|  |  |
| --- | --- |
| 3GPP TS 24.543 V2.0.0 (2024-06) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Core Network and Terminals;  Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification;  (Release 18) | |
|  | |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 8

1 Scope 10

2 References 10

3 Definitions of terms, symbols and abbreviations 11

3.1 Terms 11

3.2 Abbreviations 11

4 General description 12

5 Edge applications over 3GPP services 12

6 Functional entities 12

6.1 SEAL data delivery management client (SDDM-C) 12

6.2 SEAL data delivery management server (SDDM-S) 13

7 Data delivery management procedures 13

7.1 General 13

7.2 On-network procedures 13

7.2.1 General 13

7.2.1.1 Authenticated identity in HTTP request 13

7.2.1.2 Authenticated identity in CoAP request 14

7.2.2 SEALDD enabled signalling transmission connection establishment procedure 14

7.2.2.1 SDDM client HTTP procedure 14

7.2.2.2 SDDM server HTTP procedure 15

7.2.2.3 SDDM client CoAP procedure 16

7.2.2.4 SDDM server CoAP procedure 17

7.2.3 SEALDD enabled signalling transmission connection release procedure 19

7.2.3.1 SDDM client HTTP procedure 19

7.2.3.2 SDDM server HTTP procedure 19

7.2.3.3 SDDM client CoAP procedure 20

7.2.3.4 SDDM server CoAP procedure 21

7.2.4 SEALDD enabled E2E redundant transmission path establishment procedure 21

7.2.4.1 SDDM client HTTP procedure 21

7.2.4.2 SDDM server HTTP procedure 22

7.2.4.3 SDDM client CoAP procedure 23

7.2.4.4 SDDM server CoAP procedure 23

7.2.5 SEALDD enabled E2E redundant transmission path release procedure 24

7.2.5.1 SDDM client HTTP procedure 24

7.2.5.2 SDDM server HTTP procedure 24

7.2.5.3 SDDM client CoAP procedure 25

7.2.5.4 SDDM server CoAP procedure 25

7.2.6 SEALDD enabled E2E redundant transmission path connection update procedure 26

7.2.6.1 SDDM client HTTP procedure 26

7.2.6.2 SDDM server HTTP procedure 26

7.2.6.3 SDDM client CoAP procedure 27

7.2.6.4 SDDM server CoAP procedure 27

7.2.7 SEALDD server discovery and selection procedure 28

7.2.8 SEALDD enabled data storage creation procedure 28

7.2.8.1 SDDM client HTTP procedure 28

7.2.8.2 SDDM server HTTP procedure 28

7.2.8.3 SDDM client CoAP procedure 29

7.2.8.4 SDDM server CoAP procedure 29

7.2.9 SEALDD enabled data storage reservation procedure 30

7.2.9.1 SDDM client HTTP procedure 30

7.2.9.2 SDDM server HTTP procedure 30

7.2.9.3 SDDM client CoAP procedure 31

7.2.9.4 SDDM server CoAP procedure 31

7.2.10 SEALDD enabled data storage notification procedure 32

7.2.10.1 SDDM client HTTP procedure 32

7.2.10.2 SDDM server HTTP procedure 32

7.2.10.3 SDDM client CoAP procedure 32

7.2.10.4 SDDM server CoAP procedure 32

7.2.11 SEALDD enabled data storage query procedure 33

7.2.11.1 SDDM client HTTP procedure 33

7.2.11.2 SDDM server HTTP procedure 33

7.2.11.3 SDDM client CoAP procedure 34

7.2.11.4 SDDM server CoAP procedure 34

7.2.12 SEALDD enabled data storage management procedure 34

7.2.12.1 SDDM client HTTP procedure 34

7.2.12.2 SDDM server HTTP procedure 35

7.2.12.3 SDDM client CoAP procedure 35

7.2.12.4 SDDM server CoAP procedure 36

7.2.13 SEALDD server relocation procedure 37

7.2.14 SEALDD enabled data transmission quality measurement subscription procedure 37

7.2.14.1 SDDM client HTTP procedure 37

7.2.14.2 SDDM server HTTP procedure 38

7.2.14.3 SDDM client CoAP procedure 38

7.2.14.4 SDDM server CoAP procedure 39

7.2.15 SEALDD enabled data transmission quality measurement notification procedure 40

7.2.15.1 SDDM client HTTP procedure 40

7.2.15.2 SDDM server HTTP procedure 40

7.2.15.3 SDDM client CoAP procedure 41

7.2.15.4 SDDM server CoAP procedure 41

7.2.16 SEALDD enabled data transmission quality guarantee procedure 42

7.2.16.1 SDDM client HTTP procedure 42

7.2.16.2 SDDM server HTTP procedure 42

7.2.16.3 SDDM client CoAP procedure 43

7.2.16.4 SDDM server CoAP procedure 43

7.3 Off-network procedures 43

8 Coding 44

8.1 General 44

8.2 Application unique ID 44

8.3 Structure 44

8.4 XML schema 48

8.4.1 General 48

8.4.2 XML schema 48

8.5 Data semantics 57

8.6 MIME type 62

8.7 IANA registration template 62

Annex A (normative): CoAP resource representation and encoding 64

A.1 General 64

A.2 Data types applicable to multiple resource representations 64

A.2.1 General 64

A.2.2 Referenced structured data types 64

A.2.3 Referenced simple data types 65

A.2.4 Common structured data types 65

A.2.4.1 Type: EstablishmentResponse 65

A.2.5 Common simple data types 65

A.2.6 Common enumerations 66

A.2.6.1 Enumeration: RequestorId 66

A.2.6.2 Enumeration: ResultOp 66

A.2.6.3 Enumeration: Cause 66

A.3 Resource representation and APIs provided by SDDM-S 66

A.3.1 Sdd\_RegularTransmissionConnection API 66

A.3.1.1 API URI 66

A.3.1.2 Resources 67

A.3.1.2.1 Overview 67

A.3.1.2.2 Resource: SDD Regular Transmission Connection 67

A.3.1.2.2.1 Description 67

A.3.1.2.2.2 Resource Definition 67

A.3.1.2.2.3 Resource Standard Methods 68

A.3.1.3 Data Model 69

A.3.1.3.1 General 69

A.3.1.3.2 Structured data types 70

A.3.1.3.2.1 Type: EstablishmentRequest 70

A.3.1.3.2.2 Type: ReleaseRequest 70

A.3.1.3.3 Simple data types and enumerations 70

A.3.1.4 Error Handling 70

A.3.1.5 CDDL Specification 70

A.3.1.5.1 Introduction 70

A.3.1.5.2 CDDL document 71

A.3.1.6 Media Types 71

A.3.1.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-establishment-req-info+cbor 71

A.3.1.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-establishment-res-info+cbor 72

A.3.1.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-release-req-info+cbor 72

A.3.2 Sdd\_TransmissionQualityMeasurement API 73

A.3.2.1 API URI 73

A.3.2.2 Resources 74

A.3.2.2.1 Overview 74

A.3.2.2.2 Resource: SDD Transmission Quality Measurement 74

A.3.2.2.2.1 Description 74

A.3.2.2.2.2 Resource Definition 75

A.3.2.2.2.3 Resource Standard Methods 75

A.3.2.2.2.3.1 POST 75

A.3.2.2.2.3.2 PUT 75

A.3.2.2.2.3.3 DELETE 76

A.3.2.3 Data Model 76

A.3.2.3.1 General 76

A.3.2.3.2 Structured data types 78

A.3.2.3.2.1 Type: MeasurementsSubscriptionRequest 78

A.3.2.3.2.2 Type: MeasurementsSubscriptionResponse 78

A.3.2.3.2.3 Type: MeasurementsNotification 79

A.3.2.3.2.4 Type: ReportingCriteria 80

A.3.2.3.2.5 Type: LatencyValue 80

A.3.2.3.2.6 Type: BitrateValue 80

A.3.2.3.2.7 Type: MeasurementConditions 81

A.3.2.3.2.8 Type: MeasurementPeriod 81

A.3.2.3.2.9 Type: SpatialConditions 81

A.3.2.3.3 Simple data types and enumerations 81

A.3.2.4 Error Handling 81

A.3.2.5 CDDL Specification 81

A.3.2.5.1 Introduction 81

A.3.2.5.2 CDDL document 81

A.3.2.6 Media Types 84

A.3.2.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-measurement-subscription-req-info+cbor 85

A.3.2.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-measurement-subscription-res-info+cbor 85

A.3.2.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-measurement-notification-info+cbor 86

A.3.3 Sdd\_TransmissionQualityManagement API 87

A.3.3.1 API URI 87

A.3.3.2 Resources 88

A.3.3.2.1 Overview 88

A.3.3.2.2 Resource: SDD Transmission Quality Management 88

A.3.3.2.2.1 Description 88

A.3.3.2.2.2 Resource Definition 88

A.3.3.2.2.3 Resource Standard Methods 89

A.3.3.2.2.3.1 POST 89

A.3.3.2.2.3.2 DELETE 89

A.3.3.3 Data Model 90

A.3.3.3.1 General 90

A.3.3.3.2 Structured data types 91

A.3.3.3.2.1 Type: TxQualityManagementRequest 91

A.3.3.3.2.2 Type: TxQualityManagementResponse 91

A.3.3.3.3 Simple data types and enumerations 91

A.3.3.4 Error Handling 91

A.3.3.5 CDDL Specification 91

A.3.3.5.1 Introduction 91

A.3.3.5.2 CDDL document 91

A.3.3.6 Media Types 92

A.3.3.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-req-info+cbor 92

A.3.3.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-res-info+cbor 93

A.4 Resource representation and APIs provided by SDDM-C 94

A.4.1 Sdd\_RegularTransmissionConnection API 94

A.4.1.1 API URI 94

A.4.1.2 Resources 94

A.4.1.2.1 Overview 94

A.4.1.2.2 Resource: SDD Regular Transmission Connection 95

A.4.1.2.2.1 Description 95

A.4.1.2.2.2 Resource Definition 95

A.4.1.2.2.3 Resource Standard Methods 95

A.4.1.3 Data Model 96

A.4.1.3.1 General 96

A.4.1.3.2 Structured data types 97

A.4.1.3.2.1 Type: EstablishmentRequest 97

A.4.1.3.2.2 Type: ReleaseRequest 97

A.4.1.3.3 Simple data types and enumerations 97

A.4.1.4 Error Handling 97

A.4.1.5 CDDL Specification 98

A.4.1.5.1 Introduction 98

A.4.1.5.2 CDDL document 98

A.4.1.6 Media Types 98

A.4.2 Sdd\_URLCCTransmissionConnection API 98

A.4.2.1 API URI 98

A.4.2.2 Resources 99

A.4.2.2.1 Overview 99

A.4.2.2.2 Resource: URLLC Transmission Connection 99

A.4.2.2.2.1 Description 99

A.4.2.2.2.2 Resource Definition 100

A.4.2.2.2.3 Resource Standard Methods 100

A.4.2.3 Data Model 101

A.4.2.3.1 General 101

A.4.2.3.2 Structured data types 102

A.4.2.3.2.1 Type: URLLCEstablishmentRequest 102

A.4.2.3.2.2 Type: URLLCEstablishmentResponse 102

A.4.2.3.2.3 Type: URLLCUpdateRequest 103

A.4.2.3.2.4 Type: URLLCReleaseRequest 103

A.4.2.3.3 Simple data types and enumerations 103

A.4.2.4 Error Handling 103

A.4.2.5 CDDL Specification 103

A.4.2.5.1 Introduction 103

A.4.2.5.2 CDDL document 103

A.4.2.6 Media Types 103

A.4.2.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-establishment-req-info+cbor 104

A.4.2.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-establishment-res-info+cbor 104

A.4.2.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-update-req-info+cbor 105

A.4.2.10 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-release-req-info+cbor 106

A.4.3 Sdd\_DataStorage API 107

A.4.3.1 API URI 107

A.4.3.2 Resources 107

A.4.3.2.1 Overview 107

A.4.3.2.2 Resource: SDD Data Storage 108

A.4.3.2.2.1 Description 108

A.4.3.2.2.2 Resource Definition 108

A.4.3.2.2.3 Resource Standard Methods 108

A.4.3.2.2.3.1 POST 108

A.4.3.2.2.3.2 PUT 109

A.4.3.2.2.3.3 DELETE 109

A.4.3.2.2.3.4 GET 109

A.4.3.2.2.3.5 FETCH 110

A.4.3.3 Data Model 110

A.4.3.3.1 General 110

A.4.3.3.2 Structured data types 112

A.4.3.3.2.1 Type: DataStorageCreationRequest 112

A.4.3.3.2.2 Type: DataStorageCreationResponse 112

A.4.3.3.2.3 Type: DataStorageReservationRequest 112

A.4.3.3.2.4 Type: DataStorageReservationResponse 112

A.4.3.3.2.5 Type: DataStorageStatusNotification 113

A.4.3.3.2.6 Type: DataStorageQueryResponse 113

A.4.3.3.2.7 Type: DataStorageMgtRequest 113

A.4.3.3.2.8 Type: StatusInformationReq 113

A.4.3.3.2.9 Type: StatusInformationRes 114

A.4.3.3.3 Simple data types and enumerations 114

A.4.3.4 Error Handling 114

A.4.3.5 CDDL Specification 114

A.4.3.5.1 Introduction 114

A.4.3.5.2 CDDL document 114

A.4.3.6 Media Types 115

A.4.2.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-creation-req-info+cbor 116

A.4.2.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-creation-res-info+cbor 116

A.4.2.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-reservation-req-info+cbor 117

A.4.2.10 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-reservation-res-info+cbor 118

A.4.2.11 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-status-notification-info+cbor 119

A.4.2.12 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-query-res-info+cbor 119

A.4.2.13 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor 120

Annex B (informative): Change history 122

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

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

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

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# 1 Scope

The present document specifies the protocol aspects for the data delivery management capability of SEAL for the application content/data for vertical applications (e.g. V2X) over the 3GPP system as part of SEAL services specified in 3GPP TS 23.434 [3] and 3GPP TS 23.433 [2].

The present document is applicable to the user equipment (UE) supporting the data delivery management client functionality as described in 3GPP TS 23.433 [2], to the application server supporting the data delivery management server functionality as described in 3GPP TS 23.433 [2] and to the application server supporting the vertical application server (VAL server) functionality as defined in the specific vertical application service (VAL service) specifications.

NOTE: The specification of the VAL server for a specific VAL service is out of scope of present document.

# 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 23.433: "Service Enabler Architecture Layer for Verticals (SEAL); Data Delivery enabler for vertical applications".

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

[4] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[5] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[6] 3GPP TS 24.546: "Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

[7] 3GPP TS 24.547: "Identity management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

[8] 3GPP TS 24.558: "Enabling Edge Applications; Protocol specification".

[9] 3GPP TS 29.548: "Service Enabler Architecture Layer for Verticals (SEAL); SEAL Data Delivery (SEALDD) Server Services; Stage 3".

[10] 3GPP TS 29.558: "Enabling Edge Applications; Application Programming Interface (API) specification; Stage 3".

[11] IETF RFC 3339: "Date and Time on the Internet: Timestamps".

[12] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

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

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

[15] IETF RFC 7641: "Observing Resources in the Constrained Application Protocol (CoAP)".

[16] IETF RFC 7959: "Block-Wise Transfers in the Constrained Application Protocol (CoAP) ".

[17] IETF RFC 8132: "PATCH and FETCH Methods for the Constrained Application Protocol (CoAP)".

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

[19] IETF RFC 8610: "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures".

[20] IETF RFC 8949: "Concise Binary Object Representation (CBOR)".

[21] IETF RFC 9110: "HTTP Semantics".

[22] IETF RFC 9177: "Constrained Application Protocol (CoAP) Block-Wise Transfer Options Supporting Robust Transmission".

[23] OMA OMA-TS-XDM\_Core-V2\_1-20120403-A: "XML Document Management (XDM) Specification".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

**Data delivery management SEAL client**: An entity that provides the client side functionalities corresponding to the data delivery management SEAL service.

**Data delivery management SEAL server**: An entity that provides the server side functionalities corresponding to the data delivery management SEAL service.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.434 [3] apply:

**SEAL client**

**SEAL server**

**SEAL service**

**VAL user**

**VAL server**

**VAL service**

**Vertical**

**Vertical application**

## 3.2 Abbreviations

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

ACR Application Context Relocation

API Application Programming Interface

CDDL Concise Data Definition Language

CoAP Constrained Application Protocol

DNS Domain Name System

EAS Edge Application Server

ECS Edge Configuration Server

EDN Edge Data Network

EES Edge Enabler Server

MIME Multipurpose Internet Mail Extensions

NAS Non Access Stratum

SEAL Service Enabler Architecture Layer for verticals

SEALDD SEAL Data Delivery

SDDM SEAL Data Delivery Management

SDDM-C SEAL Data Delivery Management Client

SDDM-S SEAL Data Delivery Management Server

URI Uniform Resource Identifier

URL Uniform Resource Locator

URLLC Ultra-Reliable Low Latency Communication

V2X Vehicle-to-Everything

VAL Vertical Application Layer

XCAP XML Configuration Access Protocol

# 4 General description

Data delivery management is a SEAL service that provides the data delivery management related capabilities (data delivery and storage capabilities) to one or more vertical applications. The present document enables a SEAL data delivery management client (SDDM-C) and a VAL server to communicate with a SEAL data delivery management server (SDDM-S).

# 5 Edge applications over 3GPP services

The SDDM-C and the SDDM-S can utilize edge applications over 3GPP services to support SDDM. The edge applications over 3GPP services are specified in 3GPP TS 24.558 [8] and 3GPP TS 29.558 [10]. Interactions between the SDDM-C, the SDDM-S and the edge applications over 3GPP services are described in detail in clause 7.

# 6 Functional entities

## 6.1 SEAL data delivery management client (SDDM-C)

The SDDM-C functional entity acts as the application client for data delivery management related transactions. To be compliant with the procedures in the present document the SDDM-C:

a) shall support the role of XCAP client as specified in IETF RFC 4825 [12];

b) shall support the role of XDMC as specified in OMA OMA-TS-XDM\_Core-V2\_1 [23]; and

c) shall support the data delivery management procedures in subclause 7.2.

To be compliant with the CoAP procedures in the present document the SDDM-C:

a) shall support the role of CoAP client as specified in IETF RFC 7252 [14];

b) shall support the capability to observe resources as specified in IETF RFC 7641 [15];

c) shall support the block-wise transfer as specified in IETF RFC 7959 [16];

d) may support the robust block transfer as specified in IETF RFC 9177 [22];

e) shall support FETCH method of CoAP as specified in IETF RFC 8132 [17];

f) should support CoAP over TCP and Websocket as specified in IETF RFC 8323 [18];

g) shall support CBOR encoding as specified in IETF RFC 8949 [20]; and

h) shall support the procedures defined in clause 7.2.

NOTE 1: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [7].

NOTE 2: Support for TCP for the CoAP procedures is required if the client connects over the network which blocks or impedes the use of UDP, e.g. when NATs are present in the communication path.

NOTE 3: The CoAP protocol supports mechanism for reliable message exchange over UDP. Use of TCP can also be beneficial if reliable transport is required for other reasons, e.g. better observability of resources. Usage of CoAP over TCP is an implementation choice.

NOTE 4: Support for the robust block transfer mechanism for the CoAP procedures is beneficial in environments where packet loss is highly asymmetrical and where performance optimization of block transfers is required.

## 6.2 SEAL data delivery management server (SDDM-S)

The SDDM-S is a functional entity used to provide data delivery management supported within the vertical application layer. To be compliant with the procedures in the present document the SDDM-S:

a) shall support the role of XCAP server as specified in IETF RFC 4825 [12];

b) shall support the role of XDMS as specified in OMA OMA-TS-XDM\_Core-V2\_1 [23]; and

c) shall support the data delivery management procedures in subclause 7.2.

To be compliant with the CoAP procedures in the present document the SDDM-S:

a) shall support the role of CoAP server as specified in IETF RFC 7252 [14];

b) shall support the capability to observe resources as specified in IETF RFC 7641 [15];

c) shall support the block-wise transfer as specified in IETF RFC 7959 [16];

d) shall support the robust block transfer as specified in IETF RFC 9177 [22];

e) shall support FETCH method of CoAP as specified in IETF RFC 8132 [17];

f) shall support CoAP over TCP and Websocket as specified in IETF RFC 8323 [18];

g) shall support CBOR encoding as specified in IETF RFC 8949 [20]; and

h) shall support the procedures defined in clause 7.2.

NOTE: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [7].

# 7 Data delivery management procedures

## 7.1 General

## 7.2 On-network procedures

### 7.2.1 General

#### 7.2.1.1 Authenticated identity in HTTP request

Upon receiving an HTTP request, the SDDM-S shall verify that the identity of the sender of the HTTP request (see IETF RFC 9110 [21]) is authorized as specified in 3GPP TS 24.547 [7], and if authentication is successful, the SDDM-S shall use the identity of the sender of the HTTP request as an authenticated identity.

#### 7.2.1.2 Authenticated identity in CoAP request

Upon receiving a CoAP request, the SDDM-S shall verify that the identity of the sender of the CoAP request as specified in 3GPP TS 24.547 [7], and if authentication is successful, the SDDM-S shall use the identity of the sender of the CoAP request as an authenticated identity.

### 7.2.2 SEALDD enabled signalling transmission connection establishment procedure

#### 7.2.2.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD regular transmission connection establishment request when it needs to request an SDDM connection establishment, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S.

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <establishment-req> element in the <data-delivery-info> root element which:

1) shall include a <requestor-id> element set to "sealddclient";

2) shall include a <sealdd-flow-id> element set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

3) shall include a <server-id> element set to the information of the VAL server;

4) shall include a <endpoint-id> element set to the information of the endpoint of the selected VAL server to which the SEALDD regular transmission connection establishment request has to be sent;

5) may include a <VAL-service-id> element set to the VAL service identity of the vertical application;

6) may include a <traffic-descriptor-info> element specifying the information of the traffic. In the <traffic-descriptor-info> element, the SDDM-C may include:

i) a <user-plane-address> child element specifying the identity of the IP address of the traffic;

ii) a <port-number> child element specifying the identity of the port number of the traffic;

iii) a <URL> child element specifying the address of a given unique resource on the Web for the traffic;

iv) a <transport-layer-protocol> child element specifying the transport layer protocol for the traffic; and

7) may include an <identity> element with a <VAL-user-id> child element set to the identity of the VAL user or the identity of the SDDM-C acting as the VAL UE and performing the request.

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <establishment-req> element included in the <data-delivery-info> root element;

the SDDM-C:

a) shall generate an HTTP 200 (OK) response message to the SDDM-S according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-C:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <establishment-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD regular transmission connection establishment request operation. If the result is "failure", in the <result> element, the SDDM-S may include a <cause> child element specifying the cause of the failure of the operation, e.g. VAL client error;

ii) may include a <traffic-descriptor-info> element specifying the information of the traffic. In the <traffic-descriptor-info> element, the SDDM-C may include:

A) a <user-plane-address> child element specifying the identity of the IP address of the traffic;

B) a <port-number >child element specifying the identity of the port number of the traffic;

C) a <URL> child element specifying the address of a given unique resource on the Web for the traffic; and

D) a <transport-layer-protocol> child element specifying the transport layer protocol for the traffic.

#### 7.2.2.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <establishment-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps;

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <establishment-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD regular transmission connection establishment request operation. If the result is "failure", in the <result> element, the SDDM-S may include a <cause> child element specifying the cause of the failure of the operation, e.g. VAL client error;

ii) may include a <traffic-descriptor-info> element specifying the information of the traffic. In the <traffic-descriptor-info> element, the SDDM-S may include:

A) a <user-plane-address> child element specifying the identity of the IP address of the traffic;

B) a <port-number>child element specifying the identity of the port number of the traffic;

C) a <URL> child element specifying the address of a given unique resource on the Web for the traffic;

D) a <transport-layer-protocol> child element specifying the transport layer protocol for the traffic; and

iii) may include a <expiry-time> element set to a time that triggers the re-connection from SDDM-C when bandwidth limit check is failed; and

iv) may include a <traffic-transmission-bandwidth> element indicating suggested traffic transmission bandwidth to be used by SDDM-C.

