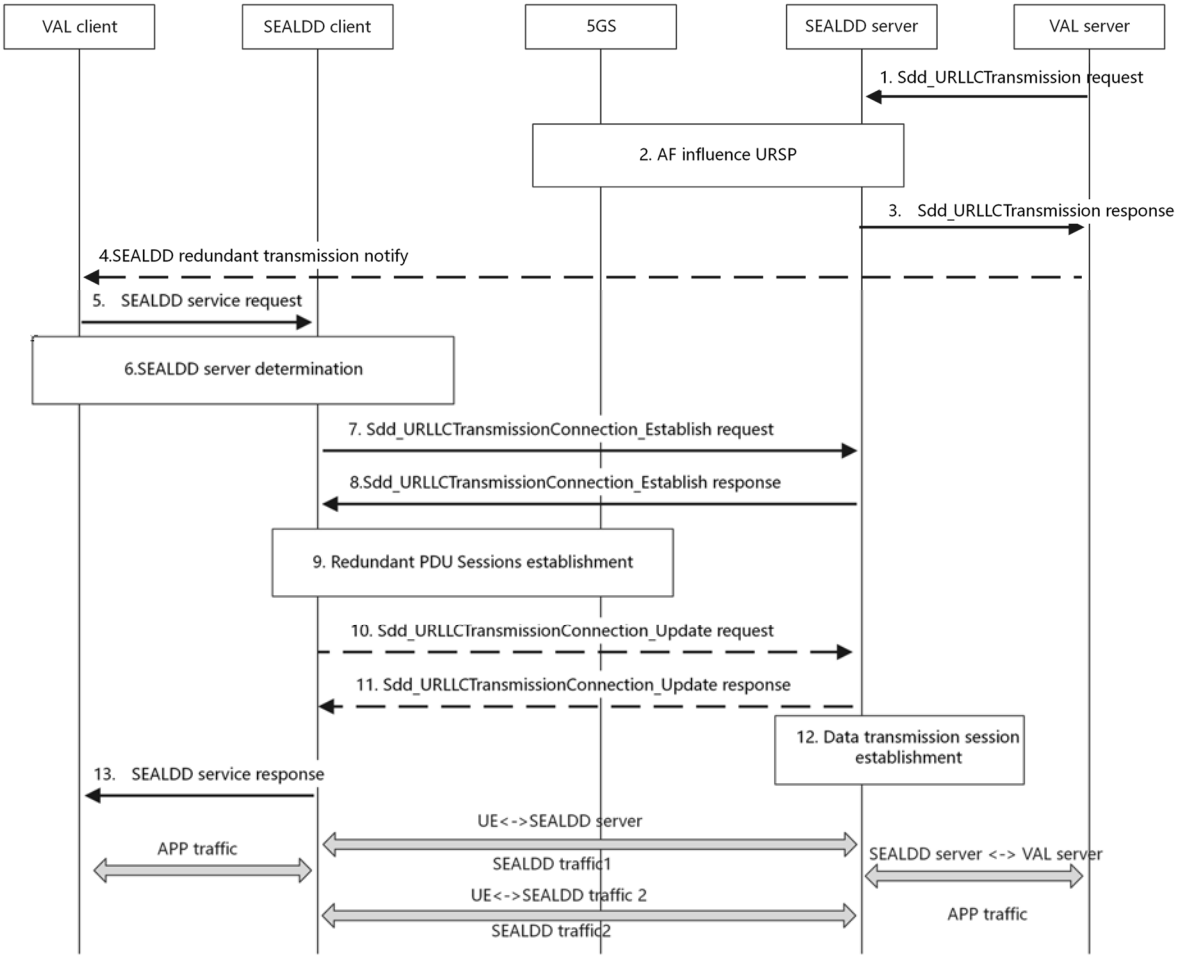

Figure 9.3.2.1-1: E2E redundant transmission path establishment

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 can be 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 addresses or ports 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 addresses or ports 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 address/port 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 can use 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 can get the SEALDD server's address.

7. The SEALDD client allocates a SEALDD flow ID mapping to the application traffic. The SEALDD client sends Sdd_URLLCTransmissionConnection_Establish request to SEALDD server. The request includes the SEALDD client ID, SEALDD flow ID, 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. the addresses or ports 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 flow ID, the SEALDD 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 flow ID 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/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.

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 flow ID. The SEALDD server gets the mapping information between the SEALDD flow ID 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 flow ID. 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.

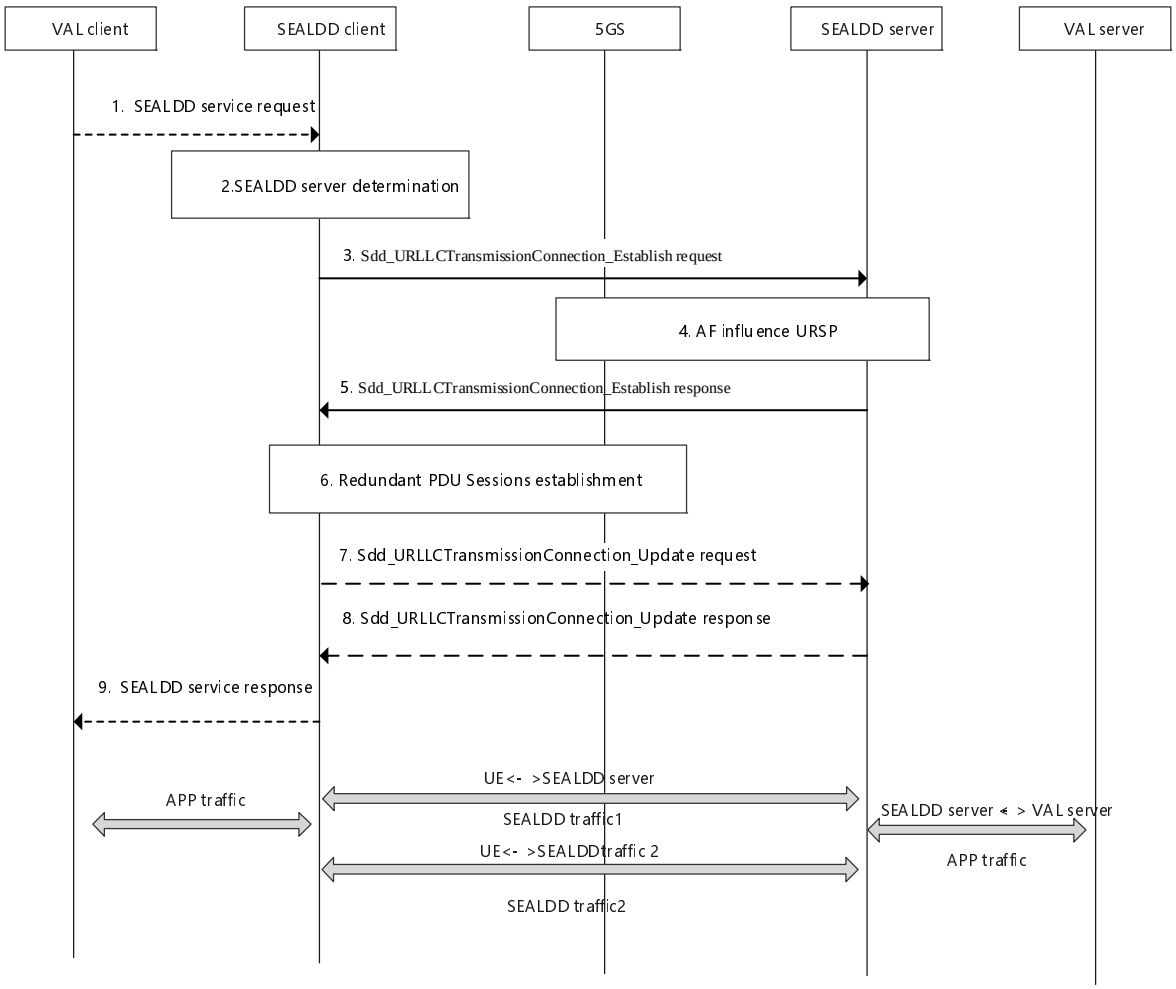

Figure 9.3.2.2-1: Client initiated E2E redundant transmission path establishment

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 a SEALDD flow ID 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 flow ID, 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 IP addresses and ports 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 or ports 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 IP addresses and ports 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 flow ID, 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 flow ID 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 client initiated connection release