The SDDM-S sends a SEALDD regular transmission connection establishment request when it needs to request a regular SEALDD connection establishment towards an SDDM-C, the SDDM-S shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-S:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-C.

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <establishment-req> element in the <data-delivery-info> root element which:

1) shall include a <requestor-id> element set to "sealddserver";

2) shall include a <sealdd-flow-id> element set to the identity of the SEALDD flow used by the SDDM-C and SDDM-S to identify the application traffic;

3) shall include a <endpoint-id> element set to the information of the endpoint of the selected VAL server to which the SEALDD regular transmission connection establishment request has to be sent;

4) shall include a <sealdd-communication-lifetime> element set to the information of the data delivery communication lifetime;

5) may include a <traffic-descriptor-info> element specifying the information of the traffic. In the <traffic-descriptor-info> element, the SDDM-S may include:

i) a <user-plane-address> child element specifying the identity of the IP address of the traffic;

ii) a <port-number >child element specifying the identity of the port number of the traffic;

iii) a <URL> child element specifying the address of a given unique resource on the Web for the traffic;

iv) a <transport-layer-protocol> child element specifying the transport layer protocol for the traffic; and

6) may include an <identity> element with a <VAL-user-id> child element set to the identity of the VAL user or the identity of the SDDM-S acting as the VAL UE.

#### 7.2.2.3 SDDM client CoAP procedure

In order to request an SEALDD regular transmission connection establishment to the SDDM-S, the SDDM-C shall send a CoAP POST request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP POST request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.1.1 with;

1) the "apiRoot" set to the SDDM-S URI; and

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-establishment-req-info+cbor";

c) shall include a "EstablishmentRequest" object:

1) shall include a "requestorId" attribute set to "sealddclient";

2) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

3) shall include a "serverId" attribute set to the information of the VAL server;

4) shall include an "endpointId" attribute set to the information of the endpoint of the selected VAL server to which the SDMM regular transmission connection establishment request has to be sent;

5) may include a "valServiceId" attribute set to the VAL service identity of the vertical application;

6) may include a "userPlaneAddress" attribute specifying the identity of the IP address of the traffic;

7) may include a"portNumber" attribute specifying the identity of the port number of the traffic;

8) may include a "url" attribute specifying the address of a given unique resource on the Web for the traffic;

9) may include a "transportLayerProtocol" attribute specifying the transport layer protocol for the traffic; and

10) may include a "valUserId" attribute set to the identity of the VAL user or the identity of the SDDM-C acting as the VAL UE and performing the request; and

c) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

Upon receiving a CoAP POST request where the CoAP URI of the CoAP POST request identifies the establishment resource as specified in clause A.3.1.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-establishment-req-info+cbor", and

b) an "EstablishmentRequest" object;

the SDDM-C shall generate a CoAP POST response according to IETF RFC 7252 [14]. In the CoAP POST response message, the SDDM-C:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-establishment-res-info+cbor";

b) shall attempt to create the SDDM regular transmission connection resource pointed at by the CoAP URI with the content of "EstablishmentRequest" object received in the request and:

1) if successfully created, shall include a "EstablishmentResponse" object in the CoAP POST 2.01 (Created) response message;

i) shall include a "result" attribute set to "success"; and

ii) may include a "userPlaneAddress" attribute specifying the identity of the IP address of the traffic;

iii) may include a "portNumber" attribute specifying the identity of the port number of the traffic;

iv) may include a "url" attribute specifying the address of a given unique resource on the Web for the traffic; and

v) may include a "transportLayerProtocol" attribute specifying the transport layer protocol for the traffic; or

2) otherwise, shall include a "EstablishmentResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP POST response; and

c) shall send the CoAP POST response towards the SDDM-S.

#### 7.2.2.4 SDDM server CoAP procedure

Upon receiving a CoAP POST request where the CoAP URI of the CoAP POST request identifies the establishment resource as specified in clause A.3.1.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-establishment-req-info+cbor", and

b) a "EstablishmentRequest" object;

the SDDM-S shall generate a CoAP POST response according to IETF RFC 7252 [14]. In the CoAP POST response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-establishment-res-info+cbor";

b) shall attempt to create the SDDM regular transmission connection resource pointed at by the CoAP URI with the content of "EstablishmentRequest" object received in the request and:

1) if successfully created, shall include an "EstablishmentResponse" object in the CoAP POST 2.01 (Created) response message;

i) shall include a "result" attribute set to "success"; and

ii) may include a "userPlaneAddress" attribute specifying the identity of the IP address of the traffic;

iii) may include a "portNumber" attribute specifying the identity of the port number of the traffic;

iv) may include a "url" attribute specifying the address of a given unique resource on the Web for the traffic; and

v) may include a "transportLayerProtocol" attribute specifying the transport layer protocol for the traffic; or

2) otherwise, shall include an "EstablishmentResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP POST response; and

c) shall send the CoAP POST response towards the SDDM-C.

In order to request an SDDM regular transmission connection establishment to the SDDM-C, the SDDM-S shall send a CoAP POST request message to the SDDM-C according to procedures specified in IETF RFC 7252 [14]. In the CoAP POST request, the SDDM-S:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-C as specified in clause A.4.1.1 with;

1) the "apiRoot" set to the SDDM-C URI; and

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-establishment-req-info+cbor";

c) shall include an "EstablishmentRequest" object:

1) shall include a "requestorId" attribute set to "sealddserver";

2) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

3) shall include an "endpointId" attribute set to the information of the endpoint of the selected VAL server to which the SDMM regular transmission connection establishment request has to be sent;

4) shall include a "sealddCommunicationLifetime" attribute set to the information of the data delivery communication lifetime;

5) may include a "valServiceId" attribute set to the VAL service identity of the vertical application;

6) may include a "userPlaneAddress" attribute specifying the identity of the IP address of the traffic;

7) may include a"portNumber" attribute specifying the identity of the port number of the traffic;

8) may include a "url" attribute specifying the address of a given unique resource on the Web for the traffic;

9) may include a "transportLayerProtocol" attribute specifying the transport layer protocol for the traffic; and

10) may include a "valUserId" attribute set to the identity of the VAL user or the identity of the SDDM-C acting as the VAL UE and performing the request; and

c) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

### 7.2.3 SEALDD enabled signalling transmission connection release procedure

#### 7.2.3.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD data transmission connection release request when it needs to release an established SEALDD connection towards an SDDM-S, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <release-req> element in the <data-delivery-info> root element which:

1) shall include a <sealdd-client-identity> element set to the identity of the SDDM-C; and

2) shall include a <sealdd-flow-id> element set to the identity of the SEALDD flow used by the SDDM-S and SDDM-C to identify the application traffic.

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <release-req> element included in the <data-delivery-info> root element;

the SDDM-C:

a) shall generate an HTTP 200 (OK) response message to the SDDM-S according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-C:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <release-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD data transmission connection release request operation.

#### 7.2.3.2 SDDM server HTTP procedure

The SDDM-S sends a SEALDD data transmission connection release request when it needs to release an established SEALDD connection towards a SDDM-C, the SDDM-S shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-S:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-C;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <release-req> element in the <data-delivery-info> root element which:

1) shall include a <server-id> element set to the information of the SDDM-S; and

2) shall include a <sealdd-flow-id> element set to the identity of the SEALDD flow used by the SDDM-S and SDDM-C to identify the application traffic.

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <release-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection release, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps;

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <release-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD regular transmission connection establishment request operation. If the result is "failure", in the <result> element, the SDDM-S may include a <cause> child element specifying the cause of the failure of the operation, e.g. SEALDD policy mismatch.

#### 7.2.3.3 SDDM client CoAP procedure

In order to request the release of an SEALDD regular data transmission connection to the SDDM-S, the SDDM-C shall send a CoAP DELETE request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP DELETE request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.1.1 with;

1) the "apiRoot" set to the SDDM-S URI; and

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-release-req-info+cbor";

c) shall include a "ReleaseRequest" object:

1) shall include a "sealClientId" attribute set to the identity of the SDDM-C;

2) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

Upon receiving a CoAP DELETE request where the CoAP URI of the CoAP DELETE request identifies the release resource as specified in clause A.3.1.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-release-req-info+cbor", and

b) a "ReleaseRequest" object;

the SDDM-C shall generate a CoAP DELETE response according to IETF RFC 7252 [14]. In the CoAP DELETE response message, the SDDM-C:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-info+cbor";

b) shall attempt to release the SDDM regular transmission connection resource pointed at by the CoAP URI with the content of "ReleaseRequest" object received in the request and:

1) if successfully release, shall use the CoAP DELETE 2.02 (Deleted) response message; or

2) otherwise, shall include an error response in the CoAP DELETE response as specified in clause  A.3.1.2.2.3.2; and

c) shall send the CoAP DELETE response towards the SDDM-S.

#### 7.2.3.4 SDDM server CoAP procedure

Upon receiving a CoAP DELETE request where the CoAP URI of the CoAP DELETE request identifies the release resource as specified in clause A.4.1.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-release-req-info+cbor", and

b) a "ReleasetRequest" object;

the SDDM-S shall generate a CoAP DELETE response according to IETF RFC 7252 [14]. In the CoAP DELETE response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-info+cbor";

b) shall attempt to release the SDDM regular transmission connection resource pointed at by the CoAP URI with the content of "ReleaseRequest" object received in the request and:

1) if successfully created, shall use the CoAP DELETE 2.02 (Deleted) response message; or

2) otherwise, shall include an error response in the CoAP DELETE response as specified in clause A.4.1.2.2.3.2; and

c) shall send the CoAP DELETE response towards the SDDM-C.

In order to request the release of an SDDM regular data transmission connection to the SDDM-C, the SDDM-S shall send a CoAP DELETE request message to the SDDM-C according to procedures specified in IETF RFC 7252 [14]. In the CoAP DELETE request, the SDDM-S:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-C as specified in clause A.3.1.1 with;

1) the "apiRoot" set to the SDDM-C URI; and

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-release-req-info+cbor";

c) shall include an "ReleaseRequest" object:

1) shall include a "serverId" attribute set to the identity of the SDDM-S;

2) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

### 7.2.4 SEALDD enabled E2E redundant transmission path establishment procedure

#### 7.2.4.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD URLLC transmission connection establishment request when it needs to request a SEALDD URLLC transmission connection establishment, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <URLLC-establishment-req> element in the <data-delivery-info> root element which:

1) shall include a <sealdd-client-identity> element set to the identity of the SDDM-C;

2) shall include a <sealdd-flow-id> element set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

3) may include an <identity> element with a <VAL-user-id> child element set to the identity of the VAL user or the identity of the SDDM-C acting as the VAL UE and performing the request;

4) may include a <server-id> element set to the information of the endpoint of the selected VAL server to which the SDDM URLLC transmission connection establishment request has to be sent;

5) may include a <VAL-service-id> element set to the VAL service identity of the vertical application; and

6) may include a <traffic-descriptor-info> element specifying the information of the traffic of the redundant SEALDD transmission connection. In the <traffic-descriptor-info> element, the SDDM-C may include:

i) a <user-plane-address> child element specifying the identity of the IP address of the traffic;

ii) a <port-number> child element specifying the identity of the port number of the traffic;

iii) a <URL> child element specifying the address of a given unique resource on the Web for the traffic;

iv) a <transport-layer-protocol> child element specifying the transport layer protocol for the traffic.

#### 7.2.4.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <URLLC-establishment-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1 and

1) if the identity of the sender of the received HTTP POST request is not authorized to request URLCC transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps; and

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <URLLC-establishment-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD URLLC transmission connection establishment request operation. If the result is "failure", in the <result> element, the SDDM-S may include a <cause> child element specifying the cause of the failure of the operation, e.g. VAL client error; and

ii) may include a <traffic-descriptor-info> element specifying the information of the traffic of the redundant SEALDD transmission connection. In the <traffic-descriptor-info> element, the SDDM-S may include:

A) a <user-plane-address> child element specifying the identity of the IP address of the traffic;

B) a <port-number>child element specifying the identity of the port number of the traffic;

C) a <URL> child element specifying the address of a given unique resource on the Web for the traffic; and

D) a <transport-layer-protocol> child element specifying the transport layer protocol for the traffic.

#### 7.2.4.3 SDDM client CoAP procedure

In order to request an SEADD URLLC transmission connection establishment to the SDDM-S, the SDDM-C shall send a CoAP POST request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP POST request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.2.1 with;

1) the "apiRoot" set to the SDDM-S URI; and

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-establishment-req-info+cbor";

c) shall include a "URLLCEstablishmentRequest" object:

1) shall include a "sealClientId" attribute set of the identity of the SDDM-C;

2) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

3) shall include a "valTgtUe" attribute set to the identity of the VAL user or the identity of the SDDM-C acting as the VAL UE and performing the request;

4) may include a "serverId" attribute set to the information of the VAL server;

5) may include a "valServiceId" attribute set to the identity of the VAL service of the vertical application;

6) may include a "userPlaneAddress" attribute specifying the identity of the IP address of the traffic;

7) may include a"portNumber" attribute specifying the identity of the port number of the traffic;

8) may include a "url" attribute specifying the address of a given unique resource on the Web for the traffic;

9) may include a "transportLayerProtocol" attribute specifying the transport layer protocol for the traffic; and

c) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.4.4 SDDM server CoAP procedure

Upon receiving a CoAP POST request where the CoAP URI of the CoAP POST request identifies the establishment resource as specified in clause A.4.2.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-establishment-req-info+cbor", and

b) a "URLCCEstablishmentRequest" object;

the SDDM-S shall generate a CoAP POST response according to IETF RFC 7252 [14]. In the CoAP POST response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-establishment-res-info+cbor";

b) shall attempt to create the URLCC transmission connection resource pointed at by the CoAP URI with the content of "EstablishmentRequest" object received in the request and:

1) if successfully created, shall include an "URLCCEstablishmentResponse" object in the CoAP POST 2.01 (Created) response message;

i) shall include a "result" attribute set to "success"; and

ii) may include a "userPlaneAddress" attribute specifying the identity of the IP address of the traffic;

iii) may include a "portNumber" attribute specifying the identity of the port number of the traffic;

iv) may include a "url" attribute specifying the address of a given unique resource on the Web for the traffic; and

v) may include a "transportLayerProtocol" attribute specifying the transport layer protocol for the traffic; or

2) otherwise, shall include an "URLCCEstablishmentResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP POST response; and

c) shall send the CoAP POST response towards the SDDM-C.

### 7.2.5 SEALDD enabled E2E redundant transmission path release procedure

#### 7.2.5.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD URLLC transmission connection release request when it needs to release an established SEALDD URLLC transmission connection towards an SDDM-S, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <URLLC-release-req> element in the <data-delivery-info> root element which:

1) shall include a <sealdd-client-identity> element set to the identity of the SDDM-C; and

2) shall include a <sealdd-flow-id> element set to the identity of the SEALDD flow used by the SDDM-S and SDDM-C to identify the application traffic.

#### 7.2.5.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <URLLC-release-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection release, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps;

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <URLLC-release-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD URLLC transmission connection release request operation. If the result is "failure", in the <result> element, the SDDM-S may include a <cause> child element specifying the cause of the failure of the operation, e.g. SEALDD policy mismatch.

#### 7.2.5.3 SDDM client CoAP procedure

In order to request the release of an SEALDD URLLC transmission connection to the SDDM-S, the SDDM-C shall send a CoAP DELETE request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP DELETE request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.2.1 with;

1) the "apiRoot" set to the SDDM-S URI; and

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-releasee-req-info+cbor";

c) shall include a "URLLCReleaseRequest" object:

1) shall include a "sealClientId" attribute set to the identity of the SDDM-C;

2) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.5.4 SDDM server CoAP procedure

Upon receiving a CoAP DELETE request where the CoAP URI of the CoAP DELETE request identifies the release resource as specified in clause A.4.2.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-releasee-req-info+cbor", and

b) a "URLLCReleasetRequest" object;

the SDDM-S shall generate a CoAP DELETE response according to IETF RFC 7252 [14]. In the CoAP DELETE response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-releasee-req-info+cbor";

b) shall attempt to release the SDDM URLLC transmission connection resource pointed at by the CoAP URI with the content of "URLLCReleaseRequest" object received in the request and:

1) if successfully created, shall use the CoAP DELETE 2.02 (Deleted) response message; or

2) otherwise, shall include an error response in the CoAP DELETE response as specified in clause A.4.2.2.2.3.3; and

c) shall send the CoAP DELETE response towards the SDDM-C.

### 7.2.6 SEALDD enabled E2E redundant transmission path connection update procedure

#### 7.2.6.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD URLLC transmission connection update request when it needs to request a SEALDD URLLC transmission connection update, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S.

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <URLLC-update-req> element in the <data-delivery-info> root element which:

1) shall include a <sealdd-client-identity> element set to the identity of the SDDM-C;

2) shall include a <sealdd-flow-id> element set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

2) may include a <server-id> element set to the information of the endpoint of the selected VAL server to which the SDDM URLLC transmission connection establishment request has to be sent;

3) may include a <VAL-service-id> element set to the VAL service identity of the vertical application;

4) may include a <traffic-descriptor-info> element specifying the information of the traffic of the redundant SEALDD transmission connection. In the <traffic-descriptor-info> element, the SDDM-C may include:

i) a <user-plane-address> child element specifying the identity of the IP address of the traffic;

ii) a <port-number> child element specifying the identity of the port number of the traffic;

iii) a <URL> child element specifying the address of a given unique resource on the Web for the traffic;

iv) a <transport-layer-protocol> child element specifying the transport layer protocol for the traffic.

#### 7.2.6.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-deliverydata-delivery-info+xml MIME body with a <URLLC-update-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps;

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-deliverydata-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-deliverydata-delivery-info+xml MIME body with a <URLLC-update-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD URLLC transmission connection update request operation. If the result is "failure", in the <result> element, the SDDM-S may include a <cause> child element specifying the cause of the failure of the operation, e.g. VAL client error.

#### 7.2.6.3 SDDM client CoAP procedure

In order to request an SEALDD URLLC transmission connection update to the SDDM-S, the SDDM-C shall send a CoAP PUT request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP PUT request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.2.1 with;

1) the "apiRoot" set to the SDDM-S URI; and

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-update-req-info+cbor";

c) shall include a "URLLCUpdateRequest" object:

1) shall include a "sealClientId" attribute set of the identity of the SDDM-C;

2) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

3) may include a "serverId" attribute set to the information of the VAL server;

4) may include a "valServiceId" attribute set to the identity of the VAL service of the vertical application;

5) may include a "userPlaneAddress" attribute specifying the identity of the IP address of the traffic;

6) may include a"portNumber" attribute specifying the identity of the port number of the traffic;

7) may include a "url" attribute specifying the address of a given unique resource on the Web for the traffic;

8) may include a "transportLayerProtocol" attribute specifying the transport layer protocol for the traffic; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.6.4 SDDM server CoAP procedure

Upon receiving a CoAP PUT request where the CoAP URI of the CoAP PUT request identifies the resource to be updated as specified in clause A.4.2.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-update-req-info+cbor", and

b) a "URLCCUpdateRequest" object;

the SDDM-S shall generate a CoAP PUT response according to IETF RFC 7252 [14]. In the CoAP PUT response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-urllc-update-req-info+cbor";

b) shall attempt to update the URLCC transmission connection resource pointed at by the CoAP URI with the content of "EstablishmentRequest" object received in the request and:

1) if successfully updated, use the CoAP PUT 2.04 (Changed) response message; or

2) otherwise, shall include an error response in the CoAP PUT response as specified in clause A.4.1.2.2.3.2; and

c) shall send the CoAP PUT response towards the SDDM-C.

### 7.2.7 SEALDD server discovery and selection procedure

When the VAL client sends a SEALDD request to the SDDM-C, the SDDM-C may need to discover and select the appropriate SDDM-S for the associated vertical application. After that, the VAL server is discovered and selected along with the associated SDDM-S so that the SDDM-C gets the address of the SDDM-S.

In an edge data network (EDN), the SDDM-C can use edge applications over 3GPP services (see clause 5) to obtain the EES, which supports the SDDM-S and the VAL server, and after that to obtain the SDDM-S address and the VAL server address.

NOTE 1: The VAL server acts as an EAS in an EDN and registers to the EES with the associated SDDM-S address as EAS endpoint in the EAS profile (see 3GPP TS 23.433 [2] clause 9.4.3.2). The Eecs\_ServiceProvisioning service to obtain the EES, which supports the SDDM-S and the VAL sever, and the Eees\_EASDiscovery service to obtain the SDDM-S address and the VAL server address are specified in clause 7.2 and clause 5.3 of 3GPP TS 24.558 [8] respectively.

In a non EDN, the SDDM-C can obtain the SDDM-S address and the VAL server address from the VAL client or from the NAS.

NOTE 2: ECS address provisioning over NAS to get ECS configuration information and EAS discovery to get EAS information are specified in 3GPP TS 24.501 [5].

NOTE 3: The VAL client can use DNS query mechanism or vertical application (e.g. V2X) layer signalling mechanism to obtain the SDDM-S address and the VAL server address. The VAL client can provide the address information to the SDDM-C.

NOTE 4: DNS query mechanism and vertical application layer signalling mechanism are out of scope of the present document.

### 7.2.8 SEALDD enabled data storage creation procedure

#### 7.2.8.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD data storage creation request when it needs to request the creation of data storage to the SDDM-S, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <data-storage-creation-req> element in the <data-delivery-info> root element which:

1) shall include a <application-data> element set to the application data needed to be stored;

2) may include a <access-control-policy> element set to the control policy for the requested data access from other consumers (e.g. SDDM-C, VAL server, other SDDM-S);

3) may include a <expiry-time> element set to the expiration time of the data to be stored; and

4) may include a <status-information-req> element set to the information of the stored data to be tracked or monitored by the SDDM-S (e.g. statistics of the stored data; indications of how often the stored data is accessed or managed) for corresponding notifications.

#### 7.2.8.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-creation-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps;

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-creation-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD data storage creation request operation; and

ii) may include a <data-identifier> element set to the identity of the stored data.

#### 7.2.8.3 SDDM client CoAP procedure

In order to request an SEALDD data storage creation to the SDDM-S, the SDDM-C shall send a CoAP POST request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP POST request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.3.1 with the "apiRoot" set to the SDDM-S URI;

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-creation-req-info+cbor";

c) shall include a "DataStorageCreationRequest" object:

1) shall include an "applicationData" attribute set to the application data needed to be stored;

2) may include an "accessControlPolicy" attribute set to the control policy for the requested data access from other consumers (e.g. SDDM-C, VAL server, other SDDM-S);

3) may include an "expiryTime" attribute set to the expiration time of the data to be stored;

4) may include a "statusInformationReq" attribute set to the information of the stored data to be tracked or monitored by the SDDM-S (e.g. statistics of the stored data; indications of how often the stored data is accessed or managed) for corresponding notifications; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.8.4 SDDM server CoAP procedure

Upon receiving a CoAP POST request where the CoAP URI of the CoAP POST request identifies the creation of a data storage resource as specified in clause A.4.3.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-creation-req-info+cbor", and

b) a "DataStorageCreationRequest" object;

the SDDM-S shall generate a CoAP POST response according to IETF RFC 7252 [14]. In the CoAP POST response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-creation-res-info+cbor";

b) shall attempt to create the SDDM data creation storage resource pointed at by the CoAP URI with the content of "DataStorageCreationRequest" object received in the request and:

1) if successfully created, shall include a "DataStorageCreationResponse" object in the CoAP POST 2.01 (Created) response message;

i) shall include a "result" attribute set to "success"; and

ii) shall include a "dataIdentifier" attribute specifying the identity of the stored data; or

2) otherwise, shall include a "DataStorageCreationResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP POST response; and

c) shall send the CoAP POST response towards the SDDM-C.

### 7.2.9 SEALDD enabled data storage reservation procedure

#### 7.2.9.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD data storage reservation request when it needs to request the reservation of data storage to the SDDM-S, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <data-storage-reservation-req> element in the <data-delivery-info> root element which:

1) shall include a <VAL-service-id> element set to the VAL service identity of the vertical application;

2) may include a <data-length> element set to the data length to be stored;

#### 7.2.9.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-reservation-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps;

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-reservation-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD data storage reservation request operation; and

ii) may include a <address> element set to the reserved address for data storage.

#### 7.2.9.3 SDDM client CoAP procedure

In order to request an SEALDD data storage reservation to the SDDM-S, the SDDM-C shall send a CoAP POST request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP POST request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.3.1 with the "apiRoot" set to the SDDM-S URI;

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-reservation-req-info+cbor";

c) shall include a "DataStorageReservationRequest" object:

1) shall include a "valServiceId" attribute set to the identity of the VAL service of the vertical application;

2) may include a "dataLength" attribute set to the data length to be stored; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.9.4 SDDM server CoAP procedure

Upon receiving a CoAP POST request where the CoAP URI of the CoAP POST request identifies the creation of a data storage resource as specified in clause A.4.3.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-reservation-req-info+cbor", and

b) a "DataStorageReservationRequest" object;

the SDDM-S shall generate a CoAP POST response according to IETF RFC 7252 [14]. In the CoAP POST response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-reservation-res-info+cbor";

b) shall attempt to create the SDDM data creation storage resource pointed at by the CoAP URI with the content of "DataStorageReservationRequest" object received in the request and:

1) if successfully created, shall include a "DataStorageReservationResponse" object in the CoAP POST 2.01 (Created) response message;

i) shall include a "result" attribute set to "success"; and

ii) shall include an "address" attribute specifying the reserved address for data storage; or

2) otherwise, shall include a "DataStorageReservationResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP POST response; and

c) shall send the CoAP POST response towards the SDDM-C.

### 7.2.10 SEALDD enabled data storage notification procedure

#### 7.2.10.1 SDDM client HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-status-notification> element included in the <data-delivery-info> root element;

the SDDM-C:

a) shall generate an HTTP 200 (OK) response message to the SDDM-S according to IETF RFC 9110 [21].; and

b) may communicate the received data storage notification information to the VAL client.

#### 7.2.10.2 SDDM server HTTP procedure

The SDDM-S sends a SEALDD data storage notification when it needs to provide the SDDM-C with the collected management or storage status information of the stored data. The SDDM-S shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-S:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-C:

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <data-storage-status-notification > element in the <data-delivery-info> root element which:

1) shall include a <data-identifier> element set to the identity of the stored data; and

2) shall include a <status-information-rsp> element set to the information of the stored data to be tracked or monitored by the SDDM-S (e.g. statistics of the stored data, indications of how often the stored data is accessed or managed), of the stored data requested by using the SEALDD data storage creation request as described in clause 7.2.7.1.

NOTE: Push notification service can be used to send HTTP POST request to the client. Details about the push notification service is out of scope this specification.

#### 7.2.10.3 SDDM client CoAP procedure

Upon receiving a CoAP FETCH 2.05 (Content) response (as specified in IETF RFC 8132 [17]) to a CoAP FETCH request message used to observe an SDDM data storage resource as specified in clause A.4.3.2.2.3.5, and containing:

a) an "observe" option;

b) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-status-notification-info+cbor", and

c) a "DataStorageStatusNotification" object;

NOTE: The SDDM-C can communicate the received data storage notification information to the VAL client.

#### 7.2.10.4 SDDM server CoAP procedure

In order to notify a SDDM-C about information of an SDDM data storage resource, the SDDM-S shall send a CoAP FETCH response (as specified in IETF RFC 8132 [17]) message to the SDDM-C according to procedures specified in IETF RFC 7252 [14] in response to a CoAP FETCH request message used to observe an SDDM data storage resource as specified in clause A.4.3.2.2.3.5. In the CoAP FETCH response, the SDDM-S:

a) shall include an "observe" option;

b) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-status-notification-info+cbor";

c) shall include an "DataStorageStatusNotification" object in the CoAP FETCH 2.05 (Content) response message; and

d) shall send the CoAP FETCH response towards the SDDM-C.

### 7.2.11 SEALDD enabled data storage query procedure

#### 7.2.11.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD data storage query request when it needs to query stored data in the SDDM-S, the SDDM-C shall send an HTTP GET request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP GET request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <data-storage-query-req> element in the <data-delivery-info> root element which:

1) shall include a <data-identifier> element set to the identity of the stored data which is queried.

#### 7.2.11.2 SDDM server HTTP procedure

Upon receiving an HTTP GET request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-query-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP GET request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP GET request is not authorized to request signalling transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP GET request and shall skip rest of the steps;

2) shall support handling an HTTP GET request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "GET Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-query-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD data storage query request operation;

ii) shall include a <data-identifier> element set to the identity of the stored data which is queried; and

iii) may include a <application-data> element set to the application data queried.

#### 7.2.11.3 SDDM client CoAP procedure

In order to query an SDDM data storage resource, the SDDM-C shall send a CoAP GET request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP GET request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.3.1 with:

1) the "apiRoot" set to the SDDM-S URI; and

2) the "data-identifier" query option is set to the identity of the stored data which is queried; and

b) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.11.4 SDDM server CoAP procedure

Upon receiving a CoAP GET request where the CoAP URI of the CoAP GET request identifies the creation of a data storage resource as specified in clause A.4.3.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-info+cbor", and

b) a "data-identifier" query option;

the SDDM-S shall generate a CoAP GET response according to IETF RFC 7252 [14]. In the CoAP GET response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-query-res-info+cbor ";

b) shall attempt to create the SDDM data creation storage resource pointed at by the CoAP URI with the content of "DataStorageQueryRequest" object received in the request and:

1) if successfully created, shall include a "DataStorageQueryResponse" object in the CoAP GET 2.05 (Content) response message:

i) shall include a "result" attribute set to "success";

ii) shall include a "dataIdentifier" attribute specifying the identity of the stored data; and

iii) may include an "applicationData" attribute set to the application data queried; or

2) otherwise, shall include a "DataStorageQueryResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP GET response; and

c) shall send the CoAP GET response towards the SDDM-C.

### 7.2.12 SEALDD enabled data storage management procedure

#### 7.2.12.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD data storage management request when it needs to request management of the stored data in the SDDM-S such as to update, refresh, or delete the stored data, the SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <data-storage-mgt-req> element in the <data-delivery-info> root element which:

1) shall include a <data-identifier> element set to the identity of the stored data which is requested to be managed;

2) shall include a <operation> element set to the operation to be performed such as to update, refresh, or delete the stored data; and

3) may include an <application-data> element set to the application data needed to be updated if the operation to be performed is to update the stored data.

#### 7.2.12.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-mgt-req> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1; and

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps;

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-S:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <data-storage-mgt-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD data storage query request operation;

ii) shall include a <data-identifier> element set to the identity of the stored data which is queried; and

iii) may include a <application-data> element set to the application data managed according to the operation requested on the stored data.

#### 7.2.12.3 SDDM client CoAP procedure

In order to request an SEALDD data storage management request to the SDDM-S, the SDDM-C shall send:

a) a CoAP PUT request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14] when it needs to request update of the stored data; or

b) a CoAP DELETE request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14] when it needs to request delete of the stored data.

In the CoAP PUT request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.3.1 with the "apiRoot" set to the SDDM-S URI;

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor";

c) shall include a "DataStorageMgtRequest" object:

1) shall include a "dataIdentifier" attribute set to the identity of the stored data which is requested to be managed;

2) shall include an "applicationData" attribute set to the application data needed to be stored; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

In the CoAP DELETE request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.4.3.1 with the "apiRoot" set to the SDDM-S URI;

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor";

c) shall include a "DataStorageMgtRequest" object:

1) shall include a "dataIdentifier" attribute set to the identity of the stored data which is requested to be managed; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.12.4 SDDM server CoAP procedure

Upon receiving a CoAP PUT request or a CoAP DELETE request where the CoAP URI of the CoAP PUT request or the CoAP DELETE request identifies the resource to be updated as specified in clause A.4.3.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor", and

b) a "DataStorageMgtRequest" object;

the SDDM-S shall generate either a CoAP PUT response or a CoAP DELETE response according to IETF RFC 7252 [14]. In either the CoAP PUT response message or the CoAP DELETE message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor";

b) if the received message is a CoAP PUT request:

1) shall attempt to update the SDDM data storage resource pointed at by the CoAP URI with the content of "DataStorageMgtRequest" object received in the CoAP PUT request and:

i) if successfully updated, shall use the CoAP PUT 2.04 (Changed) response message; or

ii) otherwise, shall include an error response in the CoAP PUT response as specified in clause A.4.3.2.2.3.2; and

iii) shall send the CoAP PUT response towards the SDDM-C; or

b) if the received message is a CoAP DELETE request:

1) shall attempt to release the SDDM data storage resource pointed at by the CoAP URI with the content of "DataStorageMgtRequest" object received in the CoAP DELETE request and:

i) if successfully created, shall use the CoAP DELETE 2.02 (Deleted) response message; or

ii) otherwise, shall include an error response in the CoAP DELETE response as specified in clause A.3.2.2.2.3.2; and

iii) shall send the CoAP DELETE response towards the SDDM-C.

### 7.2.13 SEALDD server relocation procedure

The SDDM-S can be relocated because of either SDDM-C mobility or SDDM-S load re-balancing (see 3GPP TS 23.433 [2] clause 9.6).

NOTE 1: SEALDD server relocation is specified in 3GPP TS 29.548 [9].

In an edge data network (EDN),the SDDM-C can use edge applications over 3GPP services (see clause 5) to discover the new SDDM-S. The SDDM-C can obtain the new SDDM-S address by using the SEALDD server discovery and selection procedure described in clause 7.2.7.

NOTE 2: The VAL server acts as an EAS in an EDN and it registers to the EES with the associated SDDM-S address as EAS endpoint in the EAS profile (see 3GPP TS 23.433 [2] clause 9.6.2.2). The SDDM-C mobility triggers the execution of an application context relocation (ACR) procedure or the VAL server triggers ACR due to load re-balancing. The Eees\_ACREvents service and the Eees\_AppContextRelocation service are specified in 3GPP TS 24.558 [8] and 3GPP TS 29.558 [10].

In a non EDN, the SDDM-C can obtain the new SDDM-S address from the VAL client or from the NAS. After that the SDDM-C can establish a new SEALDD communication channel including the old communication channel information. The SDDM-S can discover an equivalent SDDM-S (e.g. using DNS query mechanism).

NOTE 3: The VAL client can use DNS query mechanism or vertical application (e.g. V2X) layer signalling mechanism to obtain the new SDDM-S address. The VAL client can provide the address information to the SDDM-C.

NOTE 4: DNS query mechanism and vertical application layer signalling mechanism are out of scope of the present document.

NOTE 5: The SDDM-C and vertical applications can receive one or more EAS rediscovery indication(s) from the NAS as specified in 3GPP TS 24.501 [5] and 3GPP TS 24.008 [4].

### 7.2.14 SEALDD enabled data transmission quality measurement subscription procedure

#### 7.2.14.1 SDDM client HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <measurements-subscription-req> element included in the <data-delivery-info> root element;

the SDDM-C:

a) shall generate an HTTP 200 (OK) response message to the SDDM-S according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-C:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <measurements-subscription-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD data transmission quality measurement subscription request operation; and

ii) may include a <expiry-time> element specifying the expiration time of the subscription. This element shall be included when the SEALDD data transmission quality measurement subscription request operation is "success", otherwise this element shall be ignored by the SDDM-S.

#### 7.2.14.2 SDDM server HTTP procedure

The SDDM-S sends a SEALDD data transmission quality measurement subscription request when it needs to request to carry out data transmission quality measurement towards an SDDM-C, the SDDM-S shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-S:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-C.

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <measurements-subscription-req> element in the <data-delivery-info> root element which:

1) shall include a <sealdd-flow-id> element set to the identity of the SDDM flow used by the SDDM-C and SDDM-S;

2) shall include a <measurement-requirement-list> element specifying measurement requirement information. In the <measurement-requirement-list> element, the SDDM-S:

i) shall include a <measurement-id> child element set to measurement identifiers, e.g. latency, bitrate, jitter;

ii) may include a <reporting-frequency> child element set to reporting frequency of measurement results (e.g. "periodic", "now"). If not present, it implies periodic reporting;

iii) may include a <reporting-periodicity> child element set to the reporting periodicity if the reporting frequency is periodic. This child element shall be included when the reporting frequency of a measurement identifier is "periodic";

iv) may include a <measurement-window> child element set to the measurement period window for transmission quality measurements;

v) may include a <expiry-time> child element set to the expiration time of the measurement;

vi) may include a <sealdd-policy> child element specifying quality guarantee policies associated with the SEALDD connection. In the <sealdd-policy> element, the SDDM-S shall include:

A) a <quality-guarantee-policy> child element set to the measurement threshold to be measured for the quality guarantee; and

vii) may include a <reporting-criteria> child element set to 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 criterion of more than one criteria is specified.

3) may include a <measurement-conditions> element set to the temporal conditions, spatial conditions or both.

#### 7.2.14.3 SDDM client CoAP procedure

Upon receiving a CoAP POST request where the CoAP URI of the CoAP POST request identifies the establishment resource as specified in clause A.3.2.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-measurement-subscription-req-info+cbor", and

b) a "MeasurementsSubscriptionRequest" object;

the SDDM-C shall generate a CoAP POST response according to IETF RFC 7252 [14]. In the CoAP POST response message, the SDDM-C:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-measurement-subscription-res-info+cbor";

b) shall attempt to create the SDDM data transmission quality measurement resource pointed at by the CoAP URI with the content of "MeasurementsSubscriptionResquest" object received in the request and:

1) if successfully created, shall include a "MeasurementsSubscriptionResponse" object in the CoAP POST 2.01 (Created) response message;

i) shall include a "result" attribute set to "success"; and

ii) may include an "expiryTime" attribute specifying the expiration time of the subscription; or

2) otherwise, shall include a "MeasurementsSubscriptionResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP POST response; and

c) shall send the CoAP POST response towards the SDDM-S.

#### 7.2.14.4 SDDM server CoAP procedure

In order to request an SEALDD data transmission quality measurement subscription establishment to the SDDM-C, the SDDM-S shall send a CoAP POST request message to the SDDM-C according to procedures specified in IETF RFC 7252 [14]. In the CoAP POST request, the SDDM-S:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-C as specified in clause A.3.2.1 with the "apiRoot" set to the SDDM-C URI:

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-measurement-subscription-req-info+cbor";

c) shall include a "MeasurementsSubscriptionRequest" object:

1) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic;

2) shall include a "measurementId" attribute set to the measurement identifiers, e.g. latency, bitrate, jitter;

3) may include a "reportingFrequency" attribute set to reporting frequency of measurement results (e.g. "periodic", "now"). If not present, it implies periodic reporting;

4) may include a "reportingPeriodicity" attribute set to the reporting periodicity if the reporting frequency is periodic. This attribute shall be included when the reporting frequency of a measurement identifier is "periodic";

5) may include a "measurementWindow" attribute set to the measurement period window for transmission quality measurements;

6) may include an "expiryTime" attribute set to the expiration time of the measurement;

7) may include a "sealddPolicy" object specifying quality guarantee policies associated with the SEALDD connection;

8) may include a "reportingCriteria" attribute set to 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 criterion of more than one criteria is specified;

9) may include a "measurementConditions" object specifying the temporal conditions, spatial conditions or both; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

### 7.2.15 SEALDD enabled data transmission quality measurement notification procedure

#### 7.2.15.1 SDDM client HTTP procedure

The SDDM-C sends a SEALDD data transmission quality measurement notification when it needs to provide the SDDM-S with transmission quality measurements. The SDDM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-C:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-S;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <measurements-notification> element in the <data-delivery-info> root element which:

1) shall include a <measurement-requirement-notify-list> element specifying measurement requirement information. In the <measurement-requirement-notify-list> element, the SDDM-S:

i) shall include a <measurement-id> child element set to measurement identifiers, e.g. latency, bitrate, jitter;

ii) may include an <identity-measurements> child element which shall include one of the following elements:

A) a <VAL-ue-id-list> element with one or more <VAL-ue-id> child elements set to the identities of the VAL UEs for whom SEALDD measurement applies. For multiple VAL UEs reporting granularity set to individual UE, the associated measurement values are for individual VAL UE; or

B) a <VAL-group-id> element set to the identity of the VAL group for whom SEALDD measurement applies for which the associated measurement values are aggregation for all VAL UEs or the VAL UE group;

iii) may include a <average-measurement-value> child element set to the average measurement value of measurement results;

iv) may include a <minimum-measurement-value> child element set to the minimum measurement value of measurement results;

v) may include a <maximum-measurement-value> child element set to the maximum measurement value of measurement results;

vi) may include a <standard-deviation-measurement-value> child element set to standard deviation measurement value of measurement results;

vii) may include a <kpercentile-measurement-value> child element set to the kpercentile measurement value of measurement results;

viii) may include a <measurement-period> child element set to the measurement period; and

ix) may include a <timestamp> child element set to the timestamp of measurement results.

#### 7.2.15.2 SDDM server HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <measurements-notification> element included in the <data-delivery-info> root element;

the SDDM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 7.2.1.1 and:

1) if the identity of the sender of the received HTTP POST request is not authorized to request signalling transmission connection establishment, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps; and

2) shall support handling an HTTP POST request from an SDDM-C according to procedures specified in IETF RFC 4825 [12] "POST Handling"; and

b) shall generate an HTTP 200 (OK) response message to the SDDM-C according to IETF RFC 9110 [21]. The SDDM-S shall communicate the received data transmission quality measurement results (e.g. latency, jitter, bitrate) to the VAL server by using the SDD\_TransmissionQualityMeasurement service as specified in 3GPP TS 29.548 [9].

#### 7.2.15.3 SDDM client CoAP procedure

In order to provide an SALDD data transmission quality measurement to the SDDM-S, the SDDM-C shall send a CoAP PUT request message to the SDDM-S according to procedures specified in IETF RFC 7252 [14]. In the CoAP PUT request, the SDDM-C:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-S as specified in clause A.3.2.1 with the "apiRoot" set to the SDDM-S URI;

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-measurement-notification-info+cbor";

c) shall include a "MeasurementsNotification" object:

1) shall include a "measurementId" attribute set to the measurement identifiers, e.g. latency, bitrate, jitter;

2) may include a "valUeIdList" attribute set to the identities of the VAL UEs for whom SEALDD measurement applies. For a single VAL UE, this attribute can be omitted and the associated measurement values are for the single VAL UE. For multiple VAL UEs with reporting granularity set to individual UE, the associated measurement values are for individual VAL UE. For multiple VAL UEs with reporting granularity set to VAL UE group or all VAL UEs, the associated measurement values are aggregation for all VAL UEs or the VAL UE group;

3) may include an "averageMeasurementValue" attribute set to the average measurement value of measurement results;

4) may include a "maximumMeasurementValue" attribute set to the maximum measurement value of measurement results;

5) may include a "minimumMeasurementValue" attribute set to the minimum measurement value of measurement results;

6) may include a "standardDeviationMeasurementValue" attribute set to the standard deviation measurement value of measurement results;

7) may include a "kPercentileMeasurementValue" attribute set to the kpercentile measurement value of measurement results;

8) may include a "measurementPeriod" attribute set to the measurement period;

9) may include a "timeStamp" attribute set to the timestamp of measurement results; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

#### 7.2.15.4 SDDM server CoAP procedure

Upon receiving a CoAP PUT request where the CoAP URI of the CoAP PUT request identifies the resource to be updated as specified in clause A.3.2.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-measurement-notification-info+cbor", and

b) a "MeasurementsNotification" object;

the SDDM-S shall generate a CoAP PUT response according to IETF RFC 7252 [14]. In the CoAP PUT response message, the SDDM-S:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-info+cbor";

b) shall attempt to update the SDDM transmission quality measurement resource pointed at by the CoAP URI with the content of "MeasurementsNotification" object received in the CoAP PUT request and:

1) if successfully updated, shall use the CoAP PUT 2.04 (Changed) response message; or

2) otherwise, shall include an error response in the CoAP PUT response as specified in clause A.3.2.2.2.3.2; and

c) shall send the CoAP PUT response towards the SDDM-C; and

d) The SDDM-S shall communicate the received data transmission quality measurement results (e.g. latency, jitter, bitrate) to the VAL server by using the SDD\_TransmissionQualityMeasurement service as specified in 3GPP TS 29.548 [9].

### 7.2.16 SEALDD enabled data transmission quality guarantee procedure

#### 7.2.16.1 SDDM client HTTP procedure

Upon receiving an HTTP POST request containing:

a) an Accept header field set to "application/vnd.3gpp.seal-data-delivery-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

c) an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <tx-quality-management-req> element included in the <data-delivery-info> root element;

the SDDM-C:

a) shall generate an HTTP 200 (OK) response message to the SDDM-S according to IETF RFC 9110 [21]. In the HTTP 200 (OK) response message, the SDDM-C:

1) shall include a Content-Type header field set to "application/vnd.3gpp.seal-data-delivery-info+xml"; and

2) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with a <tx-quality-management-rsp> element in the <data-delivery-info> root element which:

i) shall include a <result> element set to "success" or "failure" indicating success or failure of the SEALDD data transmission quality management request operation.

#### 7.2.16.2 SDDM server HTTP procedure

The SDDM-S sends a SEALDD data transmission quality management request when it needs to request to data transmission quality management towards an SDDM-C, the SDDM-S shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [21]. In the HTTP POST request message, the SDDM-S:

a) shall include a Request-URI set to the URI corresponding to the identity of the SDDM-C;

b) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [13]; and

c) shall include an application/vnd.3gpp.seal-data-delivery-info+xml MIME body with an <tx-quality-management-req> element in the <data-delivery-info> root element which:

1) shall include a <sealdd-flow-id> element set to the identity of the SDDM flow used by the SDDM-C and SDDM-S; and

2) shall include a <tx-quality-management-action> element set to 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 was triggered by an event (e.g. measurement threshold).

#### 7.2.16.3 SDDM client CoAP procedure

Upon receiving a CoAP POST request where the CoAP URI of the CoAP POST request identifies the establishment resource as specified in clause A.3.3.1, and containing:

a) a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-req-info+cbor"; and

b) a "TxQualityManagementRequest" object;

the SDDM-C shall generate a CoAP POST response according to IETF RFC 7252 [14]. In the CoAP POST response message, the SDDM-C:

a) shall include a Content-Format option set to "application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-res-info+cbor";

b) shall attempt to create the SDDM data transmission quality guarantee resource pointed at by the CoAP URI with the content of "TxQualityManagementResquest" object received in the request and:

1) if successfully created, shall include a "TxQualityManagementResponse" object in the CoAP POST 2.01 (Created) response message;

i) shall include a "result" attribute set to "success"; or

2) otherwise, shall include a "TxQualityManagementResponse" object with a "result" attribute set to "failure" and a "cause" attribute specifying the cause of the failure of the operation, e.g. VAL client error in the CoAP POST response; and

c) shall send the CoAP POST response towards the SDDM-S.

#### 7.2.16.4 SDDM server CoAP procedure

In order to request an SEALDD data transmission quality guarantee establishment to the SDDM-C, the SDDM-S shall send a CoAP POST request message to the SDDM-C according to procedures specified in IETF RFC 7252 [14]. In the CoAP POST request, the SDDM-S:

a) shall include a CoAP URI set to the URI corresponding to the identity of the SDDM-C as specified in clause A.3.3.1 with the "apiRoot" set to the SDDM-C URI;

b) shall include Content-Format option set to "application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-req-info+cbor";

c) shall include a "TxQualityManagementRequest" object:

1) shall include a "sealddFlowId" attribute set to the identity of the SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic; and

2) shall include a "txQualityManagementAction" attribute set to 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 was triggered by an event (e.g. measurement threshold); and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [7].

## 7.3 Off-network procedures

The off-network procedures are out of scope of the present document in this release of the specification.

# 8 Coding

## 8.1 General

This clause specifies the coding to enable an SDDM-C and an SDDM-S to communicate.

## 8.2 Application unique ID

The AUID shall be set to the VAL service ID as specified in specific VAL service specification.

## 8.3 Structure

The data delivery management document shall conform to the XML schema described in clause 8.4.

The <data-delivery-info> element shall be the root element of the SEALDataDeliveryManagement document.