Figure 9.3.2.3-1 illustrates the procedure for SEALDD client initiated connection release procedure from the SEALDD client to the SEALDD server.

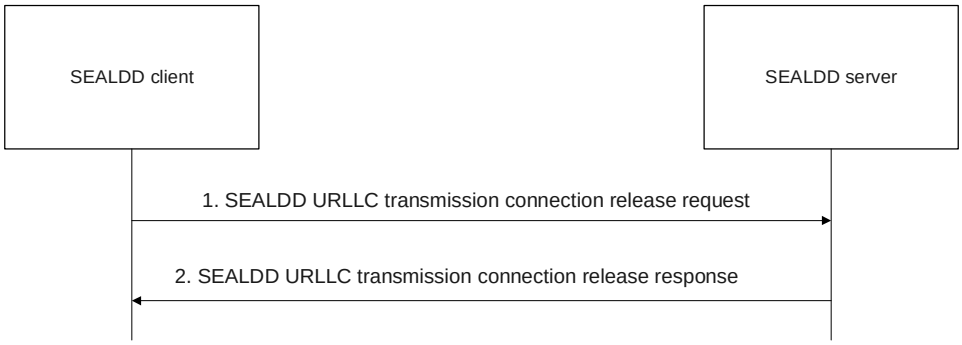

Figure 9.3.2.3-1: SEALDD client initiated connection release

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 can release 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 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	M	Identity of the SEALDD client.
Identity	O	The VAL user ID of the VAL user or VAL UE ID
SEALDD flow ID	M (See NOTE)	Identity of the SEALDD flow.
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 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.		

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 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 used to establish redundant 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		

9.3.3.5 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 flow ID	M (See NOTE)	Identity of the SEALDD flow.
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 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.		

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
	Update	Request/Response	SEALDD client
	Release	Request/Response	SEALDD client

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 for 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 9.3.2.3 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 can be 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]).

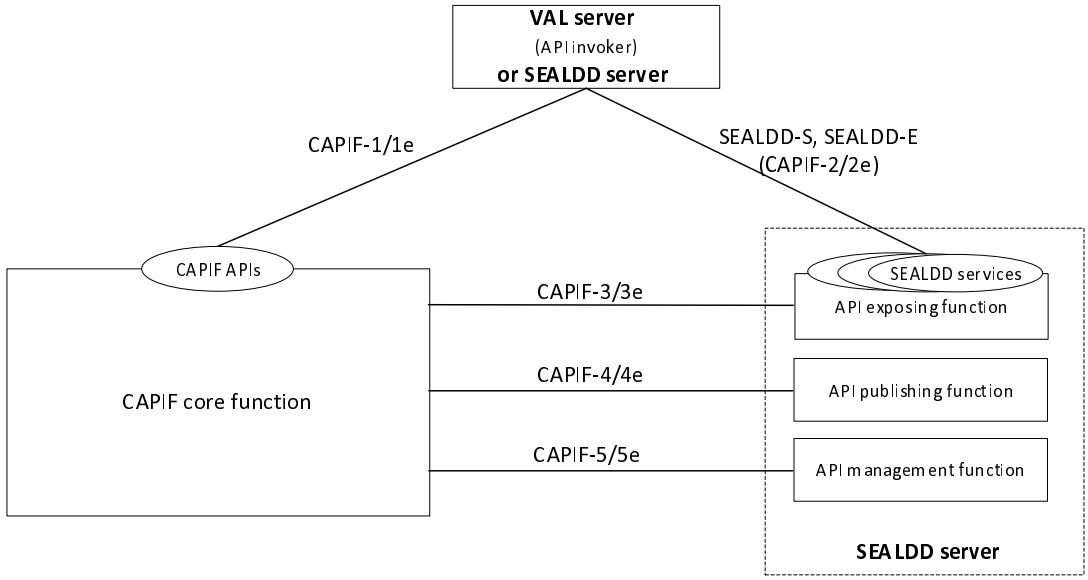

Figure 9.4.2.2-1: SEALDD adaptation in the CAPIF architecture

The VAL server can discover 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 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 can use 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 can provide 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] can be 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

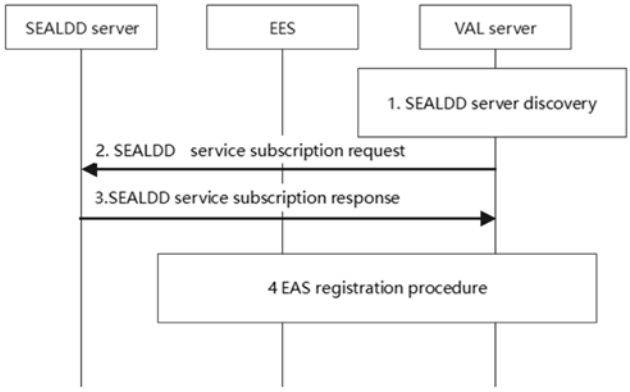

Figure 9.4.3.2.1-1: VAL server registered to EES with associated SEALDD server address as VAL server endpoint

1. The VAL server can discover and select 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 can use 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 can initiate SEALDD service via SEALDD client with the SEALDD server's address. This procedure can be used for scenario (a).

9.4.3.2.2 EAS registered to EES with associated SEALDD server information

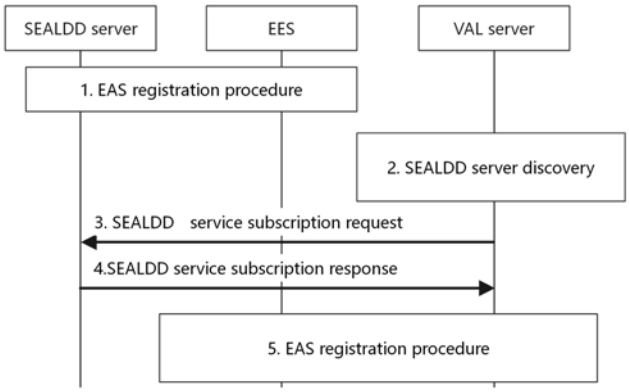

Figure 9.4.3.2.2-1: EAS register to EES with associated SEALDD server information

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 can discover and select 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 can use 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 can initiate SEALDD service via SEALDD client with the SEALDD server's address. For scenario (b), the VAL client can also establish 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