The <establishment-req> element:

a) shall include a <requestor-id> element;

b) shall include a <sealdd-flow-id> element;

c) may include a <server-id> element;

d) may include a <endpoint-id> element;

e) may include a <VAL-service-id> element;

f) may include a <sealdd-communication-lifetime> element;

g) may include a <traffic-descriptor-info> element which shall include at least one of the following sub-elements:

1) a <user-plane-address> element;

2) a <port-number> element;

3) a <URL> element; or

4) a <transport-layer-protocol> element; and

h) may include an <identity> element.

The <identity> element shall include one of the following:

a) a <VAL-user-id> element may include a <VAL-client-id> element; or

b) a <VAL-ue-id> element.

The <establishment-rsp> element:

a) shall include a <result> element which may include a <cause> sub-element; and

b) may include a <traffic-descriptor-info> element which shall include at least one of the following sub-elements:

1) a <user-plane-address> element;

2) a <port-number> element;

3) a <URL> element; or

4) a <transport-layer-protocol> element; and

c) a <expiry-time> element; and

d) a <traffic-transmission-bandwidth> element.

The <release-req> element:

a) shall include either a <server-id> element or a <sealdd-client-identity> element; and

b) shall include a <sealdd-flow-id> element.

The <release-rsq> element:

a) shall include a <result> element which may include a <cause> sub-element.

The <URLLC-establishment-req> element:

a) shall include a <sealdd-client-identity> element;

b) shall include a <sealdd-flow-id> element;

c) may include a <identity> element;

d) may include a <server-id> element;

e) may include a <VAL-service-id> element;

f) may include a <traffic-descriptor-info> element which shall include at least one of the following sub-elements:

1) a <user-plane-address> element;

2) a <port-number> element;

3) a <URL> element; or

4) a <transport-layer-protocol> element.

The <identity> element shall include one of the following:

a) a <VAL-user-id> element may include a <VAL-client-id> element; or

b) a <VAL-ue-id> element.

The <URLLC-establishment-rsp> element:

a) shall include a <result> element which may include a <cause> sub-element; and

b) may include a <traffic-descriptor-info> element which shall include at least one of the following sub-elements:

1) a <user-plane-address> element;

2) a <port-number> element;

3) a <URL> element; or

4) a <transport-layer-protocol> element.

The <URLLC-release-req> element:

a) shall include a <sealdd-client-identity> element; and

b) shall include a <sealdd-flow-id> element.

The <URLLC-release-rsp> element:

a) shall include a <result> element which may include a <cause> sub-element.

The <URLLC-update-req> element:

a) shall include a <sealdd-client-identity> element;

b) shall include a <sealdd-flow-id> element;

c) may include a <server-id> element

d) may include a <VAL-service-id> element;

e) may include a <traffic-descriptor-info> element which shall include at least one of the following sub-elements:

1) a <user-plane-address> element;

2) a <port-number> element;

3) a <URL> element; or

4) a <transport-layer-protocol> element.

The <URLLC-update-rsp> element:

a) shall include a <result> element which may include a <cause> sub-element.

The <data-storage-creation-req> element:

a) shall include a <application-data> element;

b) may include a <access-control-policy> element;

c) may include a <expiry-time> element; and

d) may include a <status-information-req> element which shall include at least one of the following sub-elements:

1) a <no-times-data-accessed> element; and

2) a <no-times-data-managed> element.

The <data-storage-creation-rsp> element:

a) shall include a <result> element; and

b) may include a <data-identifier> element.

The <data-storage-reservation-req> element:

a) shall include a <VAL-service-id> element;

b) may include a <data-length> element.

The <data-storage-reservation-rsp> element:

a) shall include a <result> element; and

b) may include a <address> element.

The <data-storage-status-notification> element:

a) shall include a <data-identifier> element; and

b) shall include a <status-information-rsp> element which shall include at least one of the following sub-elements:

1) a <no-times-data-accessed-value> element; and

2) a <no-times-data-managed-value> element.

The <data-storage-query-req> element:

a) shall include a <data-identifier> element.

The <data-storage-query-rsp> element:

a) shall include a <result> element;

b) shall include a <data-identifier> element; and

c) may include a <application-data> element.

The <data-storage-mgt-req> element:

a) shall include a <data-identifier> element;

b) shall include a <operation> element ; and

c) may include a <application-data> element.

The <data-storage-mgt-rsp> element:

a) shall include a <result> element;

b) shall include a <data-identifier> element; and

c) may include a <application-data> element.

The <measurements-subscription-req> element:

a) shall include a <sealdd-flow-id> element;

b) shall include a <measurement-requirement-list> element which shall include at least one of the following sub-elements:

1) a <measurement-id> element;

2) a <reporting-frequency> element;

3) a <reporting-periodicity> element;

4) a <measurement-window> element;

5) a <expiry time > element;

6) a <sealdd-policy> element which shall include the following sub-elements:

i) a <quality-guarantee-policy> element; and

7) a <reporting-criteria> element; and

c) may include a <measurement-conditions> element.

The <measurements-subscription-rsp> element:

a) shall include a <result> element; and

b) may include a <expiry-time> element.

The <measurements-notification> element:

a) shall include a <measurement-requirement-notify-list> element which shall include at least one of the following sub-elements:

1) a <measurement-id> element;

2) an <identity-measurements> element;

3) a <average-measurement-value> element;

4) a <minimum-measurement-value> element;

5) a <maximum-measurement-value> element;

6) a <standard-deviation-measurement-value> element;

7) a <kpercentile-measurement-value> element:

8) a <measurement-period> element; and

9) a <timestamp> element.

The <identity-measurements> element shall include one of the following:

a) a <VAL-ue-id-list> element which shall include:

1) one or more <VAL-ue-id> elements: or

b) a <VAL-group-id> element.

The <tx-quality-management-req> element:

a) shall include a <sealdd-flow-id> element; and

b) shall include a <tx-quality-management-action> element.

The <tx-quality-management-rsp> element:

a) shall include a <result> element.

## 8.4 XML schema

### 8.4.1 General

This clause defines the XML schema for data delivery information.

### 8.4.2 XML schema

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="<http://www.w3.org/2001/XMLSchema>"

targetNamespace="urn:3gpp:ns:sealDataDeliveryInfo:1.0"

xmlns:sealdatadelivery="urn:3gpp:ns:sealDataDeliveryInfo:1.0"

elementFormDefault="qualified"

attributeFormDefault="unqualified"

xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<xs:annotation>

<xs:documentation>

3GPP - SDDM messages syntax based on 3GPP TS 24.543.

</xs:documentation>

</xs:annotation>

<xs:import namespace="http://www.w3.org/XML/1998/namespace"

schemaLocation="http://www.w3.org/2001/xml.xsd"/>

<!-- the root element which contains the SEALDD protocol messages -->

<xs:element name="data-delivery-info" id="DataDelivery">

<xs:complexType>

<xs:choice>

<xs:element name="establishment-req" type="sealdatadelivery:tEstablishmentReqType"/>

<xs:element name="establishment-rsp" type="sealdatadelivery:tEstablishmentRspType"/>

<xs:element name="release-req" type="sealdatadelivery:tReleaseReqType"/>

<xs:element name="release-rsp" type="sealdatadelivery:tReleaseRspType"/>

<xs:element name="URLLC-establishment-req" type="sealdatadelivery:tURLLCEstablishmentReqType"/>

<xs:element name="URLLC-establishment-rsp" type="sealdatadelivery:tURLLCEstablishmentRspType"/>

<xs:element name="URLLC-release-req" type="sealdatadelivery:tURLLCReleaseReqType"/>

<xs:element name="URLLC-release-rsp" type="sealdatadelivery:tURLLCReleaseRspType"/>

<xs:element name="URLLC-update-req" type="sealdatadelivery:tURLLCUpdateReqType"/>

<xs:element name="URLLC-update-rsp" type="sealdatadelivery:tURLLCUpdateRspType"/>

<xs:element name="data-storage-creation-req" type="sealdatadelivery:tDataStorageCreationReqType"/>

<xs:element name="data-storage-creation-rsp" type="sealdatadelivery:tDataStorageCreationRspType"/>

<xs:element name="data-storage-reservation-req" type="sealdatadelivery:tDataStorageReservationReqType"/>

<xs:element name="data-storage-reservation-rsp" type="sealdatadelivery:tDataStorageReservationRspType"/>

<xs:element name="data-storage-status-notification" type="sealdatadelivery:tDataStorageStatusNotificationType"/>

<xs:element name="data-storage-query-req" type="sealdatadelivery:tDataStorageQueryReqType"/>

<xs:element name="data-storage-query-rsp" type="sealdatadelivery:tDataStorageQueryRspType"/>

<xs:element name="data-storage-mgt-req" type="sealdatadelivery:tDataStorageMgtReqType"/>

<xs:element name="data-storage-mgt-rsp" type="sealdatadelivery:tDataStorageMgtRspType"/>

<xs:element name="measurements-subscription-req" type="sealdatadelivery:tMeasurementsSubscriptionReqType"/>

<xs:element name="measurements-subscription-rsp" type="sealdatadelivery:tMeasurementsSubscriptionRspType"/>

<xs:element name="measurements-notification" type="sealdatadelivery:tMeasurementsNotificationType"/>

<xs:element name="tx-quality-management-req" type="sealdatadelivery:tTxQualityManagementReqType"/>

<xs:element name="tx-quality-management-rsp" type="sealdatadelivery:tTxQualityManagementRspType"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs= "unbounded"/>

</xs:choice>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

</xs:element>

<xs:complexType name="tEstablishmentReqType">

<xs:sequence>

<xs:element name="requestor-id" type="sealdatadelivery:tRequestorIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="sealdd-flow-id" type="sealdatadelivery:tSealFlowIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="server-id" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="endpoint-id" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="VAL-service-id" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="sealdd-communication-lifetime" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="traffic-descriptor-info" type="sealdatadelivery:tTrafficDescriptorInfoType" minOccurs="0" maxOccurs="1"/>

<xs:element name="Identity" type="sealdatadelivery:tIdentityType" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="tRequestorIdType">

<xs:restriction base="xs:string">

<xs:enumeration value="sealddclient"/>

<xs:enumeration value="sealddserver"/>

</xs:restriction>

</xs:simpleType>

<xs:simpleType name="tSealFlowIdType">

<xs:restriction base="xs:positiveInteger">

<xs:minInclusive value="1"/>

<xs:maxInclusive value="65535"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tIdentityType">

<xs:choice>

<xs:element name="VAL-user-id" type="sealdatadelivery:contentType" minOccurs="0" maxOccurs="1"/>

<xs:element name="VAL-ue-id" type="xs:string" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:choice>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tTrafficDescriptorInfoType">

<xs:sequence>

<xs:element name="user-plane-address" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="port-number" type="sealdatadelivery:tPortNumberType" minOccurs="0" maxOccurs="1"/>

<xs:element name="URL" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="transport-layer-protocol" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs: sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="tPortNumberType">

<xs:restriction base="xs:positiveInteger">

<xs:minInclusive value="1"/>

<xs:maxInclusive value="65535"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tEstablishmentRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="traffic-descriptor-info" type="sealdatadelivery:tTrafficDescriptorInfoType" minOccurs="0" maxOccurs="1"/>

<xs:element name="expiry-time" type="xs:nonPositiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:element name="traffic-transmission-bandwidth" type="xs:positiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tResultType">

<xs:sequence>

<xs:element name="operation-result" type="sealdatadelivery:tOperationResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="cause" type="sealdatadelivery:tCauseType" minOccurs="0" maxOccurs="1"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="tOperationResultType">

<xs:restriction base="xs:string">

<xs:enumeration value="success"/>

<xs:enumeration value="failure"/>

</xs:restriction>

</xs:simpleType>

<xs:simpleType name="tCauseType">

<xs:restriction base="xs:string">

<xs:enumeration value="SEALDD policy mismatch"/>

<xs:enumeration value="VAL client error"/>

<xs:enumeration value="Other"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tReleaseReqType">

<xs:sequence>

<xs:element name="server-id" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="sealdd-client-identity" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="sealdd-flow-id" type="sealdatadelivery:tSealFlowIdType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tReleaseRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tResultType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tURLLCEstablishmentReqType">

<xs:sequence>

<xs:element name="sealdd-client-identity" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="sealdd-flow-id" type="sealdatadelivery:tSealFlowIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="identity" type="sealdatadelivery:tIdentityType" minOccurs="0" maxOccurs="1"/>

<xs:element name="server-id" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="VAL-service-id" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="traffic-descriptor-info" type="sealdatadelivery:tTrafficDescriptorInfoType" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="contentType">

<xs:choice>

<xs:element name="sealURI" type="xs:anyURI"/>

<xs:element name="sealString" type="xs:string"/>

<xs:element name="sealBoolean" type="xs:boolean"/>

<xs:any namespace="##other" processContents="lax"/>

</xs:choice>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tURLLCEstablishmentRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="traffic-descriptor-info" type="sealdatadelivery:tTrafficDescriptorInfoType" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tURLLCReleaseReqType">

<xs:sequence>

<xs:element name="sealdd-client-identity" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="sealdd-flow-id" type="sealdatadelivery:tSealFlowIdType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tURLLCReleaseRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tResultType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tURLLCUpdateReqType">

<xs:sequence>

<xs:element name="sealdd-client-identity" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="sealdd-flow-id" type="sealdatadelivery:tSealFlowIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="Identity" type="sealdatadelivery:tIdentityType" minOccurs="0" maxOccurs="1"/>

<xs:element name="server-id" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="VAL-service-id" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="traffic-descriptor-info" type="sealdatadelivery:tTrafficDescriptorInfoType" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tURLLCUpdateRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tResultType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tDataStorageCreationReqType">

<xs:sequence>

<xs:element name="application-data" type="xs:hexBinary" minOccurs="1" maxOccurs="1"/>

<xs:element name="access-control-policy" type="sealdatadelivery:tAccessControlPolicyType" minOccurs="0" maxOccurs="1"/>

<xs:element name="expiry-time" type="xs:nonPositiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:element name="status-information-req" type="sealdatadelivery:tStatusInformationReqType" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tStatusInformationReqType">

<xs:sequence>

<xs:element name="no-times-data-accessed" type="xs:boolean" minOccurs="0" maxOccurs="1"/>

<xs:element name="no-times-data-managed" type="xs:boolean" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="tAccessControlPolicyType">

<xs:restriction base="xs:string">

<xs:enumeration value="SDDM-C"/>

<xs:enumeration value="VAL-server"/>

<xs:enumeration value="SDDM-S"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tDataStorageCreationRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tOperationResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="data-identifier" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tDataStorageReservationReqType">

<xs:sequence>

<xs:element name="VAL-service-id" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="data-length" type="xs:positiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tDataStorageReservationRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tOperationResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="address" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tDataStorageStatusNotificationType">

<xs:sequence>

<xs:element name="data-identifier" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:element name="status-information-rsp" type="sealdatadelivery:tStatusInformationRspType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tStatusInformationRspType">

<xs:sequence>

<xs:element name="no-times-data-accessed-value" type="xs:unsignedInt" minOccurs="0" maxOccurs="1"/>

<xs:element name="no-times-data-managed-value" type="xs:unsignedInt" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tDataStorageQueryReqType">

<xs:sequence>

<xs:element name="data-identifier" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tDataStorageQueryRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tOperationResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="data-identifier" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="application-data" type="xs:hexBinary" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tDataStorageMgtReqType">

<xs:sequence>

<xs:element name="data-identifier" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="operation" type="sealdatadelivery:tOperationType" minOccurs="1" maxOccurs="1"/>

<xs:element name="application-data" type="xs:hexBinary" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="tOperationType">

<xs:restriction base="xs:string">

<xs:enumeration value="update"/>

<xs:enumeration value="refresh"/>

<xs:enumeration value="delete"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tDataStorageMgtRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tOperationResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="data-identifier" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:element name="application-data" type="xs:hexBinary" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tMeasurementsSubscriptionReqType">

<xs:sequence>

<xs:element name="sealdd-flow-id" type="sealdatadelivery:tSealFlowIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="measurement-requirement-list" type="sealdatadelivery:tMeasurementRequirementListType" minOccurs="1" maxOccurs="1"/>

<xs:element name="measurement-conditions" type="sealdatadelivery:tMeasurementConditionsType" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tMeasurementConditionsType">

<xs:sequence>

<xs:element name="temporal-conditions" type="sealdatadelivery:tTemporalConditionsType" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="spacial-conditions" type="sealdatadelivery:tSpatialConditionsType" minOccurs="0" maxOccurs="unbounded"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tTemporalConditionsType">

<xs:sequence>

<xs:element name="time-range" type="sealdatadelivery:rangeType" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="rangeType">

<xs:sequence>

<xs:element name="start-time" type="xs:dateTime" minOccurs="0"/>

<xs:element name="end-time" type="xs:dateTime" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="tSpatialConditionsType">

<xs:sequence>

<xs:element name="PolygonArea" type="sealdatadelivery:tPolygonAreaType" minOccurs="0"/>

<xs:element name="EllipsoidArcArea" type="sealdatadelivery:tEllipsoidArcType" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="protectionType">

<xs:restriction base="xs:string">

<xs:enumeration value="Normal"/>

<xs:enumeration value="Encrypted"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tPolygonAreaType">

<xs:sequence>

<xs:element name="Corner" type="sealdatadelivery:tPointCoordinateType" minOccurs="3" maxOccurs="15"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tEllipsoidArcType">

<xs:sequence>

<xs:element name="Center" type="sealdatadelivery:tPointCoordinateType"/>

<xs:element name="Radius" type="xs:nonNegativeInteger"/>

<xs:element name="OffsetAngle" type="xs:unsignedByte"/>

<xs:element name="IncludedAngle" type="xs:unsignedByte"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tPointCoordinateType">

<xs:sequence>

<xs:element name="longitude" type="sealdatadelivery:tCoordinateType"/>

<xs:element name="latitude" type="sealdatadelivery:tCoordinateType"/>

<xs:element name="altitude" type="sealdatadelivery:tCoordinateType" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tCoordinateType">

<xs:choice minOccurs="1" maxOccurs="1">

<xs:element name="threebytes" type="sealdatadelivery:tThreeByteType" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:choice>

<xs:attribute name="type" type="sealdatadelivery:protectionType"/>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="tThreeByteType">

<xs:restriction base="xs:integer">

<xs:minInclusive value="0"/>

<xs:maxInclusive value="16777215"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tMeasurementRequirementListType">

<xs:sequence maxOccurs="unbounded">

<xs:element name="measurement-requirement" type="sealdatadelivery:tMeasurementRequirementType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="tMeasurementRequirementType">

<xs:sequence>

<xs:element name="measurement-id" type="sealdatadelivery:tMeasurementIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="reporting-frequency" type="sealdatadelivery:tReportingFrequencyType" minOccurs="0" maxOccurs="1"/>

<xs:element name="reporting-periodicity" type="xs:unsignedInt" minOccurs="0" maxOccurs="1"/>

<xs:element name="measurement-window" type="xs:unsignedInt" minOccurs="0" maxOccurs="1"/>

<xs:element name="expiry-time" type="xs:nonPositiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:element name="sealdd-policy" type="sealdatadelivery:tSealddPolicyType" minOccurs="0" maxOccurs="1"/>

<xs:element name="reporting-criteria" type="sealdatadelivery:tReportingCriteriaType" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tSealddPolicyType">

<xs:sequence>

<xs:element name="quality-guarantee-event" type="sealdatadelivery:tQualityGuaranteeEventType" minOccurs="1" maxOccurs="1"/>

<xs:element name="quality-guarantee-action" type="xs:string" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:simpleType name="tReportingFrequencyType">

<xs:restriction base="xs:string">

<xs:enumeration value="periodic"/>

<xs:enumeration value="now"/>

</xs:restriction>

</xs:simpleType>

<xs:simpleType name="tMeasurementIdType">

<xs:restriction base="xs:string">

<xs:enumeration value="latency"/>

<xs:enumeration value="bitrate"/>

<xs:enumeration value="jitter"/>

<xs:enumeration value="packetloss"/>

</xs:restriction>

</xs:simpleType>

<xs:complexType name="tQualityGuaranteeEventType">

<xs:simpleContent>

<xs:extension base="xs:integer">

<xs:attribute name="TriggerEvent" type="xs:string" use="required"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>

<xs:complexType name="tReportingCriteriaType">

<xs:sequence>

<xs:element name="latency-threshold-value" type="xs:positiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:element name="above-or-below-latency-threshold-value" type="xs:boolean" minOccurs="0" maxOccurs="1"/>

<xs:element name="bitrate-threshold-value" type="xs:positiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:element name="above-or-below-bitrate-threshold-value" type="xs:boolean" minOccurs="0" maxOccurs="1"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tMeasurementsSubscriptionRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tOperationResultType" minOccurs="1" maxOccurs="1"/>

<xs:element name="expiry-time" type="xs:nonPositiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tMeasurementsNotificationType">

<xs:sequence>

<xs:element name="measurement-requirement-notify-list" type="sealdatadelivery:tMeasurementRequirementNotifyListType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tMeasurementRequirementNotifyListType">

<xs:sequence>

<xs:element name="measurement-id" type="sealdatadelivery:tMeasurementIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="identity-measurements" type="sealdatadelivery:tIdentityMeasurementsType" minOccurs="1" maxOccurs="1"/>

<xs:element name="average-measurement-value" type="xs:integer" minOccurs="0" maxOccurs="1"/>

<xs:element name="minimum-measurement-value" type="xs:integer" minOccurs="0" maxOccurs="1"/>

<xs:element name="maximum-measurement-value" type="xs:integer" minOccurs="0" maxOccurs="1"/>

<xs:element name="standard-deviation-measurement-value" type="xs:integer" minOccurs="0" maxOccurs="1"/>

<xs:element name="kpercentile-measurement-value" type="xs:integer" minOccurs="0" maxOccurs="1"/>

<xs:element name="measurement-period" type="xs:positiveInteger" minOccurs="0" maxOccurs="1"/>

<xs:element name="timestamp" type="xs:dateTime" minOccurs="0" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tIdentityMeasurementsType">

<xs:choice>

<xs:element name="VAL-ue-id-list" type="sealdatadelivery:tValUeIdListType" minOccurs="0"/>

<xs:element name="VAL-group-id" type="xs:string" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:choice>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tValUeIdListType">

<xs:choice>

<xs:element name="VAL-ue-id" type="xs:string" minOccurs="0"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:choice>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tTxQualityManagementReqType">

<xs:sequence>

<xs:element name="sealdd-flow-id" type="sealdatadelivery:tSealFlowIdType" minOccurs="1" maxOccurs="1"/>

<xs:element name="tx-quality-management-action" type="xs:string" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<xs:complexType name="tTxQualityManagementRspType">

<xs:sequence>

<xs:element name="result" type="sealdatadelivery:tOperationResultType" minOccurs="1" maxOccurs="1"/>

<xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

<xs:element name="anyExt" type="sealdatadelivery:anyExtType" minOccurs="0"/>

</xs:sequence>

<xs:anyAttribute namespace="##any" processContents="lax"/>

</xs:complexType>

<!-- XML attribute for any future extension -->

<xs:complexType name="anyExtType">

<xs:sequence>

<xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

</xs:sequence>

</xs:complexType>

</xs:schema>

## 8.5 Data semantics

The <data-delivery-info> element is the root element of the XML document. The <data-delivery-info> element contains the <establishment-req>, <establishment-rsp>, <release-req>, <release-rsp>, <URLLC-establishment-req>, <URLLC-establishment-rsq>, <URLCC-release-req>, <URLCC-release-rsp>, <URLLC-update-req>, <URLLC-update-rsp>, <data-storage-creation-req>, <data-storage-creation-rsp>, <data-storage-reservation-req>, <data-storage-reservation-rsp>, <data-storage-status-notification>, <measurements-subscription-req> , <measurements-subscription-rsp>, <data-storage-query-req>, <data-storage-query-rsp>, <data-storage-mgt-req>, <data-storage-mgt-rsp>, <measurements-notification>, <identity-measurements>, <tx-quality-management-req>, <tx-quality-management-rsp> sub-elements.

<establishment-req> element contains the following sub-elements:

a) <requestor-id>, a mandatory element. This element contains a string set to either "sealddclient" or "sealddserver" used to specify the identity of the requestor being either an SDDM-C or an SDDM-S.

b) <sealdd-flow-id>, a mandatory element specifying the identity of the seal flow.

c) <server-id>, an optional element specifying the VAL server.

d) <endpoint-id>, an optional element specifying the endpoint of a selected VAL server.

e) <sealdd-communication-lifetime>, an optional element specifying the data delivery communication lifetime.

f) <VAL-service-id>, an optional element specifying the VAL service identity of the vertical application.

g) <traffic-descriptor-info>, an optional element specifying the information of the traffic that contains one or more of the following sub-elements:

1) a <user-plane-address> element set to user plane IP address used for the traffic;

2) a <port-number> element set to the port number for the traffic;

3) a <URL> element set to a text format that specifies how to access the resource on the Internet for the traffic; or

4) a <transport-layer-protocol> element set to the transport protocol used for the traffic (e.g. TCP, UDP).

h) <identity>, an optional element set to the identity of the VAL user or the identity of the SDDM-C acting as the VAL UE and performing the request or the SDDM-S that performs the request.

<establishment-rsp> element contains the following sub-elements:

a) <result>, which includes a sub-element <operation-result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation. If the result is "failure", the <result> element may contain a <cause> sub-element set to the cause of the failure of the operation (e.g. SEALDD policy mismatch).

b) <traffic-descriptor-info>, an optional element specifying the information of the traffic that contains one or more of the following sub-elements:

1) a <user-plane-address> element set to user plane IP address used for the traffic;

2) a <port-number> element set to the port number for the traffic;

3) a <URL> element set to a text format that specifies how to access the resource on the Internet for the traffic; or

4) a <transport-layer-protocol> element set to the transport protocol used for the traffic (e.g. TCP, UDP); and

c) a <expiry-time> element set to a time in milliseconds that triggers the re-connection from either the SDDM-C or the SDDM-S when bandwidth limit check has failed; and

d) a <traffic-transmission-bandwidth> element set to the suggested traffic transmission bandwidth to be used by either the SDDM-C or the SDDM-S.

<identity> element contains one of following sub-elements:

a) <VAL-user-id> element specifying the identity of the VAL user; or

b) <VAL-UE-id> element specifying the identity of the VAL UE.

<release-req> element contains the following sub-elements:

a) <server-id>, an optional element specifying the endpoint of a selected VAL server;

b) <sealdd-client-identity>, an optional element specifying the identity of the SDDM-C; and

c) <sealdd-flow-id>, a mandatory element specifying the identity of the seal flow.

<release-rsp> element contains the following sub-elements:

a) <result>, which includes a sub-element <operation-result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation. If the result is "failure", the <result> element may contain a <cause> sub-element set to the cause of the failure of the operation.

<URLCC-establishment-req> element contains the following sub-elements:

a) <sealdd-client-identity>, a mandatory element specifying the identity of the SDDM-C.

b) <sealdd-flow-id>, a mandatory element specifying the identity of the seal flow.

c) <server-id>, an optional element specifying the endpoint of a selected VAL server.

d) <identity>, an optional set to the identity of the VAL user or the identity of the SDDM-C acting as the VAL UE and performing the request.

e) <VAL-service-id>, an optional element specifying the VAL service identity of the vertical application.

f) <traffic-descriptor-info>, an optional element specifying the information of the traffic that contains one or more of the following sub-elements:

1) a <user-plane-address> element set to user plane IP address used for the traffic;

2) a <port-number> element set to the port number for the traffic;

3) a <URL> element set to a text format that specifies how to access the resource on the Internet for the traffic; or

4) a <transport-layer-protocol> element set to the transport protocol used for the traffic (e.g. TCP, UDP).

<URLCC-establishment-rsp> element contains the following sub-elements:

a) <result>, which includes a sub-element <operation-result>,a mandatory element set to either "success" or "failure" indicating success or failure of the operation. If the result is "failure", the <result> element may contain a <cause> sub-element set to the cause of the failure of the operation (e.g. SEALDD policy mismatch).

b) <traffic-descriptor-info>, an optional element specifying the information of the traffic that contains one or more of the following sub-elements:

1) a <user-plane-address> element set to user plane IP address used for the traffic;

2) a <port-number> element set to the port number for the traffic;

3) a <URL> element set to a text format (URL) that specifies how to access the resource on the Internet for the traffic; or

4) a <transport-layer-protocol> element set to the transport protocol used for the traffic (e.g. TCP, UDP).

<URLCC-release-req> element contains the following sub-elements:

a) <sealdd-client-identity>, a mandatory element specifying the identity of the SDDM-C; and

c) <sealdd-flow-id>, a mandatory element specifying the identity of the seal flow.

<URLLC-release-rsp> element contains the following sub-elements:

a) <result>, which includes a sub-element <operation-result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation. If the result is "failure", the <result> element may contain a <cause> sub-element set to the cause of the failure of the operation.

<URLCC-update-req> element contains the following sub-elements:

a) <sealdd-client-identity>, a mandatory element specifying the identity of the SDDM-C.

b) <sealdd-flow-id>, a mandatory element specifying the identity of the seal flow.

c) <server-id>, an optional element specifying the endpoint of a selected VAL server.

d) <VAL-service-id>, an optional element specifying the VAL service identity of the vertical application.

e) <traffic-descriptor-info>, an optional element specifying the information of the traffic that contains one or more of the following sub-elements:

1) a <user-plane-address> element set to user plane IP address used for the traffic;

2) a <port-number> element set to the port number for the traffic;

3) a <URL> element set to a text format that specifies how to access the resource on the Internet for the traffic; or

4) a <transport-layer-protocol> element set to the transport protocol used for the traffic (e.g. TCP, UDP).

<URLCC-update-rsp> element contains the following sub-element:

a) <result>, which includes a sub-element <operation-result>,a mandatory element set to either "success" or "failure" indicating success or failure of the operation. If the result is "failure", the <result> element may contain a <cause> sub-element set to the cause of the failure of the operation (e.g. SEALDD policy mismatch).

<data-storage-creation-req> element contains the following sub-elements:

a) <application-data>, a mandatory element that provides the application data in hexadecimal to be;

b) <access-control-policy>, an optional element set to the control policy for the requested data access from other consumers (i.e.. SDDM-C, VAL-server, other SDDM-S);

c) <expiry-time>, an optional element set to the expiration time in minutes of the data to be stored; and

d) <status-information-req>, an optional element that contains one or more of the following sub-elements:

1) a <no-times-data-accessed> element that indicates whether information of how many times the stored data is accessed is requested for corresponding notifications; and

2) a <no-times-data-managed> element that indicates whether information of how many times the stored data is managed is requested for corresponding notifications.

<data-storage-creation-rsp> element contains the following sub-elements:

a) <result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation; and

b) <data-identifier>, an optional element set to the identity of the stored data.

<data-storage-reservation-req> element contains the following sub-elements:

a) <VAL-service-id>, a mandatory element set to the VAL service identity of the vertical application; and

b) <data-length>, an optional element set to the data length in bytes to be stored;

<data-storage-reservation-rsp> contains the following sub-elements:

a) <result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation; and

b) <address>, an optional element set to the reserved address for data storage.

<data-storage-status-notification> element contains the following sub-elements:

a) <data-identifier>, a mandatory element set to the identity of the stored data being notified; and

b) <status-information-rsp>, a mandatory element that contains one or more of the following sub-elements:

1) <no-times-data-accessed-value>, an optional element set to the value of how many times the stored data is accessed; and

2) <no-times-data-managed-value> an optional element set to the value of how many times the stored data is managed.

<data-storage-query-req> element contains the following sub-element:

a) <data-identifier>, a mandatory element set to the identity of the stored data which is requested to be queried.

<data-storage-query-rsp> contains the following sub-elements:

a) <result>, a mandatory element set to either set to "success" or "failure" indicating success or failure of the operation;

b) <dta-identifier>, a mandatory element set to the identity of the stored data which is queried; and

c) <application-data>, a mandatory element that provides the application data which is queried.

<data-storage-mgt-req> element contains the following sub-elements:

a) <data-identifier>, a mandatory element set to the identity of the stored data which is requested to be managed;

b) <operation>, a mandatory element set to the operation to be performed such as to "update", "refresh" or "delete" the stored data; and

c) <application-data>, an optional element that provides the application data in hexadecimal to be updated if the operation to be performed is to update the stored data.

<data-storage-mgt-rsp> element contains the following sub-elements:

a) <result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation;

b) <data-identifier>, a mandatory element set to the identity of the stored data which is managed; and

c) <application-data>, an optional element that provides the application data which is managed.

<measurements-subscription-req> element contains the following sub-elements:

a) <sealdd-flow-id>, a mandatory element specifying the identity of the seal flow;

b) <measurement-conditions>, an optional element specifying the temporal conditions, spatial conditions or both for the measurements; and

c) <measurement-requirement-list>, a mandatory element that contains one or more of the <measurement-requirement> element which each contain the following sub-elements:

1) <measurement-id>, a mandatory element set to measurement identifiers "latency", "bitrate", "jitter" or "packet loss";

2) <reporting-frequency>, an optional element set to reporting frequency of measurement results "periodic", "now". If not present, it implies periodic reporting;

3) <reporting-periodicity>, an optional element set to the reporting periodicity in seconds if the reporting frequency is periodic. This child element shall be included when the <reporting-frequency> element is set to "periodic" or not present;

4) <measurement-window>, an optional element set to the measurement period window in milliseconds for transmission quality measurements;

5) <expiry time >, an optional element set to the expiration time in milliseconds of the measurement identifier;

6) <sealdd-policy>, an optional element that contains the following sub-elements:

i) <quality-guarantee-policy>, a mandatory element set to the action to be performed "Redundant transmission path", "Re-establish transmission path", "Switch to backup transmission path" when the measurement event occurs, in order to meet the quality guarantee; and

7) <reporting-criteria>, an optional element set to the criteria for reporting measurement results that contains the following sub-elements:;

i) a <latency-threshold-value>, an optional element set to the latency threshold value for reporting measurements results in milliseconds;

ii) a <above-or-below-latency-threshold-value>, an optional element specifying whether the criterion for reporting measurements results is based on reaching above the latency value indicated by the <latency-threshold-value> element or not. Value "1" indicates that the criterion for reporting measurements results is based on reaching above the latency value indicated by the <latency-threshold-value> element. Value "0" indicates that the criterion for reporting measurements results is based on reaching below the latency value indicated by the <latency-threshold-value> element;

iii) a <bitrate-threshold-value> element set to the bitrate threshold value for reporting measurements results in Mbps; and

iv) a <above-or-below-bitrate-threshold-value>, an optional element specifying whether the criterion for reporting measurements results is based on reaching above the bitrate value indicated by the <bitrate-threshold-value> element or not. Value "1" indicates that the criterion for reporting measurements results is based on reaching above the bitrate value indicated by the <bitrate-threshold-value> element. Value "0" indicates that the criterion for reporting measurements results is based on reaching below the bitrate value indicated by the <bitrate-threshold-value> element.

<measurements-subscription-rsp> element contains the following sub-elements:

a) <result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation; and

b) <expiry-time>, an optional element set to the expiration time in milliseconds of the measurement requested.

<measurements-notification> element contains the following sub-elements:

a) <measurement-requirement-notify-list>, a mandatory element that contains one or more of the following sub-elements:

1) a <measurement-id> element set to measurement identifiers "latency", "bitrate", "jitter" or "packet loss";

2) an <identity-measurements> element set to the identity of the VAL UE(s) or VAL user(s) under SEALDD measurement;

3) an <average-measurement-value> element set to the average measurement value of measurement results ("latency" and "jitter" are in milliseconds, "bitrate" is in Mbps, "packet loss" is in percentage of the number of packets that fail to reach their destination);

4) a <minimum-measurement-value> element set to the minimum measurement value of measurement results ("latency" and "jitter" are in milliseconds, "bitrate", is in Mbps, "packet loss" is in percentage of the number of packets that fail to reach their destination);

5) a <maximum-measurement-value> element set to the maximum measurement value of measurement results ("latency" and "jitter" are in milliseconds, "bitrate", is in Mbps, "packet loss" is in percentage of the number of packets that fail to reach their destination);

6) a <standard-deviation-measurement-value> element set to standard deviation measurement value of measurement results;

7) a <kpercentile-measurement-value> element set to the kpercentile measurement value of measurement results:

8) a <measurement-period> element set to the measurement period in seconds; and

9) a <timestamp> element set to the timestamp in date and time of the measurement results with an offset from the UTC time.

<identity-measurements> element contains one of following sub-elements:

a) <VAL-ue-id-list>, an optional element that contains one or more <VAL-ue-id> elements. Each <VAL-ue-id> element contains the identity of the VAL UE for whom SEALDD measurement applies. For multiple VAL UEs reporting granularity set to individual UE, the associated measurement values are for individual VAL UE; or

b) <VAL-group-id>, an optional element specifying the identity of the VAL group for whom SEALDD measurement applies for which the associated measurement values are aggregation for all VAL UEs or the VAL UE group.

<tx-quality-management-req> element contains the following sub-elements:

a) <sealdd-flow-id>, a mandatory element specifying the identity of the seal flow; and

b) <tx-quality-guarantee-action>, a mandatory element set to the data transmission quality "Redundant transmission path", "Re-establish transmission path", "Switch to backup transmission path" or "Back to single transmission path" that was triggered by an event (e.g. measurement threshold).

NOTE: The strings allowed in <tx-quality-guarantee-action> are case sensitive.

<tx-quality-management-rsp> element contains the following sub-element:

a) <result>, a mandatory element set to either "success" or "failure" indicating success or failure of the operation.

## 8.6 MIME type

The MIME type for the DataDeliveryInfo document shall be "application/vnd.3gpp.seal-data-delivery-info+xml".

Editor’s note: The MIME type needs to be registered after the approval of the TS.

## 8.7 IANA registration template

Your Name:

<TS rapporteur name>

Your Email Address:

<TS rapporteur email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.seal-data-delivery-info+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in HTTP. Hence, the security considerations from IETF RFC 2616 apply while exchanging information in HTTP.

The information transported in this media type does not include active or executable content.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL)", available via https://www.3gpp.org/ftp/Specs/archive/24\_series/24.543.

Applications which use this media type:

Applications supporting the SEAL Data delivery management as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none

2. Magic number(s): none

3. File extension(s): none

4. Macintosh File Type Code(s): none

5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>

- Email: <MCC email address>

- Author/Change controller:

i) Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

ii) Change controller: <MCC name>/<MCC email address>

Annex A (normative):  
CoAP resource representation and encoding

# A.1 General

The information in this annex provides a normative description of CoAP resource representation and encoding.

The general rules for resource URI structure, cache usage, error handling, and common data types are described in clause C.1 of 3GPP TS 24.546 [6].

# A.2 Data types applicable to multiple resource representations

## A.2.1 General

This clause defines structured data types, simple data types, and enumerations that are applicable to several APIs defined for CoAP resource representations in the present specification.

## A.2.2 Referenced structured data types

Table A.2.2.1 lists structured data types referenced by multiple CoAP resource representations and defined in other specifications.

Table A.2.2.1: Referenced structured data types

|  |  |  |
| --- | --- | --- |
| Data type | Reference | Description |
| ValTargetUe | 3GPP TS 24.546 [6] | Information identifying a VAL user ID or VAL UE ID. |
| GeographicalCoordinates | 3GPP TS 24.546 [6] | Information identifying geographical coordinates. |
| GeographicArea | 3GPP TS 24.546 [6] | Information identifying a geographical area. |

## A.2.3 Referenced simple data types

Table A.2.3.1 lists simple datatypes referenced by multiple CoAP resource representations and defined in other specifications.

Table A.2.3.1: Referenced simple data types

|  |  |  |
| --- | --- | --- |
| Type name | Reference | Description |
| Uinteger | 3GPP TS 24.546 [6] | Unsigned integer, i.e. only value 0 and values above 0 are permissible. |
| TimeOfDay | 3GPP TS 24.546 [6] | String with format partial-time or full-time as defined in clause 5.6 of IETF RFC 3339 [11]. |
| DateTime | 3GPP TS 24.546 [6] | String in the standard format described by the "date-time" production in IETF RFC3339 [11]. |

## A.2.4 Common structured data types

### A.2.4.1 Type: EstablishmentResponse

Table A.2.4.1.1: Definition of type EstablishmentResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| result | ResultOp | M | 1 | Result of the establishment request. |  |
| cause | Cause | O | 0..1 | Reason of the cause of the failure of the establishment request (NOTE 1). |  |
| userPlaneAddress | string | O | 0..1 | Identity of the IP address of the traffic (NOTE 2). |  |
| portNumber | Uinteger | O | 0..1 | Identity of the port number of the traffic (NOTE 2). |  |
| url | string | O | 0..1 | Identity of the address of a given unique resource on the Web for the traffic (NOTE 2). |  |
| transportLayer | string | O | 0..1 | Identity of the transport layer protocol for the traffic (NOTE 2). |  |
| NOTE 1: This attribute shall be included if result is set to "FAILURE".  NOTE 2: This attribute may be included if result is set to "SUCCESS". | | | | | |

## A.2.5 Common simple data types

Table A.2.5.1: Simple data types applicable to multiple CoAP resource representations

|  |  |
| --- | --- |
| Type name | Description |
| ServerId | String representing a unique identifier of a VAL server. |

## A.2.6 Common enumerations

### A.2.6.1 Enumeration: RequestorId

Table A.2.6.1.1: RequestorId

|  |  |  |
| --- | --- | --- |
| Enumeration value | Description | Applicability |
| SEALDDCLIENT | SEALDD client is the requestor. |  |
| SEALDDSERVER | SEALDD server is the requestor. |  |

### A.2.6.2 Enumeration: ResultOp

Table A.2.6.2.1: ResultOp

|  |  |  |
| --- | --- | --- |
| Enumeration value | Description | Applicability |
| SUCCESS | Success of the operation. |  |
| FAILURE | Failure of the operation. |  |

### A.2.6.3 Enumeration: Cause

Table A.2.6.3.1: Cause

|  |  |  |
| --- | --- | --- |
| Enumeration value | Description | Applicability |
| VAL CLIENT ERROR | A VAL client error occurs. |  |
| SEALDD POLICY MISMATCH | A SEALDD policy mismatch occurs. |  |
| OTHER | Any other cause occurs than the ones defined in this table. |  |

# A.3 Resource representation and APIs provided by SDDM-S

## A.3.1 Sdd\_RegularTransmissionConnection API

### A.3.1.1 API URI

The CoAP URIs used in CoAP requests from SDDM-S towards the SDMM-C shall have the Resource URI structure as defined in clause C.1.1 of 3GPP TS 24.546 [6] with the following clarifications:

a) the <apiName> shall be "sdd-rtc-s";

b) the <apiVersion> shall be "v1"; and

c) the <apiSpecificSuffixes> shall be set as described in clause A.3.1.2.

### A.3.1.2 Resources

#### A.3.1.2.1 Overview



Figure A.3.1.2.1.1: Resource URI structure of the Sdd\_RegularTransmissionConnection API provided by SDDM-S

Table A.3.1.2.1.1 provides an overview of the resources and applicable CoAP methods.

Table A.3.1.2.1.1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name | Resource URI | CoAP method | Description |
| SDD Regular Transmission Connection | val-services/{valServiceId}/sdd-regular-transmission-connection | POST | Establish anSDDM regular transmission connection. |
| DELETE | Release anSDDM regular transmission connection |

#### A.3.1.2.2 Resource: SDD Regular Transmission Connection

##### A.3.1.2.2.1 Description

The SDD regular transmission connection resource represents an SDD regular transmission connection to be created at a given SDDM-S and SDDM-C.

##### A.3.1.2.2.2 Resource Definition

Resource URI: **{apiRoot}/sdd-rtc-s/<apiVersion>/val-services/{valServiceId}/sdd-regular-transmission-connection**

This resource shall support the resource URI variables defined in the table A.3.1.2.2.2.1.

Table A.3.1.2.2.2.1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Definition |
| apiRoot | string | See clause C.1.1 of 3GPP TS 24.546 [6]. |
| apiVersion | string | See clause A.3.1.1. |
| valServiceId | string | Identifier of a VAL service. |

##### A.3.1.2.2.3 Resource Standard Methods

A.3.1.2.2.3.1 POST

This operation allows to establish an SDDM regular transmission connection.

This method shall support the request data structures the data structures, request codes and response codes specified in table A.3.1.2.2.3.1.1 and A.3.1.2.2.3.1.2.

Table A.3.1.2.2.3.1.1: Data structures supported by the POST Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| EstablishmentRequest | M | 1 | The information of request of establishment of an SDDM regular transmission connection. |

Table A.3.1.2.2.3.1.2: Data structures supported by the POST Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| EstablishmentResponse | M | 1 | 2.01 Created | SDDM regular transmission connection created successfully. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [31] shall also apply. | | | | |

A.3.1.2.2.3.2 DELETE

This operation releases an SDDM regular transmission connection.

This method shall support the request data structures the data structure, request codes and response codes specified in table A.3.1.2.2.3.2.1 and A.3.1.2.2.3.2.2.

Table A.3.1.2.2.3.2.1: Data structures supported by the DELETE Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| ReleaseRequest | M | 1 | The information of request of release of an SDDM regular transmission connection. |

Table A.3.1.2.2.3.2.2: Data structures supported by the DELETE Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.02 Deleted | SDDM regular transmission connection released successfully. |
| NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 of 3GPP TS 24.546 [31] shall also apply. | | | | |

### A.3.1.3 Data Model

#### A.3.1.3.1 General

Table A.3.1.3.1.1 specifies the data types defined specifically for the SDD\_RegularTransmissionConnection API service provided by SDDM-S.

Table A.3.1.3.1.1: SDD\_RegularTransmissionConnection API provided by SDDM-S specific data types

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Data type | | Section defined | | Description | | Applicability | |
| ValTargetUe | | A.2.2 | | Information identifying a VAL user ID or VAL UE ID. | |  | |
| EstablishmentResponse | | A.2.4.1 | | Information identifying an SDD regular transmission connection establishment response. | |  | |
| EstablishmentRequest | | A.3.1.3.2.1 | | Information identifying an SDD regular transmission connection establishment request. | |  | |
| ReleaseRequest | | A.3.1.3.2.3 | | Information identifying an SDD regular transmission connection release request. | |  | |

Table A.3.1.3.1.2 specifies the simple data types defined specifically for the SDD\_RegularTransmissionConnection API service provided by SDDM-S.

Table A.3.1.3.1.2: SDD\_RegularTransmissionConnection API provided by SDDM-S specific simple data types

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| Uinteger | A.2.3 | Unsigned integer. |
| ServerId | A.2.5 | String representing a unique identifier of a VAL server. |

Table A.3.1.3.1.3 specifies the enumerations defined specifically for the SDD\_RegularTransmissionConnection API service provided by SDDM-S.

Table A.3.1.3.1.3: SDD\_RegularTransmissionConnection API provided by SDDM-S specific enumeration

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| RequestorId | A.2.6.1 | Information identifying a VAL user ID or VAL UE ID. |
| ResultOp | A.2.6.2 | Information identifying the result of an operation. |
| Cause | A.2.6.3 | Information identifying the reason of the cause of the failure of an operation. |

#### A.3.1.3.2 Structured data types

##### A.3.1.3.2.1 Type: EstablishmentRequest

Table A.3.1.3.2.1.1: Definition of type EstablishmentRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| requestorId | RequestorId | M | 1 | Identity of the requestor of the establishment request (NOTE). |  |
| sealflowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |
| endpointId | string | M | 1 | Identity of the endpoint of the selected VAL server to which the establishment request has to be sent. |  |
| sealddCommunicationLifetime | string | O | 1 | Information of the data delivery communication lifetime. |  |
| valServiceId | string | O | 0..1 | Identity of the VAL service enabled by the SDD regular transmission connection. |  |
| userPlaneAddress | string | O | 0..1 | Identity of the IP address of the traffic. |  |
| portNumber | Uinteger | O | 0..1 | Identity of the port number of the traffic. |  |
| url | string | O | 0..1 | Identity of the address of a given unique resource on the Web for the traffic. |  |
| transportLayer | string | O | 0..1 | Identity of the transport layer protocol for the traffic. |  |
| valTgtUe | ValTargetUe | O | 0..1 | VAL user to whom the establishment request is applied. |  |
| NOTE: This attribute shall be set to "SEALDDSERVER". | | | | | |

##### A.3.1.3.2.2 Type: ReleaseRequest

Table A.3.1.3.2.2.1: Definition of type ReleaseRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| serverId | string | M | 1 | Identity of the VAL server. |  |
| sealflowId | number | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |

#### A.3.1.3.3 Simple data types and enumerations

None.