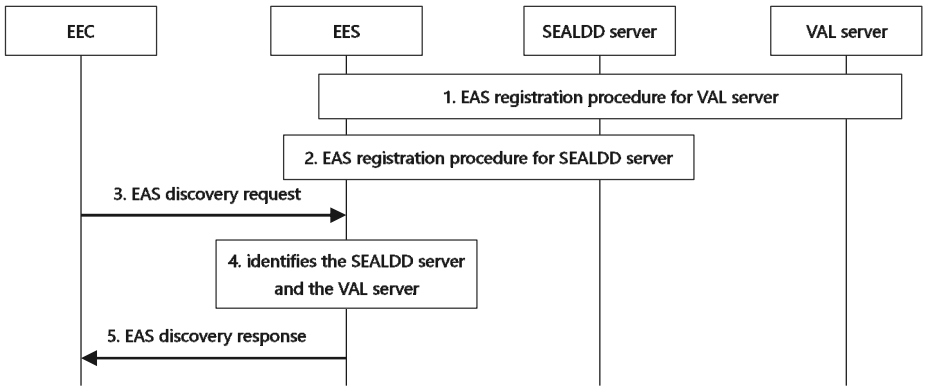

Figure 9.4.3.2.3-1: VAL server and SEALDD server registered to EES

1. The VAL server (acting as an EAS) registers to the EES.
2. 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).
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 can initiate SEALDD service via SEALDD client with the SEALDD server's address. The data transmission between the VAL client and the VAL server can be 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 can reuse 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 can refer 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 can reuse 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, can reuse 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 can refer 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 can 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.

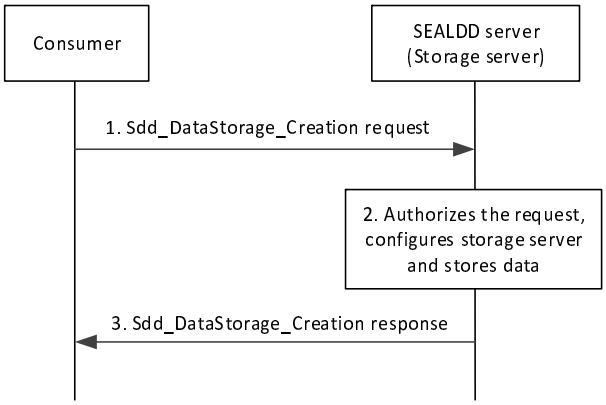

Figure 9.5.2.1-1: Storage service creation

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. 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. 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.

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.

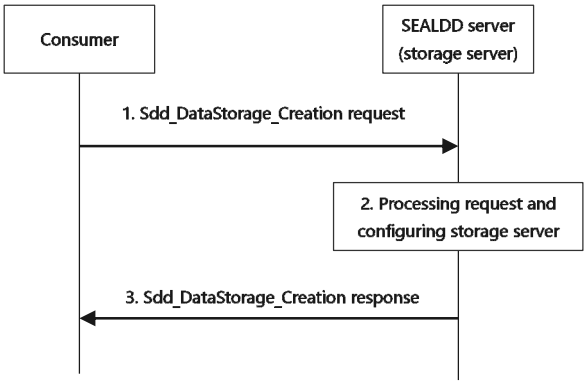

Figure 9.5.2.2-1: Storage service reservation

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 query

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).

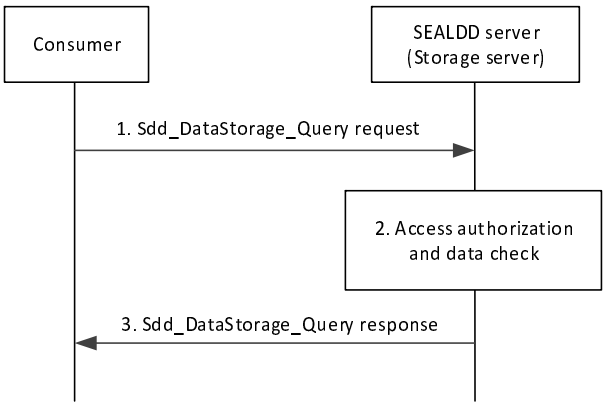

Figure 9.5.2.3-1: Access to stored data in SEALDD server

1. The consumer (e.g. SEALDD client/VAL server/other SEALDD server) sends a Sdd_DataStorage_Query 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) can be accessed by the consumer. The SEALDD server will also check whether the stored data is expired.

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).

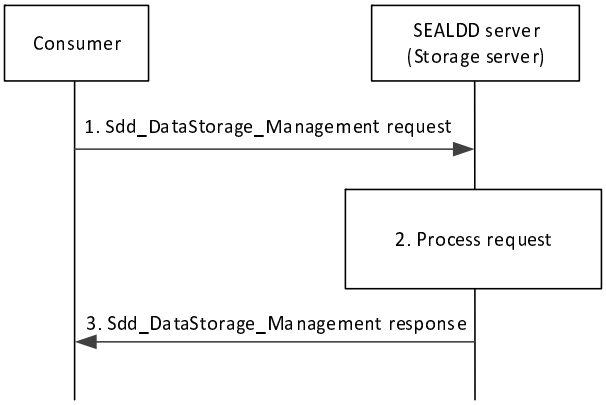

Figure 9.5.2.4-1: Storage management procedure

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.

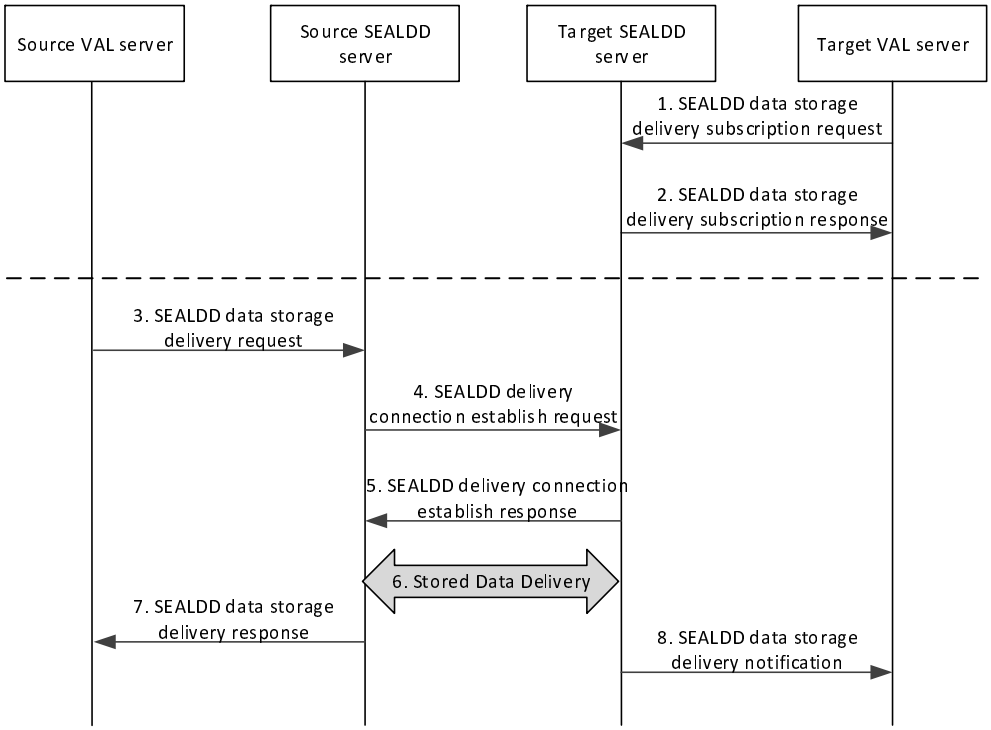

Figure 9.5.2.5-1: Stored data transfer procedure between VAL servers

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 can obtain the stored data originated from the source VAL server, by invoking the Sdd_DataStorage_Query 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
NOTE 1: These IEs are used for stroing 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)	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.		

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 query 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 query.

Table 9.5.3.4-1: SEALDD data storage query 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 query 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 query request.

Table 9.5.3.5-1: SEALDD data storage query response

Information element	Status	Description
Result	M	Success or failure.
The queried application data	O	The queried 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_Query	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_Query Request operation

API operation name: Sdd_DataStorage_Query Request

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

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 can be 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 can discover (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 can discover (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.

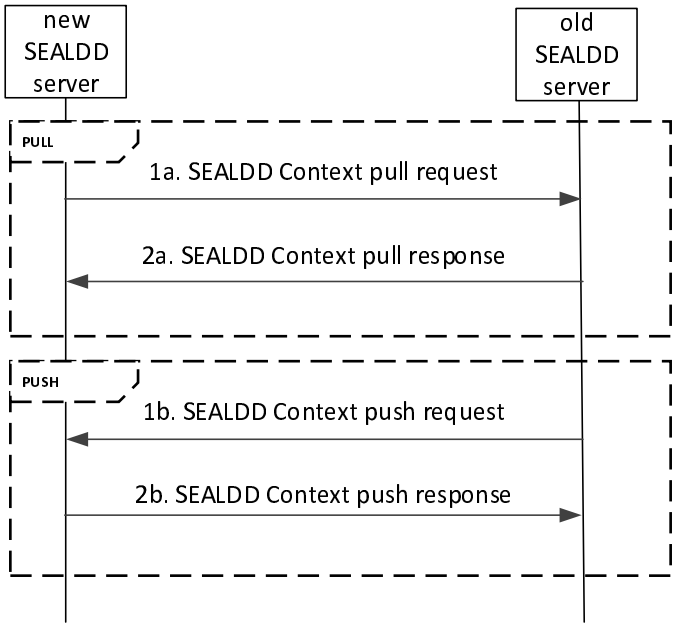

Figure 9.6.2.1-1: SEALDD context transfer

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 can pull 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 can request 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 can request 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.

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.

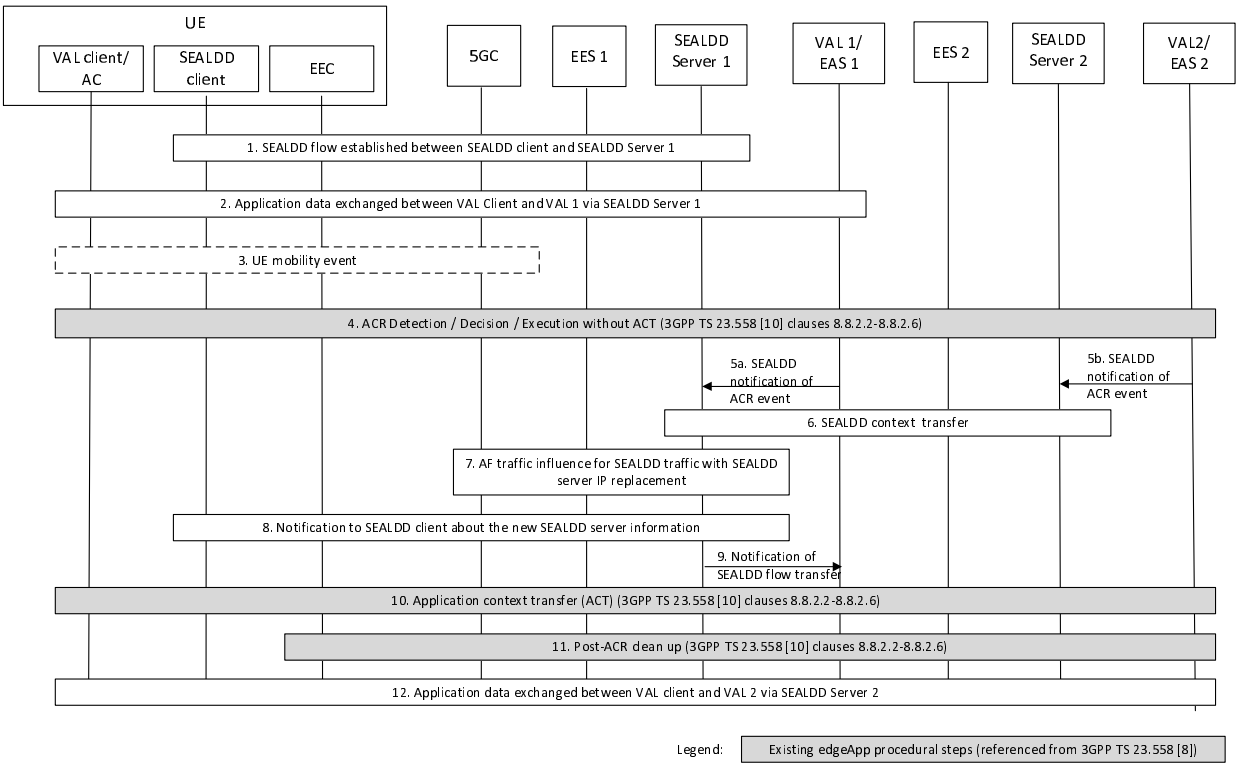

Figure 9.6.2.2-1: SEALDD support of UE's service continuity

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

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

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 signaling. 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 can obtain 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 can obtain 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 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 flow (with SEALDD server 2) to VAL Server 2.

NOTE: The SEALDD-UU client endpoint of the SEALDD 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.

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.		

9.6.4 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

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.

9.7 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.