### A.3.1.4 Error Handling

General error responses are defined in clause C.1.3 of 3GPP TS 24.546 [6].

### A.3.1.5 CDDL Specification

#### A.3.1.5.1 Introduction

The data model described in clause A.3.1.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [20].

Clause A.3.1.5.2 uses the concise data definition language described in IETF RFC 8610 [19] and provides corresponding representation of the SDD\_RegularTransmissionConnection API provided by the SDDM-S data model.

#### A.3.1.5.2 CDDL document

Editor’s note: The CDDL document is FFS.

### A.3.1.6 Media Types

The media type for a request to establish an SDDM regular transmission connection shall be "application/vnd.3gpp.seal-data-delivery-establishment-req-info+cbor".

The media type for a response of establishing an SDDM regular transmission connection shall be "application/vnd.3gpp.seal-data-delivery-establishment-res-info+cbor".

The media type for a request to release an SDDM regular transmission connection shall be "application/vnd.3gpp.seal-data-delivery-release-req-info +cbor".

Editor’s note: The MIME types need to be registered after the approval of the TS.

### A.3.1.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-establishment-req-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-establishment-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "EstablishmentRequest" data type in 3GPP TS 24.543 clause A.3.1.3.2.1 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.3.1.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-establishment-res-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-establishment-res-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "EstablishmentResponse" data type in 3GPP TS 24.543 clause A.3.1.3.2.2 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.3.1.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-release-req-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-release-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "ReleaseRequest" data type in 3GPP TS 24.543 clause A.3.1.3.2.2 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

## A.3.2 Sdd\_TransmissionQualityMeasurement API

### A.3.2.1 API URI

The CoAP URIs used in CoAP requests from SDDM-S towards the SDMM-C shall have the Resource URI structure as defined in clause C.1.1 of 3GPP TS 24.546 [6] with the following clarifications:

a) the <apiName> shall be "sdd-rtc-s";

b) the <apiVersion> shall be "v1"; and

c) the <apiSpecificSuffixes> shall be set as described in clause A.3.2.2.

### A.3.2.2 Resources

#### A.3.2.2.1 Overview



Figure A.3.2.2.1.1: Resource URI structure of the Sdd\_TransmissionQualityMeasurement API provided by SDDM-S

Table A.3.2.2.1.1 provides an overview of the resources and applicable CoAP methods.

Table A.3.2.2.1.1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name | Resource URI | CoAP method | Description |
| SDD Transmission Quality Measurement | val-services/{valServiceId}/sdd-transmission-quality-measurement | POST | Establish an SDDM data transmission quality measurement. |
| PUT | Report SDDM data transmission quality measurement of the SDDM-C. |
| DELETE | Releases an SDDM data transmission quality measurement. |

#### A.3.2.2.2 Resource: SDD Transmission Quality Measurement

##### A.3.2.2.2.1 Description

The SDD transmission quality measurement resource allows an SDDM-C to manage an SDDM data transmission quality measurement of an SDDM-S.

##### A.3.2.2.2.2 Resource Definition

Resource URI: **{apiRoot}/sdd-rtc-s/<apiVersion>/val-services/{valServiceId}/sdd--transmission-quality-measurement**

This resource shall support the resource URI variables defined in the table A.3.2.2.2.2.1.

Table A.3.2.2.2.2.1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Definition |
| apiRoot | string | See clause C.1.1 of 3GPP TS 24.546 [6]. |
| apiVersion | string | See clause A.3.2.1. |
| valServiceId | string | Identifier of a VAL service. |

##### A.3.2.2.2.3 Resource Standard Methods

###### A.3.2.2.2.3.1 POST

This operation allows to establish an SDDM data transmission quality measurement.

This method shall support the request data structures the data structures, request codes and response codes specified in table A.3.2.2.2.3.1.1 and A.3.2.2.2.3.1.2.

Table A.3.2.2.2.3.1.1: Data structures supported by the POST Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| MeasurementsSubscriptionResquest | M | 1 | The information of request of establishment of an SDDM data transmission quality measurement. |

Table A.3.2.2.2.3.1.2: Data structures supported by the POST Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| MeasurementsSubscriptionResponse | M | 1 | 2.01 Created | SDDM data transmission quality measurement created successfully. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

###### A.3.2.2.2.3.2 PUT

This operation updates an SDDM data transmission quality measurement.

This method shall support the data structures, request codes and response codes specified in table A.3.2.2.2.3.2.1 and A.3.2.2.2.3.2.2.

Table A.3.2.2.2.3.2.1: Data structures supported by the PUT Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| DataStorageMgtRequest | M | 1 | The information of request of update an SDDM datatransmission quality measurement. |

Table A.3.2.2.2.3.2.1: Data structures supported by the PUT Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.04 Changed | SDDM data transmission quality measurement updated successfully. |
| NOTE: The mandatory CoAP error status codes for the PUT method listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

###### A.3.2.2.2.3.3 DELETE

This operation releases an SDDM data transmission quality measurement.

This method shall support the request data structures the data structure, request codes and response codes specified in table A.3.2.2.2.3.3.1 and A.3.2.2.2.3.3.2.

Table A.3.2.2.2.3.3.1: Data structures supported by the DELETE Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| n/a |  |  | The information of request of release of an SDDM data transmission quality measurement. |

Table A.3.2.2.2.3.3.2: Data structures supported by the DELETE Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.02 Deleted | SDDM data transmission quality measurement released successfully. |
| NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

### A.3.2.3 Data Model

#### A.3.2.3.1 General

Table A.3.2.3.1.1 specifies the data types defined specifically for the SDD\_TransmissionQualityMeasurement API service provided by SDDM-S.

Table A.3.2.3.1.1: SDD\_TransmissionQualityMeasurement API provided by SDDM-S specific data types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Section defined | Description | Applicability |
| ValTargetUe | A.2.2 | Information identifying a VAL user ID or VAL UE ID. |  |
| GeographicArea | A.2.2 | Information identifying a geographical area. |  |
| GeographicalCoordinates | A.2.2 | Information identifying geographical coordinates. |  |
| MeasurementsSubscriptionRequest | A.3.2.3.2.1 | Information identifying an SDD data transmission quality measurement subscription establishment request. |  |
| MeasurementsSubscriptionResponse | A.3.2.3.2.2 | Information identifying an SDD data transmission quality measurement subscription establishment response. |  |
| MeasurementsNotification | A.3.2.3.2.3 | Information identifying an SDD data transmission quality measurement notification. |  |
| ReportingCriteria | A.3.2.3.2.4 | Information of the criteria for reporting measurement results. |  |
| MeasurementPeriod | A.3.2.3.2.5 | Information of the measurement period. |  |
| SpatialConditions | A.3.2.3.2.6 | Information of the spatial conditions. |  |

Table A.3.2.3.1.2 specifies the simple data types defined specifically for the SDD\_TransmissionQualityMeasurement API service provided by SDDM-S.

Table A.3.2.3.1.2: SDD\_TransmissionQualityMeasurement API provided by SDDM-S specific simple data types

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| Uinteger | A.2.3 | Unsigned integer. |

Table A.3.2.3.1.3 specifies the enumerations defined specifically for the SDD\_TransmissionQualityMeasurement API service provided by SDDM-S.

Table A.3.2.3.1.3: SDD\_TransmissionQualityMeasurement API provided by SDDM-S specific enumeration

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| ResultOp | A.2.6.2 | Information identifying the result of an operation. |
| Cause | A.2.6.3 | Information identifying the reason of the cause of the failure of an operation. |

#### A.3.2.3.2 Structured data types

##### A.3.2.3.2.1 Type: MeasurementsSubscriptionRequest

Table A.3.2.3.2.2.1: Definition of type MeasurementsSubscriptionRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| sealFlowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |
| measurementId | string | M | 1 | Identity of the measurement to be performed which is set to "LATENCY", "BITRATE", "JITTER" or "PACKET LOSS". |  |
| reportingFrequency | string | O | 0..1 | Information of the reporting frequency of measurement results which is set to "PERIODIC" or "NOW". |  |
| reportingPeriodicity | Uinteger | O | 0..1 | Identity of the reporting periodicity of measurement results in seconds (NOTE). |  |
| measurementWindow | Uinteger | O | 0..1 | Identity of the measurement period window for transmission quality measurements in milliseconds. |  |
| expiryTimer | Uinteger | O | 0..1 | Identity of the expiration time of the measurement in milliseconds. |  |
| sealPolicy | string | O | 0..1 | Information of the quality guarantee policies associated with the SEALDD connection set to the action to be performed "REDUNDANT TRANSMISSION PATH", "RE-ESTABLISH TRANSMISSION PATH", "SWITCH TO BACKUP TRANSMISSION PATH" when the measurement event occurs. |  |
| reportingCriteria | array(ReportingCriteria) | O | 0..N | Information of 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 criterion of more than one criteria is specified. |  |
| measurementConditions | MeasurementConditions | O | 0..1 | Information of the temporal conditions, spatial conditions or both. |  |
| valTgtUe | ValTargetUe | O | 0..1 | VAL user to whom the subscription request is applied. |  |
| NOTE: This attribute shall be included if reportingFrequency is set to "PERIODIC". | | | | | |

##### A.3.2.3.2.2 Type: MeasurementsSubscriptionResponse

Table A.3.2.3.2.2.1: Definition of type MeasurementsSubscriptionResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| result | ResultOp | M | 1 | Result of the establishment request. |  |
| cause | Cause | O | 0..1 | Reason of the cause of the failure of the establishment request (NOTE 1). |  |
| expiryTime | DateTime | O | 0..1 | Information of the expiration time of the subscription (NOTE 2). |  |
| NOTE 1: This attribute shall be included if result is set to "FAILURE".  NOTE 2: This attribute may be included if result is set to "SUCCESS". | | | | | |

##### A.3.2.3.2.3 Type: MeasurementsNotification

Table A.3.2.3.2.3.1: Definition of type MeasurementsNotification

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| sealFlowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |
| measurementId | string | M | 1 | Identity of the measurement performed which is set to "LATENCY", "BITRATE", "JITTER" or "PACKET LOSS". |  |
| valUeIdList | array(ValTargetUe) | O | 0..N | Information of the identities of the VAL UEs or VAL users for whom SEALDD measurement applies. This attribute can be omitted and the associated measurement values are for the single VAL UE (NOTE). |  |
| averageMeasurementValue | Uinteger | O | 0..1 | Information of average measurement value of measurement results. If measurementId is "LATENCY" or "JITTER", the value is in milliseconds. If measurementId is "BITRATE", the value is in Mbps. If the measurementId is "PACKET LOSS", the value is in percentage of the number of packets that fail to reach their destination. |  |
| maximumMeasurementValue | Uinteger | O | 0..1 | Information of the maximum measurement value of measurement results. If measurementId is "LATENCY" or "JITTER", the value is in milliseconds. If measurementId is "BITRATE", the value is in Mbps. If the measurementId is "PACKET LOSS", the value is in percentage of the number of packets that fail to reach their destination. |  |
| minimumMeasurementValue | Uinteger | O | 0..1 | Information of the minimum measurement value of measurement results. If measurementId is "LATENCY" or "JITTER", the value is in milliseconds. If measurementId is "BITRATE", the value is in Mbps. If the measurementId is "PACKET LOSS", the value is in percentage of the number of packets that fail to reach their destination. |  |
| standardDeviationMeasurementValue | Uinteger | O | 0..1 | Information of the standard deviation measurement value of measurement results. |  |
| kPercentileMeasurementValue | Uinteger | O | 0..1 | Information of the kpercentile measurement value of measurement results. |  |
| measurementPeriod | MeasurementPeriod | O | 0..1 | Information of the measurement period. |  |
| timeStamp | TimeOfDay | O | 0..1 | Information of the timestamp of measurement results. |  |
| NOTE: This attribute can be omitted and the associated measurement values are for the single VAL UE. | | | | | |

##### A.3.2.3.2.4 Type: ReportingCriteria

Table A.3.2.3.2.4.1: Definition of type ReportingCriteria

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| latency | LatencyValue | O | 0..1 | Identify whether the criterion for reporting measurements results is based on reaching above or below certain latency values (NOTE). |  |
| bitrate | BitrateValue | O | 0..1 | Identify whether the criterion for reporting measurements results is based on reaching above or below certain bitrate value (NOTE). |  |
| NOTE: At least one of these attributes shall be included. | | | | | |

##### A.3.2.3.2.5 Type: LatencyValue

Table A.3.2.3.2.5.1: Definition of type LatencyValue

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| latencyThresholdValue | Uinteger | M | 1 | Information of the latency threshold value for reporting measurements results in milliseconds. |  |
| aboveOrBelow | boolean | M | 1 | Identify whether the criterion for reporting measurements results is based on reaching above certain latency value. Value "true" indicates that the criterion for reporting measurements results is based on reaching above the latency value indicated by the latencyThresholdValue attribute. Value "false" indicates that the criterion for reporting measurements results is based on reaching below the latency value indicated by the latencyThresholdValue attribute. |  |

##### A.3.2.3.2.6 Type: BitrateValue

Table A.3.2.3.2.6.1: Definition of type BitrateValue

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| bitrateThresholdValue | Uinteger | M | 1 | Information of the bitrate threshold value for reporting measurements results in Mbps. |  |
| aboveOrBelow | boolean | M | 1 | Identify whether the criterion for reporting measurements results is based on reaching above certain bitrate value. Value "true" indicates that the criterion for reporting measurements results is based on reaching above the bitrate value indicated by the bitrateThresholdValue attribute. Value "false" indicates that the criterion for reporting measurements results is based on reaching below the bitrate value indicated by the bitrateThresholdValue attribute. |  |

##### A.3.2.3.2.7 Type: MeasurementConditions

Table A.3.2.3.2.7.1: Definition of type MeasurementConditions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| temporalConditions | MeasurementPeriod | O | 0..1 | Information of the temporal conditions set in time range (i.e. time-of-start and time-of-end) (NOTE). |  |
| spatialConditions | SpatialConditions | O | 0..1 | Information of the spatial conditions (i.e. geographical area, geographical coordinates or both) (NOTE). |  |
| NOTE: At least one of these attributes shall be included. | | | | | |

##### A.3.2.3.2.8 Type: MeasurementPeriod

Table A.3.2.3.2.8.1: Definition of type MeasurementPeriod

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| timeStart | TimeOfDay | M | 1 | Information of the start of measurement period. |  |
| timeEnd | TimeOfDay | M | 1 | Information of the end of measurement period. |  |

##### A.3.2.3.2.9 Type: SpatialConditions

Table A.3.2.3.2.9.1: Definition of type SpatialConditions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| geographicAreaList | array(GeographicArea) | O | 0..N | Information of specific geographical area list (NOTE). |  |
| geoCoordinatesList | array(GeographicalCoordinates) | O | 0..N | Information of specific geographical coordinates (NOTE). |  |
| NOTE: At least one of these attributes shall be included. | | | | | |

#### A.3.2.3.3 Simple data types and enumerations

None.

### A.3.2.4 Error Handling

General error responses are defined in clause C.1.3 of 3GPP TS 24.546 [6].

### A.3.2.5 CDDL Specification

#### A.3.2.5.1 Introduction

The data model described in clause A.3.1.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [20].

Clause A.3.2.5.2 uses the concise data definition language described in IETF RFC 8610 [19] and provides corresponding representation of the SDD\_TransmissionQualityMeasurement API provided by the SDDM-S data model.

#### A.3.2.5.2 CDDL document

;;; MeasurementSubscriptionRequest

;;+ Represents a request for performing SDDM data transmission quality measurements.

MeasurementSubscriptionRequest = {

sealFlowId: Uinteger

measurementId: string

? reportingFrequency: string

? reportingPeriodicity: Uinteger

? measurementWindow: Uinteger

? expiryTimer: Uinteger

? sealPolicy: string

? reportingCriteria: ReportingCriteria

? measurementConditions: MeasurementConditions

? valTgtUe: ValTargetUe

}

;;; MeasurementSubscriptionResponse

;;+ Represents the response of a request for performing SDDM data transmission quality measurements.

MeasurementSubscriptionResponse = {

result: ResultOp

? cause: Cause

? expiryTime: DateTime

}

;;; MeasurementSubscriptionNotification

;;+ Represents the information of SDDM data transmission quality measurements of the SDDM-C.

MeasurementSubscriptionNotification = {

sealFlowId: Uinteger

measurementId: string

? valUeIdList: [\* ValTargetUe]

? averageMeasurementValue: Uinteger

? maximumMeasurementValue: Uinteger

? minimumMeasurementValue: Uinteger

? standardDeviationMeasurementValue: Uinteger

? kPercentileMeasurementValue: Uinteger

? measurementPeriod: MeasurementPeriod

? timeStamp: TimeOfDay

}

;;; ReportingCriteria

ReportingCriteria = {

? latency: LatencyValue

? bitrate: BitrateValue

}

;;; LatencyValue

LatencyValue = {

latencyThresholdValue: Uinteger

aboveOrBelow: bool

}

;;; BitrateValue

BitrateValue = {

bitrateThresholdValue: Uinteger

aboveOrBelow: bool

}

;;; MeasurementConditions

MeasurementConditions = {

? temporalConditions: MeasurementPeriod

? spatialConditions: SpatialConditions

}

MeasurementPeriod = {

timeStart: TimeOfDay

timeEnd: TimeOfDay

}

;;; SpatialConditons

SpatialConditions = {

? geographicAreaList: [\* GeographicArea]

? geoCordinatesList: [\*GeographicalCoordinates]

}

;;; TimeOfDay

;;+ String with format partial-time or full-time as defined in clause 5.6 of IETF RFC 3339. Examples, 20:15:00, 20:15:00-08:00 (for 8 hours behind UTC).

TimeOfDay = text

;;; ValTargetUe

;;+ Represents information identifying a VAL user ID or a VAL UE ID.

valUserId = {

valUserId: text ; Unique identifier of a VAL user.

}

valUeId = {

valUeId: text ; Unique identifier of a VAL UE.

}

ValTargetUe = valUserId / valUeId

;;; Uinteger

;;+ Unsigned Integer, i.e. only value 0 and integers above 0 are permissible.

Uinteger = int .ge 0

;;; GeographicArea

;;+ Geographic area specified by different shape.

GeographicArea = Point / PointUncertaintyCircle / PointUncertaintyEllipse / Polygon / PointAltitude / PointAltitudeUncertainty / EllipsoidArc

;;; GADShape

;;+ Common base type for GAD shapes.

GADShape = {

shape: SupportedGADShapes

}

;;; Point

;;+ Ellipsoid Point.

Point = {

~GADShape

point: GeographicalCoordinates

}

;;; PointUncertaintyCircle

;;+ Ellipsoid point with uncertainty circle.

PointUncertaintyCircle = {

~GADShape

point: GeographicalCoordinates

uncertainty: Uncertainty

}

;;; PointUncertaintyEllipse

;;+ Ellipsoid point with uncertainty ellipse.

PointUncertaintyEllipse = {

~GADShape

point: GeographicalCoordinates

uncertaintyEllipse: UncertaintyEllipse

confidence: Confidence

}

;;; Polygon

;;+ Polygon.

Polygon = {

~GADShape

pointList: PointList

}

;;; PointAltitude

;;+ Ellipsoid point with altitude.

PointAltitude = {

~GADShape

point: GeographicalCoordinates

altitude: Altitude

}

;;; PointAltitudeUncertainty

;;+ Ellipsoid point with altitude and uncertainty ellipsoid.

PointAltitudeUncertainty = {

~GADShape

point: GeographicalCoordinates

altitude: Altitude

uncertaintyEllipse: UncertaintyEllipse

uncertaintyAltitude: Uncertainty

confidence: Confidence

}

;;; EllipsoidArc

;;+ Ellipsoid Arc.

EllipsoidArc = {

~GADShape

point: GeographicalCoordinates

innerRadius: InnerRadius

uncertaintyRadius: Uncertainty

offsetAngle: Angle

includedAngle: Angle

confidence: Confidence

}

;;; GeographicalCoordinates

;;+ Geographical coordinates.

GeographicalCoordinates = {

lon: -180.0..180.0

lat: -90.0..90.0

}

;;; UncertaintyEllipse

;;+ Ellipse with uncertainty.

UncertaintyEllipse = {

semiMajor: Uncertainty

semiMinor: Uncertainty

orientationMajor: Orientation

}

;;; PointList

;;+ List of points.

PointList = [3\*15 GeographicalCoordinates]

;;; Altitude

;;+ Indicates value of altitude.

Altitude = -32767.0..32767.0

;;; Angle

;;+ Indicates value of angle.

Angle = 0..360

;;; Uncertainty

;;+ Indicates value of uncertainty.

Uncertainty = float32 .ge 0

;;; Orientation

;;+ Indicates value of orientation angle.

Orientation = 0..180

;;; Confidence

;;+ Indicates value of confidence.

Confidence = 0..100

;;; InnerRadius

;;+ Indicates value of the inner radius.

InnerRadius = (0..327675) .and int32

;;; SupportedGADShapes

;;+ Indicates supported GAD shapes.

SupportedGADShapes = "POINT" / "POINT\_UNCERTAINTY\_CIRCLE" / "POINT\_UNCERTAINTY\_ELLIPSE" / "POLYGON" / "POINT\_ALTITUDE" / "POINT\_ALTITUDE\_UNCERTAINTY" / "ELLIPSOID\_ARC" / "LOCAL\_2D\_POINT\_UNCERTAINTY\_ELLIPSE" / "LOCAL\_3D\_POINT\_UNCERTAINTY\_ELLIPSOID" / text

### A.3.2.6 Media Types

The media type for a request to establish an SDDM data transmission quality measurement shall be "application/vnd.3gpp.seal-data-delivery-measurement-subscription-req-info+cbor".

The media type for a response of establishing an SDDM data transmission quality measurement shall be "application/vnd.3gpp.seal-data-delivery-measurement-subscription-res-info+cbor".

The media type for notification of an SDDM data transmission quality measurement shall be "application/vnd.3gpp.seal-data-delivery-measurement-notification-info+cbor".

Editor’s note: The MIME types need to be registered after the approval of the TS.

### A.3.2.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-measurement-subscription-req-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-measurement-subscription-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "MeasurementSubscriptionRequest" data type in 3GPP TS 24.543 clause A.3.2.3.2.1 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.3.2.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-measurement-subscription-res-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-measurement-subscription-res-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "MeasurementSubscriptionResponse" data type in 3GPP TS 24.543 clause A.3.2.3.2.2 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.3.2.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-measurement-notification-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-measurement-notification-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "MeasurementNotification" data type in 3GPP TS 24.543 clause A.3.2.3.2.3 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

## A.3.3 Sdd\_TransmissionQualityManagement API

### A.3.3.1 API URI

The CoAP URIs used in CoAP requests from SDDM-S towards the SDMM-C shall have the Resource URI structure as defined in clause C.1.1 of 3GPP TS 24.546 [6] with the following clarifications:

a) the <apiName> shall be "sdd-rtc-s";

b) the <apiVersion> shall be "v1"; and

c) the <apiSpecificSuffixes> shall be set as described in clause A.3.3.2.

### A.3.3.2 Resources

#### A.3.3.2.1 Overview



Figure A.3.3.2.1.1: Resource URI structure of the Sdd\_TransmissionQualityManagement API provided by SDDM-S

Table A.3.3.2.1.1 provides an overview of the resources and applicable CoAP methods.

Table A.3.3.2.1.1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name | Resource URI | CoAP method | Description |
| SDD Transmission Quality Management | val-services/{valServiceId}/sdd-transmission-quality-management | POST | Establish an SDDM data transmission quality management. |
| DELETE | Releases an SDDM data transmission quality management. |

#### A.3.3.2.2 Resource: SDD Transmission Quality Management

##### A.3.3.2.2.1 Description

The SDD transmission quality management resource allows an SDDM-C to manage an SDDM data transmission quality management of an SDDM-S.

##### A.3.3.2.2.2 Resource Definition

Resource URI: **{apiRoot}/sdd-rtc-s/<apiVersion>/val-services/{valServiceId}/sdd--transmission-quality-management**

This resource shall support the resource URI variables defined in the table A.3.3.2.2.2.1.