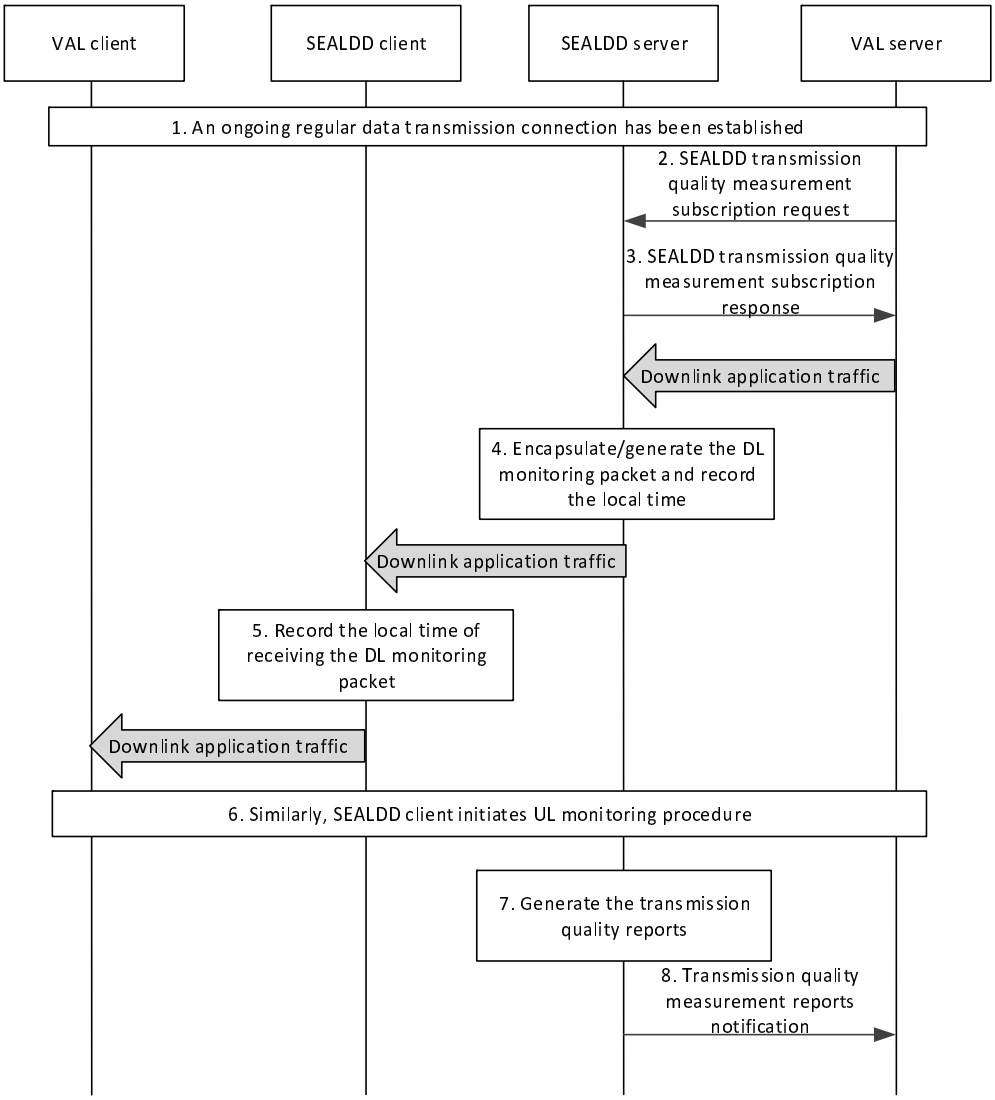

Figure 9.7.2.1-1: SEALDD enabled data transmission quality measurement procedure

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), and may also include reporting criteria, reporting frequency, spatial condition and temporal condition.

NOTE: 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: 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.

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.

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 can also calculate 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) 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 can send 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.

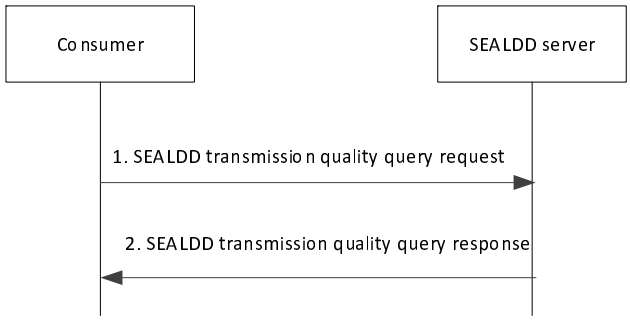

Figure 9.7.2.2-1: SEALDD enabled data transmission quality query procedure

1. The consumers (e.g. VAL server, SEALDD server, NSCE server, ADAE server) can send 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.

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.

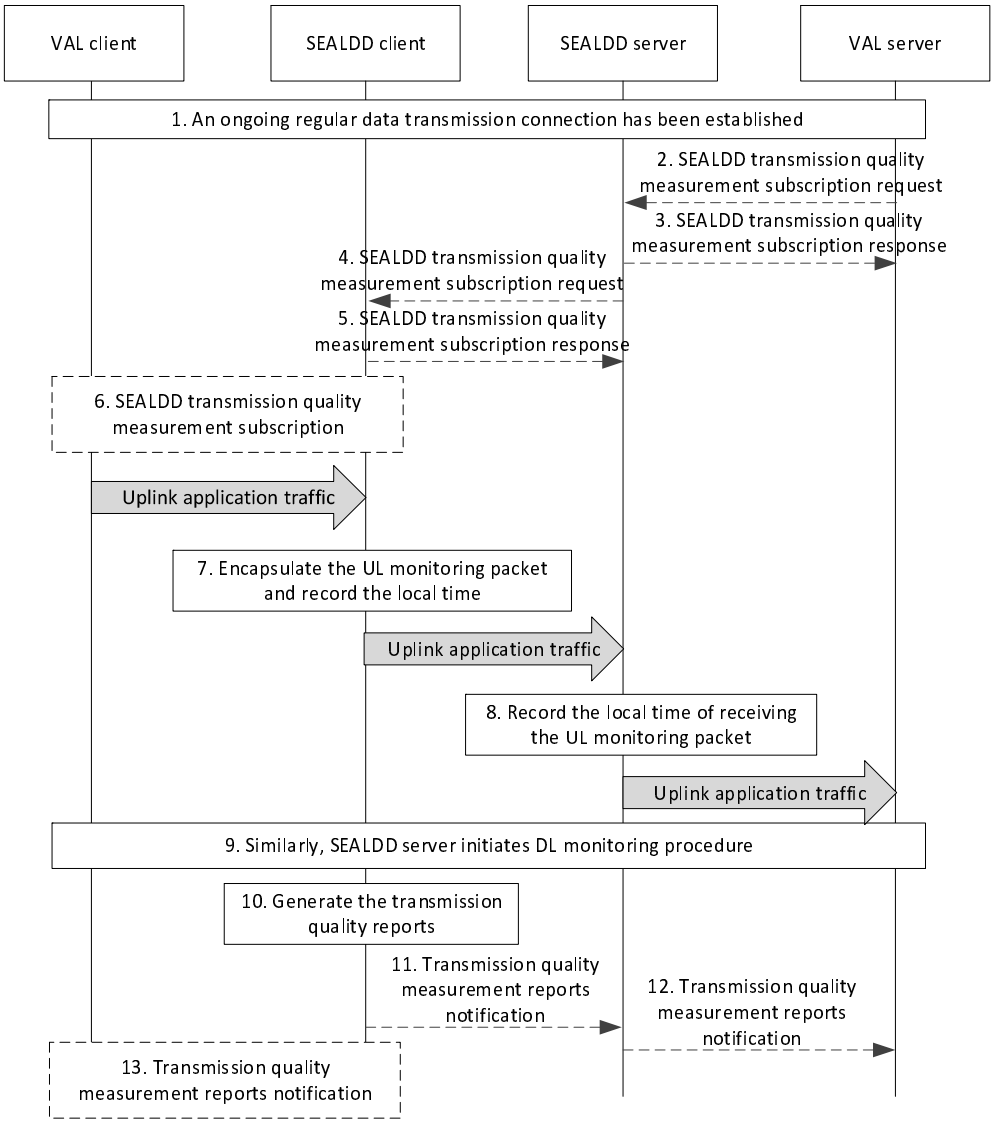

Figure 9.7.2.3-1: VAL data transmission quality measurement reported by SEALDD client

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

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

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. The SEALDD client, based on the received service quality guarantee policy including thresholds and action, can take corrective action as described in clause 9.7.2.3.

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.

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 UL 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 UL packet as monitoring response to the SEALDD client depends on SEALDD server implementation.

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 can also calculate 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 if present in the SEALDD transmission quality measurement subscription request in order to generate the transmission quality measurement report.

    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.

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.