Table A.3.3.2.2.2.1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Definition |
| apiRoot | string | See clause C.1.1 of 3GPP TS 24.546 [6]. |
| apiVersion | string | See clause A.3.3.1. |
| valServiceId | string | Identifier of a VAL service. |

##### A.3.3.2.2.3 Resource Standard Methods

###### A.3.3.2.2.3.1 POST

This operation allows to establish an SDDM data transmission quality management.

This method shall support the request data structures the data structures, request codes and response codes specified in table A.3.3.2.2.3.1.1 and A.3.3.2.2.3.1.2.

Table A.3.3.2.2.3.1.1: Data structures supported by the POST Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| MeasurementsSubscriptionResquest | M | 1 | The information of request of establishment of an SDDM data transmission quality management. |

Table A.3.3.2.2.3.1.2: Data structures supported by the POST Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| MeasurementsSubscriptionResponse | M | 1 | 2.01 Created | SDDM data transmission quality management created successfully. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

###### A.3.3.2.2.3.2 DELETE

This operation releases an SDDM data transmission quality management.

This method shall support the request data structures the data structure, request codes and response codes specified in table A.3.3.2.2.3.2.1 and A.3.3.2.2.3.2.2.

Table A.3.3.2.2.3.2.1: Data structures supported by the DELETE Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| n/a |  |  | The information of request of release of an SDDM data transmission quality management. |

Table A.3.3.2.2.3.2.2: Data structures supported by the DELETE Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.02 Deleted | SDDM data transmission quality management released successfully. |
| NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

### A.3.3.3 Data Model

#### A.3.3.3.1 General

Table A.3.3.3.1.1 specifies the data types defined specifically for the SDD\_TransmissionQualityManagement API service provided by SDDM-S.

Table A.3.3.3.1.1: SDD\_TransmissionQualityManagement API provided by SDDM-S specific data types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Section defined | Description | Applicability |
| ValTargetUe | A.2.2 | Information identifying a VAL user ID or VAL UE ID. |  |
| TxQualityManagementRequest | A.3.3.3.2.1 | Information identifying an SDD data transmission quality guarantee request. |  |
| TxQualityManagementResponse | A.3.3.3.2.2 | Information identifying an SDD data transmission quality guarantee response. |  |

Table A.3.3.3.1.2 specifies the simple data types defined specifically for the SDD\_TransmissionQualityManagement API service provided by SDDM-S.

Table A.3.3.3.1.2: SDD\_TransmissionQualityManagement API provided by SDDM-S specific simple data types

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| Uinteger | A.2.3 | Unsigned integer. |

Table A.3.3.3.1.3 specifies the enumerations defined specifically for the SDD\_TransmissionQualityManagement API service provided by SDDM-S.

Table A.3.3.3.1.3: SDD\_TransmissionQualityManagement API provided by SDDM-S specific enumeration

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| ResultOp | A.2.6.2 | Information identifying the result of an operation. |
| Cause | A.2.6.3 | Information identifying the reason of the cause of the failure of an operation. |

#### A.3.3.3.2 Structured data types

##### A.3.3.3.2.1 Type: TxQualityManagementRequest

Table A.3.3.3.2.2.1: Definition of type TxQualityManagementRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| sealFlowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |
| txQualityManagementAction | string | M | 1 | Identity of the data transmission quality guarantee action to be performed which is set to "REDUNDANT TRANSMISSION PATH", "RE-ESTABLISH TRANSMISSION PATH", "SWITCH TO BACKUP TRANSMISSION PATH" or "BACK TO SINGLE TRANSMISSION PATH" that was triggered by an event (e.g. measurement threshold). |  |

##### A.3.3.3.2.2 Type: TxQualityManagementResponse

Table A.3.3.3.2.2.1: Definition of type TxQualityManagementResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| result | ResultOp | M | 1 | Result of the establishment request. |  |
| cause | Cause | O | 0..1 | Reason of the cause of the failure of the establishment request (NOTE). |  |
| NOTE: This attribute shall be included if result is set to "FAILURE". | | | | | |

#### A.3.3.3.3 Simple data types and enumerations

None.

### A.3.3.4 Error Handling

General error responses are defined in clause C.1.3 of 3GPP TS 24.546 [6].

### A.3.3.5 CDDL Specification

#### A.3.3.5.1 Introduction

The data model described in clause A.3.3.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [20].

Clause A.3.3.5.2 uses the concise data definition language described in IETF RFC 8610 [18] and provides corresponding representation of the SDD\_TransmissionQualityManagement API provided by the SDDM-S data model.

#### A.3.3.5.2 CDDL document

;;; TxQualityManagementRequest

;;+ Represents a request for performing SDDM data transmission quality management.

TxQualityManagementRequest = {

sealFlowId: Uinteger

txQualityManagementAction: string

}

;;; TxQualityManagementResponse

;;+ Represents the response of a request for performing SDDM data transmission quality management.

TxQualityManagementResponse = {

result: ResultOp

? cause: Cause

}

;;; ResultOp

;;+ Represents the result of an operation.

ResultOp = "SUCCESS" / "FAILURE"

;;; Cause

;;+ Represents the cause of failure of an operation.

Cause = "VAL CLIENT ERROR" / "SEALDD POLICY MISMATCH" / "OTHER"

;;; ValTargetUe

;;+ Represents information identifying a VAL user ID or a VAL UE ID.

valUserId = {

valUserId: text ; Unique identifier of a VAL user.

}

valUeId = {

valUeId: text ; Unique identifier of a VAL UE.

}

ValTargetUe = valUserId / valUeId

;;; Uinteger

;;+ Unsigned Integer, i.e. only value 0 and integers above 0 are permissible.

Uinteger = int .ge 0

### A.3.3.6 Media Types

The media type for a request to establish an SDDM data transmission quality guarantee shall be "application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-req-info+cbor".

The media type for a response of establishing a SDDM data transmission quality guarantee shall be "application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-res-info+cbor".

Editor’s note: The MIME types need to be registered after the approval of the TS.

### A.3.3.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-req-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-tx-quality-mgt-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "TxQualityManagementRequest" data type in 3GPP TS 24.543 clause A.3.3.3.2.1 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.3.3.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-tx-quality-mgt-res-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-tx-quality-mgt--res-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "TxQualityManagementResponse" data type in 3GPP TS 24.543 clause A.3.3.3.2.2 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

# A.4 Resource representation and APIs provided by SDDM-C

## A.4.1 Sdd\_RegularTransmissionConnection API

### A.4.1.1 API URI

The CoAP URIs used in CoAP requests from SDDM-C towards the SDMM-S shall have the Resource URI structure as defined in clause C.1.1 of 3GPP TS 24.546 [6] with the following clarifications:

a) the <apiName> shall be "sdd-rtc-c";

b) the <apiVersion> shall be "v1"; and

c) the <apiSpecificSuffixes> shall be set as described in clause A.4.1.2.

### A.4.1.2 Resources

#### A.4.1.2.1 Overview



Figure A.4.1.2.1.1: Resource URI structure of the Sdd\_RegularTransmissionConnection API provided by SDDM-C

Table A.4.1.2.1.1 provides an overview of the resources and applicable CoAP methods.

Table A.4.1.2.1.1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name | Resource URI | CoAP method | Description |
| SDD Regular Transmission Connection | val-services/{valServiceId}/sdd-regular-transmission-connection | POST | Establish anSDDM regular transmission connection. |
| DELETE | Release anSDDM regular transmission connection |

#### A.4.1.2.2 Resource: SDD Regular Transmission Connection

##### A.4.1.2.2.1 Description

The SDD regular transmission connection resource represents an SDD regular transmission connection to be created at a given SDDM-C and SDDM-S.

The establishment request resource allows a SDDM-C to request the SDDM-S to establish an SDDM regular transmission.

##### A.4.1.2.2.2 Resource Definition

Resource URI: **{apiRoot}/sdd-rtc-c/<apiVersion>/val-services/{valServiceId}/sdd-regular-transmission-connection**

This resource shall support the resource URI variables defined in the table A.4.1.2.2.2.1.

Table A.4.1.2.2.2.1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Definition |
| apiRoot | string | See clause C.1.1 of 3GPP TS 24.546 [6]. |
| apiVersion | string | See clause A.4.1.1. |
| valServiceId | string | Identifier of a VAL service. |

##### A.4.1.2.2.3 Resource Standard Methods

A.4.1.2.2.3.1 POST

This operation allows to establish an SDDM regular transmission connection.

This method shall support the request data structures the data structures, request codes and response codes specified in table A.4.1.2.2.3.1.1 and A.4.1.2.2.3.1.2.

Table A.4.1.2.2.3.1.1: Data structures supported by the POST Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| EstablishmentRequest | M | 1 | The information of request of establishment of an SDDM regular transmission connection. |

Table A.4.1.2.2.3.1.2: Data structures supported by the POST Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| EstablishmentResponse | M | 1 | 2.01 Created | SDDM regular transmission connection created successfully. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [31] shall also apply. | | | | |

A.4.1.2.2.3.2 DELETE

This operation releases an SDDM regular transmission connection.

This method shall support the request data structures the data structures, request codes and response codes specified in table A.4.1.2.2.3.2.1 and A.4.1.2.2.3.2.2.

Table A.4.1.2.2.3.2.1: Data structures supported by the DELETE Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| ReleaseRequest | M | 1 | The information of request of release of an SDDM regular transmission connection. |

Table A.4.1.2.2.3.2.2: Data structures supported by the DELETE Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.02 Deleted | SDDM regular transmission connection released successfully. |
| NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 of 3GPP TS 24.546 [31] shall also apply. | | | | |

### A.4.1.3 Data Model

#### A.4.1.3.1 General

Table A.4.1.3.1.1 specifies the data types defined specifically for the SDD\_RegularTransmissionConnection API service provided by SDDM-C.

Table A.4.1.3.1.1: SDD\_RegularTransmissionConnection API provided by SDDM-C specific data types

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Data type | | Section defined | | Description | | Applicability | |
| ValTargetUe | | A.2.2 | | Information identifying a VAL user ID or VAL UE ID. | |  | |
| EstablishmentResponse | | A.2.4.1 | | Information identifying an SDD regular transmission connection establishment response. | |  | |
| EstablishmentRequest | | A.3.1.3.2.1 | | Information identifying an SDD regular transmission connection establishment request. | |  | |
| ReleaseRequest | | A.3.1.3.2.3 | | Information identifying an SDD regular transmission connection release request. | |  | |

Table A.4.1.3.1.2 specifies the simple data types defined specifically for the SDD\_RegularTransmissionConnection API service provided by SDDM-C.

Table A.4.1.3.1.2: SDD\_RegularTransmissionConnection API provided by SDDM-C specific simple data types

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| Uinteger | A.2.3 | Unsigned integer. |
| ServerId | A.2.5 | String representing a unique identifier of a VAL server. |

Table A.4.1.3.1.3 specifies the enumerations defined specifically for the SDD\_RegularTransmissionConnection API service provided by SDDM-C.

Table A.4.1.3.1.3: SDD\_RegularTransmissionConnection API provided by SDDM-C specific enumeration

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| RequestorId | A.2.6.1 | Information identifying a VAL user ID or VAL UE ID. |
| ResultOp | A.2.6.2 | Information identifying the result of an operation. |
| Cause | A.2.6.3 | Information identifying the reason of the cause of the failure of an operation. |

#### A.4.1.3.2 Structured data types

##### A.4.1.3.2.1 Type: EstablishmentRequest

Table A.4.1.3.2.1.1: Definition of type EstablishmentRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| requestorId | RequestorId | M | 1 | Identity of the requestor of the establishment request (NOTE). |  |
| sealFlowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |
| serverId | ServerId | M | 1 | Identity of the VAL server. |  |
| endpointId | string | M | 1 | Identity of the endpoint of the selected VAL server to which the establishment request has to be sent. |  |
| valServiceId | string | O | 0..1 | Identity of the VAL service enabled by the SDD regular transmission connection. |  |
| userPlaneAddress | string | O | 0..1 | Identity of the IP address of the traffic. |  |
| portNumber | Uinteger | O | 0..1 | Identity of the port number of the traffic. |  |
| url | string | O | 0..1 | Identity of the address of a given unique resource on the Web for the traffic. |  |
| transportLayer | string | O | 0..1 | Identity of the transport layer protocol for the traffic. |  |
| valTgtUe | ValTargetUe | O | 0..1 | VAL user to whom the establishment request is applied. |  |
| NOTE: This attribute shall be set to "SEALDDCLIENT". | | | | | |

##### A.4.1.3.2.2 Type: ReleaseRequest

Table A.4.1.3.2.2.1: Definition of type ReleaseRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| sealClientId | string | M | 1 | Identity of the SDDM-C. |  |
| sealFlowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |

#### A.4.1.3.3 Simple data types and enumerations

None.

### A.4.1.4 Error Handling

General error responses are defined in clause C.1.3 of 3GPP TS 24.546 [6].

### A.4.1.5 CDDL Specification

#### A.4.1.5.1 Introduction

The data model described in clause A.4.1.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [20].

Clause A.4.1.5.2 uses the concise data definition language described in IETF RFC 8610 [19] and provides corresponding representation of the SDD\_RegularTransmissionConnection API provided by the SDDM-C data model.

#### A.4.1.5.2 CDDL document

Editor’s note: The CDDL document is FFS.

### A.4.1.6 Media Types

See clause A.3.1.6.

## A.4.2 Sdd\_URLCCTransmissionConnection API

### A.4.2.1 API URI

The CoAP URIs used in CoAP requests from SDDM-C towards the SDMM-S shall have the Resource URI structure as defined in clause C.1.1 of 3GPP TS 24.546 [6] with the following clarifications:

a) the <apiName> shall be "sdd-rtc-c";

b) the <apiVersion> shall be "v1"; and

c) the <apiSpecificSuffixes> shall be set as described in clause A.4.2.2.

### A.4.2.2 Resources

#### A.4.2.2.1 Overview



Figure A.4.2.2.1.1: Resource URI structure of the Sdd\_URLLCTransmissionConnection API provided by SDDM-C

Table A.4.2.2.1.1 provides an overview of the resources and applicable CoAP methods.

Table A.4.2.2.1.1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name | Resource URI | CoAP method | Description |
| URLLC Transmission Connection | val-services/{valServiceId}/urllc-transmission-connection | POST | Establish a URLLC transmission connection. |
| PUT | Update a URLLC transmission connection. |
| DELETE | Releases a URLLC transmission connection. |

#### A.4.2.2.2 Resource: URLLC Transmission Connection

##### A.4.2.2.2.1 Description

The URLLC transmission connection resource allows an SDDM-S to manage a URLCC transmission connection of an SDDM-C.

##### A.4.2.2.2.2 Resource Definition

Resource URI: **{apiRoot}/sdd-rtc-c/<apiVersion>/val-services/{valServiceId}/urllc-transmission-connection**

This resource shall support the resource URI variables defined in the table A.4.2.2.2.2.1.

Table A.4.1.2.2.2.1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Definition |
| apiRoot | string | See clause C.1.1 of 3GPP TS 24.546 [6]. |
| apiVersion | string | See clause A.4.2.1. |
| valServiceId | string | Identifier of a VAL service. |

##### A.4.2.2.2.3 Resource Standard Methods

A.4.2.2.2.3.1 POST

This operation retrieves the allowed registration.

This method shall support the request data structures, request codes and response codes specified in table A.4.2.2.2.3.1.1 and A.4.2.2.2.3.1.2.

Table A.4.2.2.2.3.1.1: Data structures supported by the POST Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| URLLCEstablishmentRequest | M | 1 | The information of request of establishment of an SDDM URLLC transmission connection. |

Table A.4.2.2.2.3.1.2: Data structures supported by the POST Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| URLLCEstablishmentResponse | M | 1 | 2.01 Created | URLLC transmission connection created successfully. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [31] shall also apply. | | | | |

A.4.2.2.2.3.2 PUT

This operation updates a URLLC transmission connection.

This method shall support the request data structures the data structures, request codes and response codes specified in table A.4.2.2.2.3.2.1 and A.4.2.2.2.3.2.2.

Table A.4.2.2.2.3.2.1: Data structures supported by the PUT Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| URLLCUpdateRequest | M | 1 | The information of request of update a URLLC transmission connection. |

Table A.4.2.2.2.3.2.1: Data structures supported by the PUT Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| URLLCUpdateResponse | M | 1 | 2.04 Changed | URLLC transmission connection updated successfully. |
| NOTE: The mandatory CoAP error status codes for the PUT method listed in table C.1.3-1 of 3GPP TS 24.546 [31] shall also apply. | | | | |

A.4.2.2.2.3.3 DELETE

This operation releases a URLLC transmission connection.

This method shall support the request data structures the data structures, request codes and response codes specified in table A.4.2.2.2.3.3.1 and A.4.2.2.2.3.3.2.

Table A.4.2.2.2.3.3.1: Data structures supported by the DELETE Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| URLLCReleaseRequest | M | 1 | The information of request of release of a URLCC transmission connection. |

Table A.4.2.2.2.3.3.2: Data structures supported by the DELETE Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.02 Deleted | URLLC transmission connection released successfully. |
| NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 of 3GPP TS 24.546 [31] shall also apply. | | | | |

### A.4.2.3 Data Model

#### A.4.2.3.1 General

Table A.4.2.3.1.1 specifies the data types defined specifically for the SDD\_URLLCTransmissionConnection API service provided by SDDM-C.

Table A.4.2.3.1.1: SDD\_RegularTransmissionConnection API provided by SDDM-C specific data types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Section defined | Description | Applicability |
| ValTargetUe | A.2.2 | Information identifying a VAL user ID or VAL UE ID. |  |
| URLLCEstablishmentRequest | A.4.2.3.2.1 | Information identifying an SDD URLLC transmission connection establishment request. |  |
| URLLCEstablishmentResponse | A.4.2.3.2.2 | Information identifying an SDD URLLC transmission connection establishment response. |  |
| URLLCUpdateRequest | A.4.2.3.2.3 | Information identifying an SDD URLLC transmission connection update request. |  |
| URLLCReleaseRequest | A.4.2.3.2.4 | Information identifying an SDD URLLC transmission connection release request. |  |

Table A.4.2.3.1.2 specifies the simple data types defined specifically for the SDD\_RegularTransmissionConnection API service provided by SDDM-C.

Table A.4.2.3.1.2: SDD\_RegularTransmissionConnection API provided by SDDM-C specific simple data types

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| Uinteger | A.2.3 | Unsigned integer. |
| ServerId | A.2.5 | String representing a unique identifier of a VAL server. |

Table A.4.2.3.1.3 specifies the enumerations defined specifically for the SDD\_URLLCTransmissionConnection API service provided by SDDM-C.

Table A.4.2.3.1.3: SDD\_RegularTransmissionConnection API provided by SDDM-C specific enumeration

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| ResultOp | A.2.6.2 | Information identifying the result of an operation. |
| Cause | A.2.6.3 | Information identifying the reason of the cause of the failure of an operation. |

#### A.4.2.3.2 Structured data types

##### A.4.2.3.2.1 Type: URLLCEstablishmentRequest

Table A.4.2.3.2.1.1: Definition of type URLLCEstablishmentRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| sealClientId | string | M | 1 | Identity of the requestor of the URLLC establishment request. |  |
| sealFlowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |
| valTgtUe | ValTargetUe | M | 1 | VAL user to whom the establishment request is applied. |  |
| serverId | ServerId | M | 1 | Identity of the VAL server. |  |
| valServiceId | string | M | 0..1 | Identity of the VAL service enabled by the SDD regular transmission connection. |  |
| userPlaneAddress | string | O | 0..1 | Identity of the IP address of the traffic. |  |
| portNumber | Uinteger | O | 0..1 | Identity of the port number of the traffic. |  |
| url | string | O | 0..1 | Identity of the address of a given unique resource on the Web for the traffic. |  |
| transportLayer | string | O | 0..1 | Identity of the transport layer protocol for the traffic. |  |

##### A.4.2.3.2.2 Type: URLLCEstablishmentResponse

Table A.4.2.3.2.1.2: Definition of type URLLCEstablishmentResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| result | ResultOp | M | 1 | Result of the establishment request. |  |
| cause | Cause | O | 0..1 | Reason of the cause of the failure of the establishment request (NOTE 1). |  |
| userPlaneAddress | string | O | 0..1 | Identity of the IP address of the traffic (NOTE 2). |  |
| portNumber | Uinteger | O | 0..1 | Identity of the port number of the traffic (NOTE 2). |  |
| url | string | O | 0..1 | Identity of the address of a given unique resource on the Web for the traffic (NOTE 2). |  |
| transportLayer | string | O | 0..1 | Identity of the transport layer protocol for the traffic (NOTE 2). |  |
| NOTE 1: This attribute shall be included if result is set to "failure".  NOTE 2: This attribute may be included if result is set to "success". | | | | | |

##### A.4.2.3.2.3 Type: URLLCUpdateRequest

Table A.4.2.3.2.1.3: Definition of type URLLCUpdateRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| sealClientId | string | M | 1 | Identity of the requestor of the URLLC establishment request. |  |
| sealFlowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |
| valServiceId | string | O | 1..N | Identity of the VAL services enabled by the SDD URLLC transmission connection. |  |
| userPlaneAddress | string | O | 0..1 | Identity of the IP address of the traffic. |  |
| portNumrber | Uinteger | O | 0..1 | Identity of the port number of the traffic. |  |
| url | string | O | 0..1 | Identity of the address of a given unique resource on the Web for the traffic. |  |
| transportLayer | string | O | 0..1 | Identity of the transport layer protocol for the traffic. |  |

##### A.4.2.3.2.4 Type: URLLCReleaseRequest

Table A.4.2.3.2.4.1: Definition of type URLLCReleaseRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| sealClientId | string | M | 1 | Identity of the requestor of the establishment request. |  |
| sealflowId | Uinteger | M | 1 | Identity of SDDM flow used by the SDDM-C and SDDM-S to identify the application traffic. |  |

#### A.4.2.3.3 Simple data types and enumerations

None.

### A.4.2.4 Error Handling

General error responses are defined in clause C.1.3 of 3GPP TS 24.546 [6].

### A.4.2.5 CDDL Specification

#### A.4.2.5.1 Introduction

The data model described in clause A.4.2.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [20].

Clause A.4.2.5.2 uses the concise data definition language described in IETF RFC 8610 [19] and provides corresponding representation of the SDD\_URLLCTransmissionConnection API provided by the SDDM-C data model.

#### A.4.2.5.2 CDDL document

Editor’s note: The CDDL document is FFS.

### A.4.2.6 Media Types

The media type for a request to establish a URLLC transmission connection shall be "application/vnd.3gpp.seal-data-delivery-urllc-establishment-req-info+cbor".

The media type for a response of establishing a URLLC transmission connection shall be "application/vnd.3gpp.seal-data-delivery-urllc-establishment-res-info+cbor".

The media type for updating an established URLLC transmission connection shall be "application/vnd.3gpp.seal-data-delivery-urllc-update-req-info+cbor".

The media type for a request to release a URLLC transmission connection shall be "application/vnd.3gpp.seal-data-delivery-urllc-release-req-info+cbor".

Editor’s note: The MIME types need to be registered after the approval of the TS.

### A.4.2.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-establishment-req-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-urllc-establishment-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "URLLCEstablishmentRequest" data type in 3GPP TS 24.543 clause A.4.2.3.2.1 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-establishment-res-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-urllc-establishment-res-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "URLLCEstablishmentResponse" data type in 3GPP TS 24.543 clause A.4.2.3.2.2 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-update-req-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-urllc-update-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "URLLCUpdateRequest" data type in 3GPP TS 24.543 clause A.4.2.3.2.3 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.10 Media Type registration template for application/vnd.3gpp.seal-data-delivery-urllc-release-req-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-data-delivery-urllc-release-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "URLLCReleaseRequest" data type in 3GPP TS 24.543 clause A.4.2.3.2.4 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

## A.4.3 Sdd\_DataStorage API

### A.4.3.1 API URI

The CoAP URIs used in CoAP requests from SDDM-C towards the SDMM-S shall have the Resource URI structure as defined in clause C.1.1 of 3GPP TS 24.546 [6] with the following clarifications:

a) the <apiName> shall be "sdd-rtc-c";

b) the <apiVersion> shall be "v1"; and

c) the <apiSpecificSuffixes> shall be set as described in clause A.4.3.2.