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

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.
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, packet loss rate, 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.		

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.
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, 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. latency, bitrate, packet loss rate, jitter
> VAL UE/user ID(s)	O	It indicates the VAL UE(s) or VAL user(s) under SEALDD measurement. For a single VAL UE/user, it can be omitted and the associated measurement values are for the single VAL UE/user. For multiple VAL UEs/users with reporting granularity set to individual UE, the associated measurement values are for individual VAL UE/user 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.
> 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

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)	O	Identifier of VAL UE(s) or VAL user(s) need to be queried, e.g. single VAL UE/user, multiple VAL UEs/users, or VAL UE/user group

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 flow ID	M	Identifier of the SEALDD flow.
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
> 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 of 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.

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
> 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

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
	Update	Subscribe/Notify	VAL server
	Unsubscribe	Subscribe/Notify	VAL server
	Notify	Subscribe/notify	VAL 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_subscription 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 bandwidth control for different VAL users

9.8.1 General

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

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

9.8.2 Procedures

The SEALDD layer can provide the differentiated data delivery service with different bandwidth experience for VAL users, where the VAL server can provide the bandwidth limit (i.e., minimum bandwidth requirement and maximum bandwidth limit) for VAL users. Figure 9.8.2-1 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.

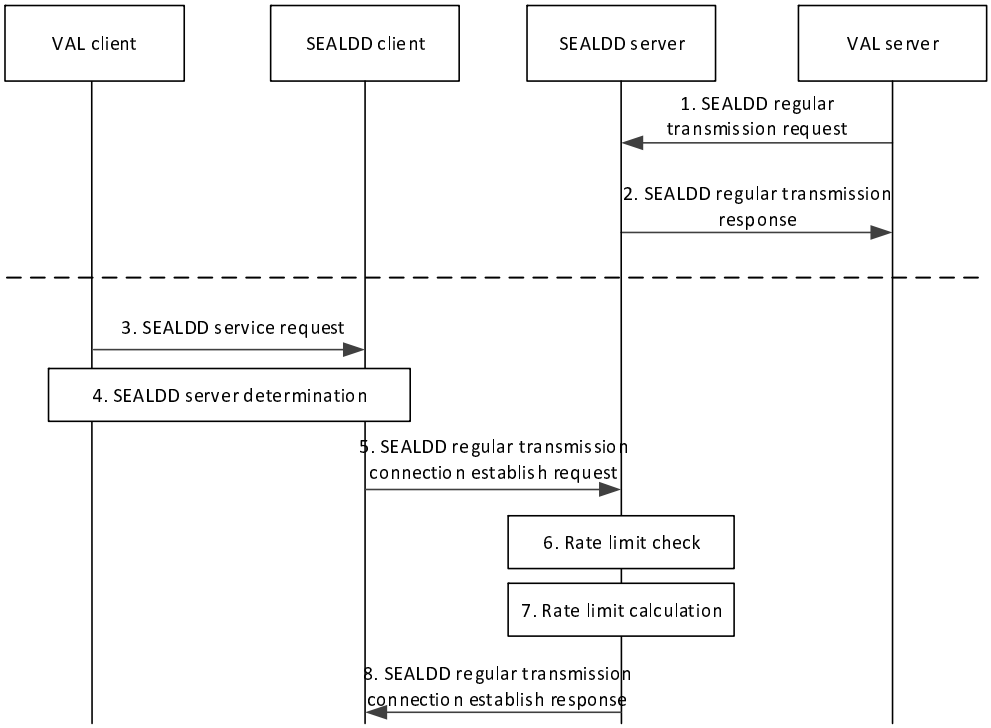

Figure 9.8.2-1: SEALDD enabled bandwidth control transmission procedure

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 can get 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.

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 can be used for the VAL user without exceeding the VAL server's total bandwidth limit) cannot 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 can meet the VAL user's requirement, the SEALDD client can establish the SEALDD connection with the SEALDD server. The SEALDD server can calculate 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).

8. If the bandwidth limit check is failed (i.e., the available bandwidth cannot meet the VAL user's minimum bandwidth requirement) in step 6, the SEALDD server can send 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 can meet the VAL user's requirement) in step 6, the SEALDD server can send 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 can re-establish SEALDD connection by performing steps 5-8, when the pending timer is expired.

For the uplink application traffic, the SEALDD client can buffer or drop some packets when the uplink traffic from VAL client exceeds the suggested traffic transmission bandwidth. Similarly, for the downlink application traffic, the SEALDD server can buffer or drop some packet when the downlink traffic from VAL server exceeds the suggested traffic transmission bandwidth.

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.

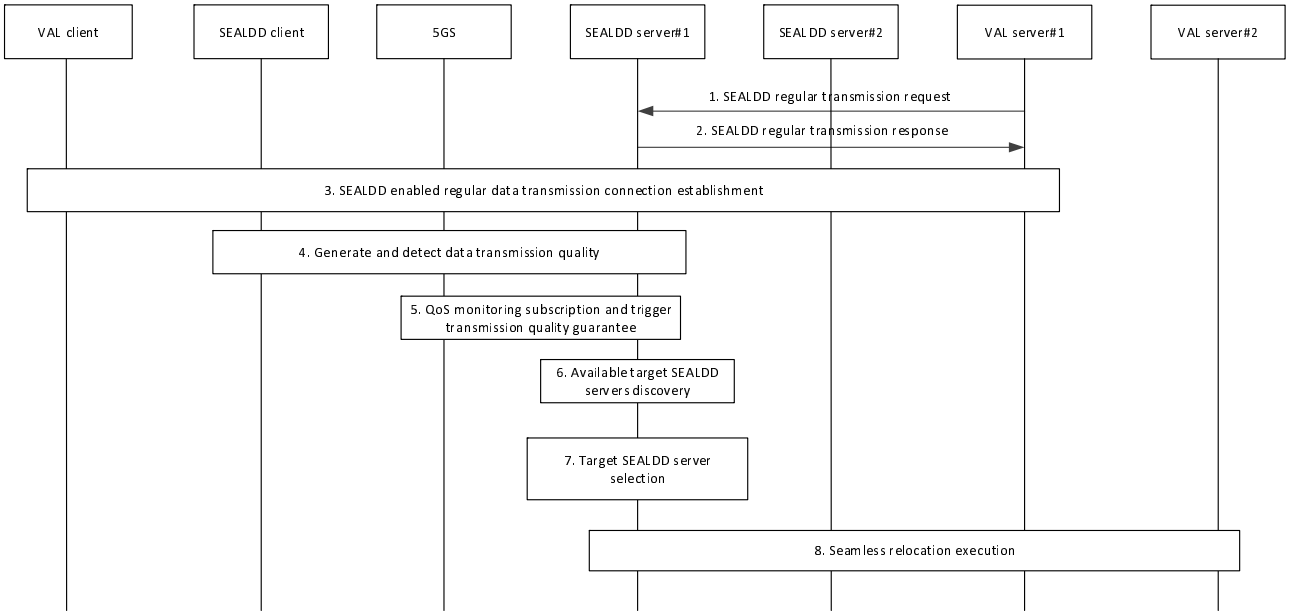

Figure 9.9.2.1-1: SEALDD enabled data transmission quality guarantee procedure by switching SEALDD server

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) can generate the transmission quality measurement report according to the SEALDD enabled transmission quality measurement procedure in clause 9.7.2.1, and detect whether the current transmission quality can satisfy 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 can determine 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 can select 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 can connect to the selected T-SEALDD server to obtain the data transmission quality guarantee service (i.e. the QoS requirements of VAL application can be 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 service policy, which includes data transmission quality guarantees, is available to SEALDD server. The policy can be 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.

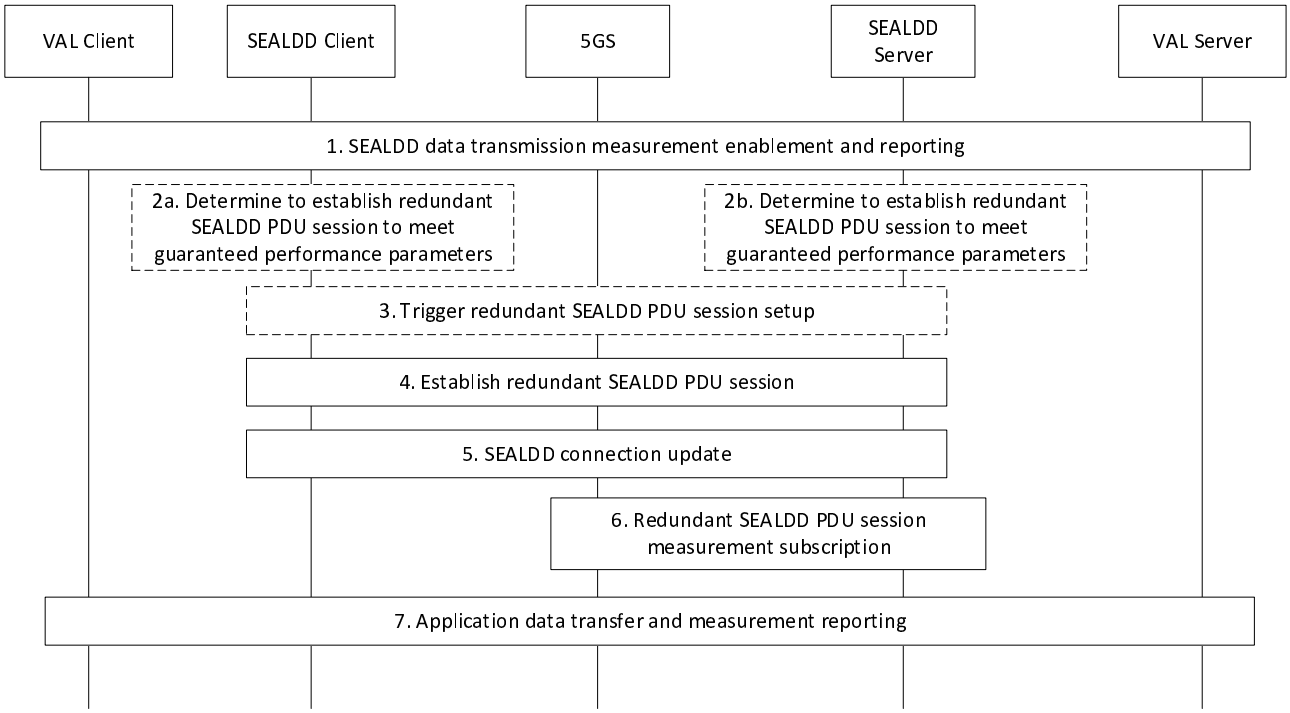

Figure 9.9.2.2-1: SEALDD data transmission quality guarantee with redundant transmission

1. A VAL client and server establish a SEALDD connection to transport the application data. As part of the connection establishment, the SEALDD service policy in precondition 1 is shared so that it is available to both the SEALDD client and the SEALDD Server. The SEALDD Server may use the data transmission quality requirements of this 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 service policy, depending on the 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 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 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 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 policy guarantee threshold, 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.

9.9.3 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 flow ID	M	Identifier of the SEALDD 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) that triggering by event (e.g. measurement threshold).

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.

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.

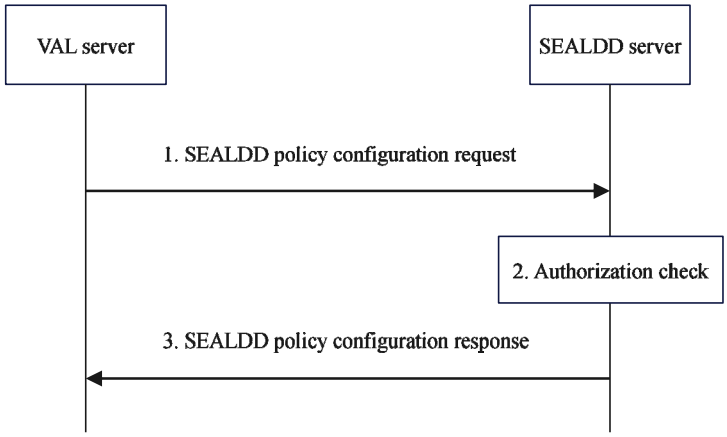

Figure 9.10.2.1-1: SEALDD policy configuration

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 can be 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.

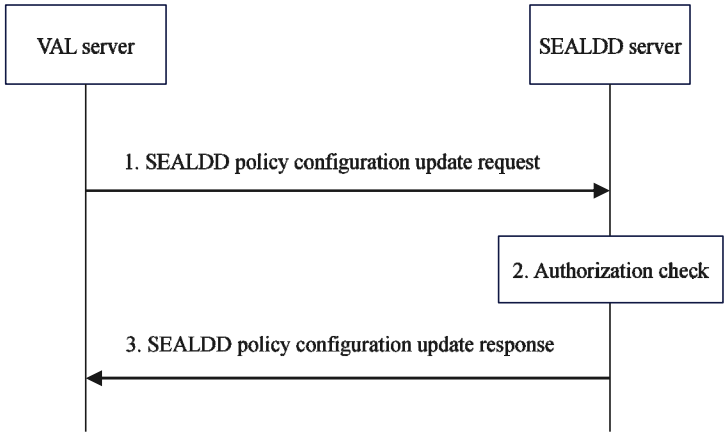

Figure 9.10.2.2-1: SEALDD policy configuration update

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 can be 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.

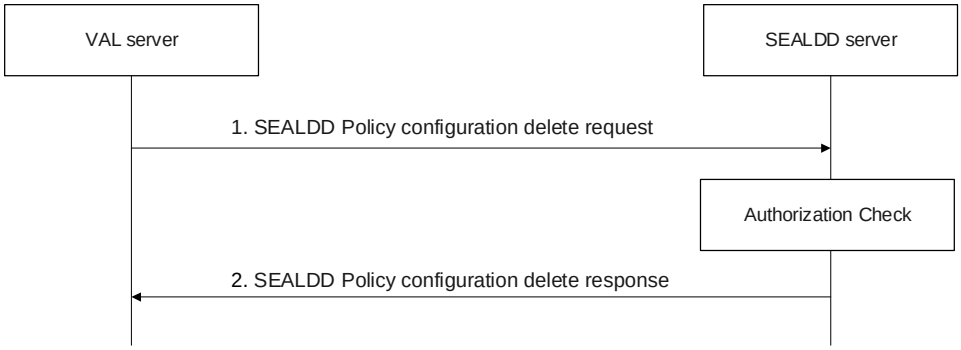

Figure 9.10.2.3-1: SEALDD policy configuration delete

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 can be 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.