### A.4.3.2 Resources

#### A.4.3.2.1 Overview



Figure A.4.3.2.1.1: Resource URI structure of the Sdd\_DataStorage API provided by SDDM-C

Table A.4.3.2.1.1 provides an overview of the resources and applicable CoAP methods.

Table A.4.3.2.1.1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name | Resource URI | CoAP method | Description |
| SDD data storage | val-services/{valServiceId}/sdd-data-storage | POST | Establish a SDDM data storage or reservation of a SDDM data storage. |
| PUT | Update a SDDM data storage. |
| DELETE | Releases a SDDM data storage. |
| GET | Retrieve a SDDM data storage. |
| FETCH | Observe a SDDM data storage. |

#### A.4.3.2.2 Resource: SDD Data Storage

##### A.4.3.2.2.1 Description

The SDDM data storage resource allows an SDDM-S to manage an SDDM data storage of an SDDM-C.

##### A.4.3.2.2.2 Resource Definition

Resource URI: **{apiRoot}/sdd-rtc-c/<apiVersion>/val-services/{valServiceId}/sdd-data-storage**

This resource shall support the resource URI variables defined in the table A.4.3.2.2.2.1.

Table A.4.3.2.2.2.1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Definition |
| apiRoot | string | See clause C.1.1 of 3GPP TS 24.546 [6]. |
| apiVersion | string | See clause A.4.3.1. |
| valServiceId | string | Identifier of a VAL service. |

##### A.4.3.2.2.3 Resource Standard Methods

###### A.4.3.2.2.3.1 POST

This operation request establishment or reservation of an SDDM data storage.

This method shall support the data structures, request codes and response codes specified in table A.4.3.2.2.3.1.1 and A.4.3.2.2.3.1.2.

Table A.4.3.2.2.3.1.1: Data structures supported by the POST Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| DataStorageCreationRequest | O | 0..1 | The information of request of establishment of an SDDM data storage. |
| DataStorageReservationRequest | O | 0..1 | The information of request of reservation of an SDDM data storage. |

Table A.4.3.2.2.3.1.2: Data structures supported by the POST Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| DataStorageCreationResponse | O | 0..1 | 2.01 Created | SDDM data storage created successfully. |
| DataStorageReservationResponse | O | 0..1 | 2.01 Created | SDDM data storage reserved successfully. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

###### A.4.3.2.2.3.2 PUT

This operation updates an SDDM data storage.

This method shall support the data structures, request codes and response codes specified in table A.4.3.2.2.3.2.1 and A.4.3.2.2.3.2.2.

Table A.4.3.2.2.3.2.1: Data structures supported by the PUT Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| DataStorageMgtRequest | M | 1 | The information of request of update an SDDM data storage. |

Table A.4.3.2.2.3.2.1: Data structures supported by the PUT Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.04 Changed | SDDM data storage updated successfully. |
| NOTE: The mandatory CoAP error status codes for the PUT method listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

###### A.4.3.2.2.3.3 DELETE

This operation releases an SDD data storage.

This method shall support the data structures, request codes and response codes specified in table A.4.3.2.2.3.3.1 and A.4.3.2.2.3.3.2.

Table A.4.3.2.2.3.3.1: Data structures supported by the DELETE Request payload on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| DataStorageMgtRequest | M | 1 | The information of request of release of an SDD data storage. |

Table A.4.3.2.2.3.3.2: Data structures supported by the DELETE Response payload on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| n/a |  |  | 2.02 Deleted | SDDM data storage released successfully. |
| NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

###### A.4.3.2.2.3.4 GET

This operation retrieves an SDDM data storage information.

This method shall support the URI query parameters, the data structures and response codes specified in table A.4.3.2.2.3.4.1 and A.4.3.2.2.3.4.2.

Table A.4.3.2.2.3.4.1: URI query options supported by the GET Request on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| data-identifier | string | M | 1 | The data identifier of an SDDM data storage. |

Table A.4.3.2.2.3.4.2: Data structures supported by the GET Response payload on this resource

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Data type | | P | Cardinality | Response  codes | Description |
| DataStorageQueryResponse | | M | 1 | 2.05 Content | The SDDM data storage information based on the request from the SDDM-C. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

###### A.4.3.2.2.3.5 FETCH

This operation provides an SDDM data storage.

This method shall support the request options, the data structures, request codes and response codes, and the response options specified in table A.4.3.2.2.3.5.1, A.4.3.2.2.3.5.2, A.4.3.2.2.3.5.3 and A.4.3.2.2.3.5.4.

Table A.4.3.2.2.3.5.1: Options supported by the FETCH Request on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| observe | Uinteger | O | 0..1 | When set to 0 (Register) it extends the FETCH request to subscribe to the changes of this resource.  When set to 1 (Deregister) it cancels the subscription. |
| NOTE: Other request options also apply in accordance with normal CoAP procedures. | | | | |

Table A.3.2.2.3.5.2: Data structures supported by the FETCH Request on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| DataStorageMgtRequest | M | 1 | The identifier of an SDDM data storage. |

Table A.3.2.2.3.5.3: Data structures supported by the FETCH Response payload on this resource

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Data type | | P | Cardinality | Response  codes | Description |
| DataStorageStatusNotification | | M | 1 | 2.05 Content | The information of an SDDM data storage based on the request from the SDDM-C. |
| NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 of 3GPP TS 24.546 [6] shall also apply. | | | | |

Table A.3.2.2.3.5.4: Options supported by the 2.05 Response Code on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| observe | Uinteger | O | 0..1 | Sequence number of the SDDM data storage notification. |
| NOTE: Other response options also apply in accordance with normal CoAP procedures. | | | | |

### A.4.3.3 Data Model

#### A.4.3.3.1 General

Table A.4.3.3.1.1 specifies the data types defined specifically for the SDD\_DataStorage API service provided by SDDM-C.

Table A.4.3.3.1.1: SDD\_DataStorage API provided by SDDM-C specific data types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Section defined | Description | Applicability |
| ValTargetUe | A.2.2 | Information identifying a VAL user ID or VAL UE ID. |  |
| DataStorageCreationRequest | A.4.3.3.2.1 | Information identifying an SDD data storage creation request. |  |
| DataStorageCreationResponse | A.4.3.3.2.2 | Information identifying an SDD data storage creation response. |  |
| DataStorageReservationRequest | A.4.3.3.2.3 | Information identifying an SDD data storage reservation request. |  |
| DataStorageReservationResponse | A.4.3.3.2.4 | Information identifying an SDD data storage reservation response. |  |
| DataStorageStatusNotification | A.4.3.3.2.5 | Information identifying an SDD data storage notification. |  |
| DataStorageQueryResponse | A.4.3.3.2.6 | Information identifying an SDD data storage query response. |  |
| DataStorageMgtRequest | A.4.3.3.2.7 | Information identifying an SDD data storage management request. |  |
| StatusInformationReq | A.4.3.3.2.8 | Information identifying the identity of stored data. |  |
| StatustInformationRes | A.4.3.3.2.9 | Information of the stored data returned by the SDDM-S which is tracked or monitored. |  |

Table A.4.3.3.1.2 specifies the simple data types defined specifically for the SDD\_DataStorage API service provided by SDDM-C.

Table A.4.3.3.1.2: SDD\_DataStorage API provided by SDDM-C specific simple data types

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| Uinteger | A.2.3 | Unsigned integer. |
| ServerId | A.2.5 | String representing a unique identifier of a VAL server. |

Table A.4.3.3.1.3 specifies the enumerations defined specifically for the SDD\_DataStorage API service provided by SDDM-C.

Table A.4.3.3.1.3: SDD\_DataStorage API provided by SDDM-C specific enumeration

|  |  |  |
| --- | --- | --- |
| Data type | Section defined | Description |
| ResultOp | A.2.6.2 | Information identifying the result of an operation. |
| Cause | A.2.6.3 | Information identifying the reason of the cause of the failure of an operation. |

#### A.4.3.3.2 Structured data types

##### A.4.3.3.2.1 Type: DataStorageCreationRequest

Table A.4.3.3.2.1.1: Definition of type DataStorageCreationRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| applicationData | bytes | M | 1 | Information of the application data to be stored. |  |
| accessControlPolicy | string | M | 1 | Identity of the control policy for the requested data access from other consumers which is set to "SDDM-C", "VAL server" or "SDDM-S". |  |
| expiryTime | DateTime | O | 0..1 | Information of the expiration time of the data to be stored. |  |
| statusInformationReq | StatusInformationReq | O | 0..1 | Identity of the information of the stored data. |  |

##### A.4.3.3.2.2 Type: DataStorageCreationResponse

Table A.4.3.3.2.2.1: Definition of type DataStorageCreationResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| result | ResultOp | M | 1 | Result of the data storage creation request. |  |
| cause | Cause | O | 0..1 | Reason of the cause of the failure of the data storage creation request (NOTE 1). |  |
| dataIdentifier | string | O | 0..1 | Information of the identity of the stored data (NOTE 2). |  |
| NOTE 1: This attribute shall be included if result is set to "FAILURE".  NOTE 2: This attribute shall be included if result is set to "SUCCESS". | | | | | |

##### A.4.3.3.2.3 Type: DataStorageReservationRequest

Table A.4.3.3.2.3.1: Definition of type DataStorageReservationRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| valServiceId | string | M | 1 | Identity of the VAL service of the vertical application. |  |
| dataLength | Uinteger | O | 0..1 | Identity of the data length to be stored. |  |

##### A.4.3.3.2.4 Type: DataStorageReservationResponse

Table A.4.3.3.2.4.1: Definition of type DataStorageReservationResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| result | ResultOp | M | 1 | Result of the data storage creation request. |  |
| cause | Cause | O | 0..1 | Reason of the cause of the failure of the data storage creation request (NOTE 1). |  |
| address | string | O | 0..1 | Information of the identity of the reserved address for data storage (NOTE 2). |  |
| NOTE 1: This attribute shall be included if result is set to "FAILURE".  NOTE 2: This attribute shall be included if result is set to "SUCCESS". | | | | | |

##### A.4.3.3.2.5 Type: DataStorageStatusNotification

Table A.4.3.3.2.5.1: Definition of type DataStorageStatusNotification

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| dataIdentifier | string | M | 1 | Information of the identity of the stored data. |  |
| statusInformationRsp | StatusInformationRsp | M | 1 | Information of the stored data returned by the SDDM-S which is tracked or monitored. |  |

##### A.4.3.3.2.6 Type: DataStorageQueryResponse

Table A.4.3.3.2.6.1: Definition of type DataStorageQueryResponse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| result | ResultOp | M | 1 | Result of the data storage creation request. |  |
| cause | Cause | O | 0..1 | Reason of the cause of the failure of the data storage creation request (NOTE 1). |  |
| dataIdentifier | string | O | 0..1 | Information of the identity of the stored data (NOTE 2). |  |
| applicationData | bytes | O | 0..1 | Information of the application data to be stored (NOTE 3). |  |
| NOTE 1: This attribute shall be included if result is set to "FAILURE".  NOTE 2: This attribute shall be included if result is set to "SUCCESS".  NOTE 3: This attribute may be included if result is set to "SUCCESS". | | | | | |

##### A.4.3.3.2.7 Type: DataStorageMgtRequest

Table A.4.3.3.2.7.1: Definition of type DataStorageMgtRequest

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| dataIdentifier | string | M | 1 | Information of the identity of the stored data. |  |
| applicationData | bytes | O | 0..1 | Information of the application data to be stored. |  |

##### A.4.3.3.2.8 Type: StatusInformationReq

Table A.4.3.3.2.8.1: Definition of type StatusInformationReq

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| noTimesDataAccessed | boolean | O | 0..1 | Identify whether information of how many times the stored data is accessed is requested. Value "true" indicates that the information about how many times the stored data is accessed is requested. Value "false" indicates that the information about how many times the stored data is accessed is not requested. |  |
| noTimesDataManaged | boolean | O | 0..1 | Identify whether information of how many times the stored data is managed is requested. Value "true" indicates that the information about how many times the stored data is managed is requested. Value "false" indicates that the information about how many times the stored data is managed is not requested. |  |

##### A.4.3.3.2.9 Type: StatusInformationRes

Table A.4.3.3.2.9.1: Definition of type StatusInformationRes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| noTimesDataAccessedValue | Uinteger | O | 0..1 | Information of the value of how many times the stored data is accessed. |  |
| noTimesDataManagedValue | Uinteger | O | 0..1 | Information of the value of how many times the stored data is managed. |  |

#### A.4.3.3.3 Simple data types and enumerations

None.

### A.4.3.4 Error Handling

General error responses are defined in clause C.1.3 of 3GPP TS 24.546 [6].

### A.4.3.5 CDDL Specification

#### A.4.3.5.1 Introduction

The data model described in clause A.4.3.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [20].

Clause A.4.3.5.2 uses the concise data definition language described in IETF RFC 8610 [19] and provides corresponding representation of the SDD\_DataStorage API provided by the SDDM-C data model.

#### A.4.3.5.2 CDDL document

;;; DataStorageCreationRequest

;;+ Represents a request for performing SDDM data data storage creation.

DataStorageCreationRequest = {

applicationData: bytes

accessControlPolicy: string

? expiryTime: DateTime

? statusInformationReq: StatusInformationReq

}

;;; DataStorageCreationResponse

;;+ Represents the response of a request for performing SDDM data data storage creation.

DataStorageCreationResponse = {

result: ResultOp

? cause: Cause

? dataIdentifier: string

}

;;; DataStorageReservationRequest

;;+ Represents a request for performing SDDM data data storage reservation.

DataStorageReservationRequest = {

valServiceId: string

? dataLength: Uinteger

}

;;; DataStorageReservationResponse

;;+ Represents the response of a request for performing SDDM data data storage reservation.

DataStorageReservationResponse = {

result: ResultOp

? cause: Cause

? address: string

}

;;; DataStorageStatusNotification

;;+ Represents the information of SDDM data storage status notification of the SDDM-C.

MeasurementSubscriptionNotification = {

dataIdentifier: string

statusInformationRsp: StatusInformationRsp

}

;;; DataStorageQueryResponse

;;+ Represents the response of a request for performing SDDM data data storage query.

DataStorageQueryResponse = {

result: ResultOp

? cause: Cause

? dataIdentifier: string

? applicationData: bytes

}

;;; DataStorageMgtRequest

;;+ Represents a request for performing SDDM data data storage management.

DataStorageMgtRequest = {

dataIdentifier: string

? applicationData: bytes

}

;;; StatusInformationReq

StatusInformationReq = {

? noTimesDataAccessed: bool

? noTimesDataManageed: bool

}

;;; StatusInformationRes

StatusInformationRes = {

noTimesDataAccessed: Uinteger

noTimesDataManageed: bool

}

;;; ResultOp

;;+ Represents the result of an operation.

ResultOp = "SUCCESS" / "FAILURE"

;;; Cause

;;+ Represents the cause of failure of an operation.

Cause = "VAL CLIENT ERROR" / "SEALDD POLICY MISMATCH" / "OTHER"

;;; ValTargetUe

;;+ Represents information identifying a VAL user ID or a VAL UE ID.

valUserId = {

valUserId: text ; Unique identifier of a VAL user.

}

valUeId = {

valUeId: text ; Unique identifier of a VAL UE.

}

ValTargetUe = valUserId / valUeId

;;; Uinteger

;;+ Unsigned Integer, i.e. only value 0 and integers above 0 are permissible.

Uinteger = int .ge 0

### A.4.3.6 Media Types

The media type for a request to create data storage to the SDDM-S shall be "application/vnd.3gpp.seal-data-delivery-data-storage-creation-req-info+cbor".

The media type for a response of creating data storage shall be "application/vnd.3gpp.seal-data-delivery-data-storage-creation-res-info+cbor".

The media type for a request to reserve data storage shall be "application/vnd.3gpp.seal-data-delivery-data-storage-reservation-req-info+cbor".

The media type for a response of reserving data storage shall be "application/vnd.3gpp.seal-data-delivery-data-storage-reservation-res-info+cbor".

The media type for a data storage notification shall be "application/vnd.3gpp.seal-data-delivery-data-storage-status-notification-info +cbor".

The media type for a response of querying data storage shall be "application/vnd.3gpp.seal-data-delivery-data-storage-query-res-info+cbor".

The media type for a request to manage data storage shall be "application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor".

Editor’s note: The MIME types need to be registered after the approval of the TS.

### A.4.2.7 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-creation-req-info+cbor

Type name: application

Subtype name: application/vnd.3gpp.seal-data-delivery-data-storage-creation-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "DataStorageCreationRequest" data type in 3GPP TS 24.543 clause A.4.3.3.2.1 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.8 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-creation-res-info+cbor

Type name: application

Subtype name: application/vnd.3gpp.seal-data-delivery-data-storage-creation-res-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "DataStorageCreationResponse" data type in 3GPP TS 24.543 clause A.4.3.3.2.2 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.9 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-reservation-req-info+cbor

Type name: application

Subtype name: application/vnd.3gpp.seal-data-delivery-data-storage-reservation-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "DataStorageReservationRequest" data type in 3GPP TS 24.543 clause A.4.3.3.2.3 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.10 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-reservation-res-info+cbor

Type name: application

Subtype name: application/vnd.3gpp.seal-data-delivery-data-storage-reservation-res-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "DataStorageReservationResponse" data type in 3GPP TS 24.543 clause A.4.3.3.2.4 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.11 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-status-notification-info+cbor

Type name: application

Subtype name: application/vnd.3gpp.seal-data-delivery-data-storage-status-notification-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "DataStorageStatusNotification" data type in 3GPP TS 24.543 clause A.4.3.3.2.5 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.12 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-query-res-info+cbor

Type name: application

Subtype name: application/vnd.3gpp.seal-data-delivery-data-storage-query-res-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "DataStorageQueryResponse" data type in 3GPP TS 24.543 clause A.4.3.3.2.6 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

### A.4.2.13 Media Type registration template for application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor

Type name: application

Subtype name: application/vnd.3gpp.seal-data-delivery-data-storage-mgt-req-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [20]. See "DataStorageQueryRequest" data type in 3GPP TS 24.543 clause A.4.3.3.2.7 for details.

Security considerations: See Section 10 of IETF RFC 8949 [20] and Section 11 of IETF RFC 7252 [14].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.543 "Data Delivery Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL data delivery management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [20]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP\_TSG\_CT\_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

Annex B (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2023-03 | CT1#140 | C1-230388 |  |  |  | Draft skeleton provided by the rapporteur. | 0.0.0 |
| 2023-03 | CT1#140 | C1-230389  C1-230394  C1-230395  C1-230868  C1-230869  C1-230870  C1-230871  C1-230872 |  |  |  | Implementing the following p-CRs agreed by CT1: C1-230389, C1-230394, C1-230395, C1-230868, C1-230869, C1-230870, C1-230871, C1-230872; and editorial changes from the rapporteur. | 0.1.0 |
| 2023-10 | CT1#144 | C1-237196  C1-237283  C1-237546  C1-237607  C1-237654  C1-237692  C1-238061  C1-238062  C1-238063  C1-238064  C1-238065  C1-238066  C1-238067  C1-238068  C1-238070  C1-238071  C1-238072  C1-238073  C1-238075  C1-238198 |  |  |  | Implementing the following p-CRs agreed by CT1: C1-237196, C1-237283, C1-237546, C1-237607, C1-237654, C1-237692, C1-238061, C1-238062, C1-238063, C1-238064, C1-238065, C1-238066, C1-238067, C1-238068, C1-238069, C1-238070, C1-238071, C1-238072, C1-238073, C1-238075, C1-238198; and editorial changes from the rapporteur. | 0.2.0 |
| 2023-11 | CT1#145 | C1-238643  C1-238644  C1-238649  C1-238650  C1-238656  C1-238657  C1-238658  C1-238659  C1-238660  C1-238661  C1-238663  C1-238664  C1-238665  C1-238666  C1-238667  C1-238674  C1-238675  C1-238676  C1-238677  C1-238678  C1-238679  C1-238680  C1-239159  C1-239400  C1-239401  C1-239402  C1-239403  C1-239494  C1-239405  C1-239408  C1-239409  C1-239410  C1-239411  C1-239412  C1-239414  C1-239571  C1-239577  C1-239578 |  |  |  | Implementing the following p-CRs agreed by CT1: C1-238643, C1-238644, C1-238649, C1-238650, C1-238656, C1-238657, C1-238658, C1-238659, C1-238660, C1-238661, C1-238663, C1-238664, C1-238665, C1-238666, C1-238667, C1-238674, C1-238675, C1-238676, C1-238677, C1-238678, C1-238679, C1-238680, C1-239159, C1-239400, C1-239401, C1-239402, C1-239403, C1-239404, C1-239405, C1-239408, C1-239409, C1-239410, C1-239411, C1-239412, C1-239414, C1-239571, C1-239577, C1-239578; and editorial changes from the rapporteur. | 0.3.0 |
| 2023-11 | CT#102 | CP-233156 |  |  |  | Version 1.0.0 created for presentation to TSG CT#102 for information. | 1.0.0 |
| 2024-01 | CT1#146 | C1-240234  C1-240252  C1-240280  C1-240309  C1-240310  C1-240311  C1-240312  C1-240313  C1-240314  C1-240317  C1-240318  C1-240401 |  |  |  | Implementing the following p-CRs agreed by CT1: C1-240234, C1-240252, C1-240280, C1-240309, C1-240310, C1-240311, C1-240312, C1-240313, C1-240314, C1-240317, C1-240318, C1-240401; and editorial changes from the rapporteur. | 1.1.0 |
| 2024-03 | CT1#147 | C1-240808  C1-240809  C1-240817  C1-240818  C1-240824  C1-240825  C1-240826  C1-241537  C1-241538  C1-241539  C1-241540  C1-241541  C1-241543  C1-241544  C1-241545  C1-241546  C1-241547  C1-241617  C1-241631  C1-241632 |  |  |  | Implementing the following p-CRs agreed by CT1: C1-240808, C1-240809, C1-240817, C1-240818, C1-240824, C1-240825, C1-240826, C1-241537, C1-241538, C1-241539, C1-241540, C1-241541, C1-241543, C1-241544, C1-241545, C1-241546, C1-241547, C1-241617, C1-241631, C1-241632; and editorial changes from the rapporteur. | 1.2.0 |
| 2024-04 | CT1#148 | C1-242099  C1-242101  C1-242102  C1-242105  C1-242107  C1-242373  C1-242374  C1-242381  C1-242382  C1-242385  C1-242386  C1-242397  C1-242471  C1-242492  C1-242763  C1-242764  C1-242765  C1-242766  C1-242767  C1-242768  C1-242769  C1-242770 |  |  |  | Implementing the following p-CRs agreed by CT1: C1-242099, C1-242101, C1-242102, C1-242105, C1-242107, C1-242373, C1-242374, C1-242381, C1-242382, C1-242385, C1-242386, C1-242397, C1-242471, C1-242492, C1-242763, C1-242764, C1-242765, C1-242766, C1-242767, C1-242768, C1-242769, C1-242770; and editorial changes from the rapporteur. | 1.3.0 |
| 2024-06 | CT1#149 | C1-243257  C1-243271  C1-243274  C1-243285  C1-243287  C1-243292  C1-243309  C1-243735  C1-243736  C1-243737  C1-243738  C1-243739  C1-243740  C1-243741  C1-243741  C1-243742  C1-243743  C1-243744  C1-243745  C1-243746  C1-243747  C1-243748  C1-243749  C1-243750  C1-243751  C1-243775 |  |  |  | Implementing the following p-CRs agreed by CT1: C1-243257, C1-243271, C1-243274, C1-243285, C1-243287, C1-243292, C1-243309, C1-243735, C1-243736, C1-243737, C1-243738, C1-243739, C1-243740, C1-243741, C1-243742, C1-243743, C1-243744, C1-243745, C1-243746, C1-243747, C1-243748, C1-243749, C1-243750, C1-243751, C1-243776; and editorial changes from the rapporteur. | 1.4.0 |
| 2024-06 | CT#104 | CP-241145 |  |  |  | Version 2.0.0 created for presentation to TSG CT#104 for approval. | 2.0.0 |