9.10.3 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)
Identity	O	Identifier of the VAL UE or VAL user for which SEALDD policy applies
SEALDD policy	M	The SEALDD policy associated with application traffic identifiers, VAL UE/user identify
> Quality guarantee policy	O (See NOTE 1)	Indicates the event (e.g. measurement threshold) to be measured for the quality guarantee
> 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
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.		

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.

9.10.4 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		

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.

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.

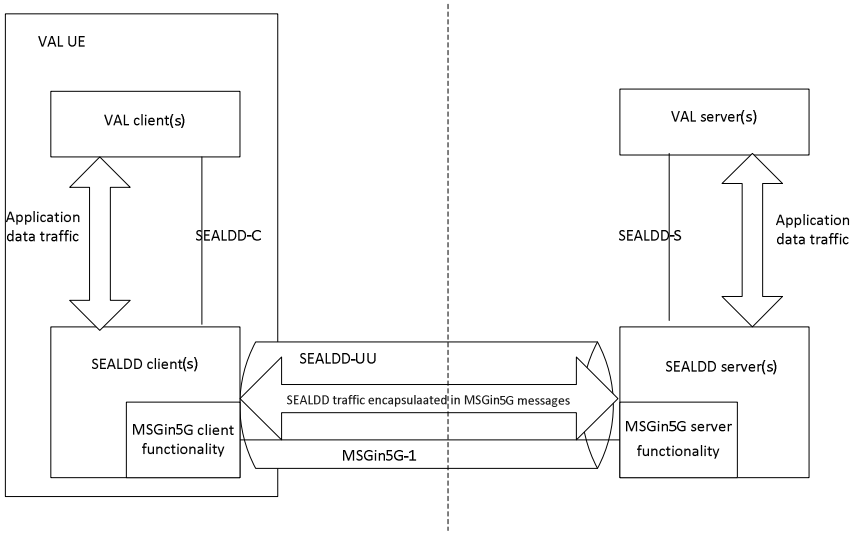

Figure B.2-1 SEALDD utilizing MSGin5G

Annex C (Informative): Overall lifecycle of SEALDD service

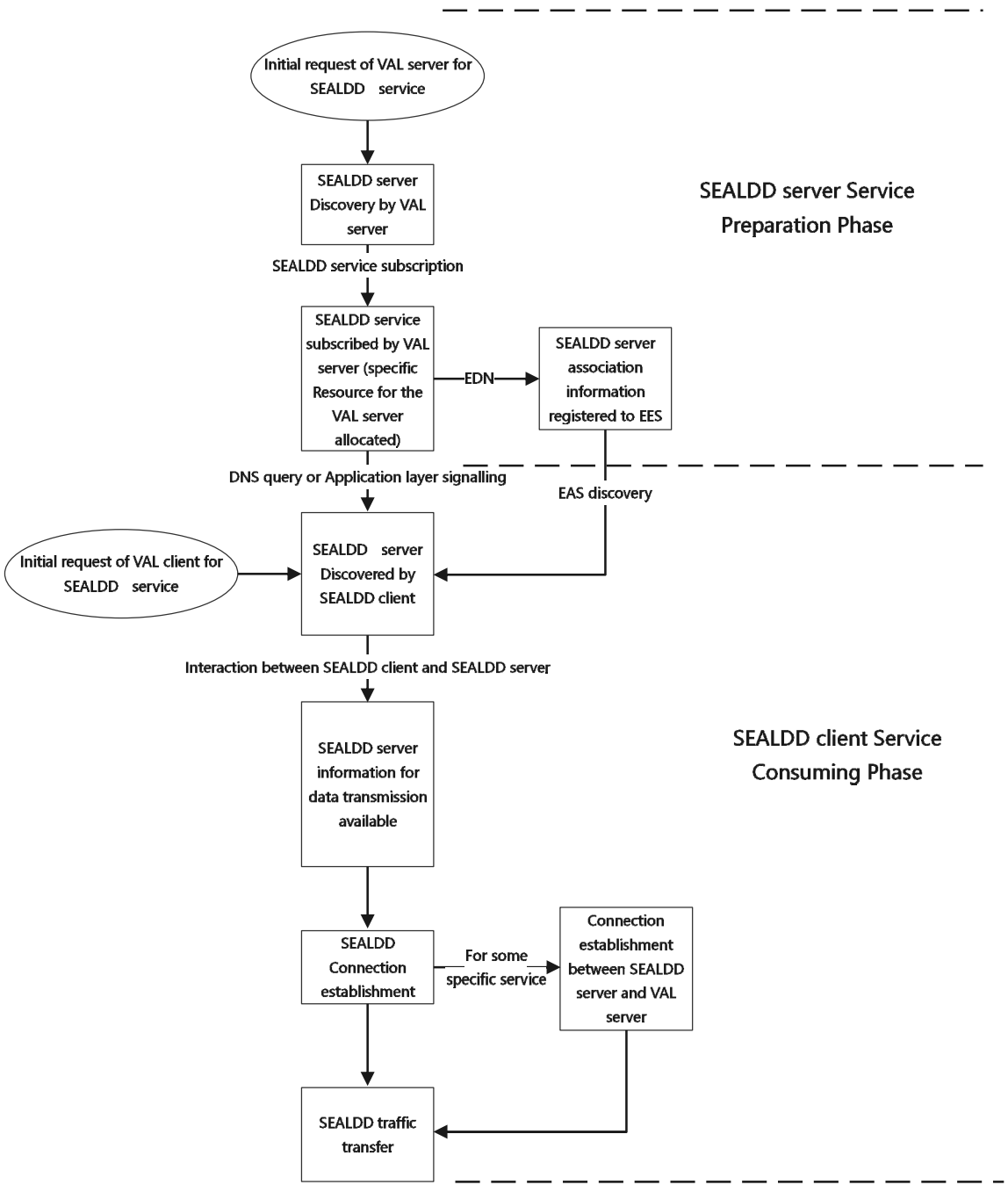

Figure C-1: Overall lifecycle of SEALDD

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): 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
2024-03	SA#103	SP-240309	0033		F	Alignment on VAL UE identity and VAL user identity	18.3.0
2024-03	SA#103	SP-240309	0035	2	F	Complete API for regular data transmission procedure	18.3.0
2024-03	SA#103	SP-240309	0037	1	F	Complete API for stored data transfer procedure	18.3.0
2024-03	SA#103	SP-240309	0041	1	F	Add release operation for URLLC connection	18.3.0
2024-03	SA#103	SP-240309	0043	2	F	Correct NRM and SEALDD interaction	18.3.0
2024-03	SA#103	SP-240309	0045		F	Correct regular transmission procedure	18.3.0
2024-03	SA#103	SP-240309	0047		F	Correct Sdd_TransmissionQualityMeasurement API	18.3.0
2024-03	SA#103	SP-240309	0049		F	Correct URLLC transmission procedure	18.3.0
2024-06	SA#104	SP-240763	0062	1	F	Alignment on data transmission connection establishment and release procedure	18.4.0
2024-06	SA#104	SP-240763	0064	1	F	Correction on E2E redundant transmission procedure	18.4.0
2024-06	SA#104	SP-240763	0066	1	F	Correction on SEALDD server discovery and selection procedure	18.4.0
2024-06	SA#104	SP-240763	0069	2	F	Correct context IE table	18.4.0

History

Document history		
V18.3.0	April 2024	Publication
V18.4.0	July 2024	Publication