ETSI TS 123 438 V19.3.0 (2026-02)

TECHNICAL SPECIFICATION

5G;
Service Enabler Architecture Layer for Verticals (SEAL);
Digital assets
(3GPP TS 23.438 version 19.3.0 Release 19)

Reference
RTS/TSGS-0623438vj30

Keywords
5G

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

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

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

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

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

can indicates that something is possible

cannot indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

Introduction

Users can be associated with one or more digital assets like Avatars, software licenses, files, etc. Applications like mobile metaverse services can utilize the digital assets related to users, and the users can benefit from having the use of their digital assets between the various metaverse applications/platforms in an interoperable way. Digital assets service enables such management and usage of digital assets in a secure and controllable way.

The requirements for Digital asset management are specified in 3GPP TS 22.156 [2]. The present document specifies the stage 2 level details like architectural requirements, architecture, procedures and APIs for digital asset service.

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

1 Scope

The present document specifies the application layer architecture, procedures and information flows necessary for digital asset service to support mobile metaverse services. It includes architectural requirements, application layer architecture fulfilling the architecture requirements and procedures to manage digital assets.

The normative work in the present document is based on the requirements as defined in 3GPP TS 22.156 [2].

NOTE: In the current release of this specification, the digital asset type is limited to digital avatar. Other types of digital asset are for the consideration of future release.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.156: "Mobile Metaverse Services".

[3] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

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

[5] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

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].

Digital asset profile: It is a digital asset specific configuration and parameters (e.g. allowed locations) applicable to one or more application(s). The digital asset profile may be associated with one or more VAL user(s). In this release, avatar is considered as a digital asset.

Digital asset identifier: A digital asset identifier is used to uniquely identify a digital asset across different mobile metaverse services.

For the purposes of the present document, the following terms given in 3GPP TS 22.156 [2] apply:

Avatar

digital asset

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].

CAPIF	Common API Framework for 3GPP northbound APIs
DA	Digital Asset
SEAL	Service Enabler Architecture Layer for verticals
VAL	Vertical Application Layer

4 Overview

4.1 General

This clause provides an overview of the features supported by digital asset service. The digital asset service is supported for both IMS and non-IMS communication. In this specification, the digital asset is implemented as a combination of digital asset profile along with associated media to represent the asset. The digital asset service supports the following features:

- Management of digital assets profile
- Management of digital asset media
- Discovery of digital assets

4.2 Digital asset profile management

The digital asset profile management feature is specified in clause 8.2. It enables a consumer (VAL server or DA client) of digital asset service to be able to manage (CRUD) a digital asset profile. This is a necessary feature to make a digital asset exposure via the digital asset service.

4.3 Digital asset discovery

The digital asset profile discovery feature is specified in clause 8.3. It enables a DA client to discover digital assets available in the digital asset service.

4.4 Digital asset media management

The digital asset media management feature is specified in clause 8.4. It enables a consumer (VAL server or DA client) of digital asset service to manage the media related to digital asset profile.

5 Architectural requirements

5.1 General

This clause specifies the architectural requirements for digital asset service.

5.2 Digital asset profile management requirements

This clause specifies the requirements for digital asset profile management.

[AR-5.2-a] The digital asset service shall provide mechanisms to support management (CRUD) of digital assets profiles.

[AR-5.2-b] Void

[AR-5.2-c] The digital asset service shall provide mechanisms to control access to digital assets by one or more users other than the owner of the digital asset.

[AR-5.2-d] The digital asset service shall provide mechanisms to control access to digital assets by one or more applications.

5.3 Digital asset discovery requirements

This clause specifies the requirements for digital asset discovery.

[AR-5.3-a] The digital asset service shall provide mechanisms to support discovery of digital assets.

5.4 Digital asset media management requirements

This clause specifies the requirements for digital asset media management.

[AR-5.4-a] The digital asset service shall provide mechanisms to upload/store the digital asset media corresponding to a digital asset profile.

[AR-5.4-b] The digital asset service shall provide mechanisms to download the digital asset media corresponding to authorized users of the digital asset.

6 Architecture

6.1 General

The digital asset service architecture enables the digital asset service capabilities and resources to be offered as APIs to be consumed by the VAL services deployed in the network and to be consumed by the VAL services and DA clients deployed on the UE. The different architecture representations are specified in this clause.

6.2 Architecture description

Figure 6.2-1 illustrates the digital asset service architecture to support Metaverse services using SEAL architecture specified in 3GPP TS 23.434 [4].

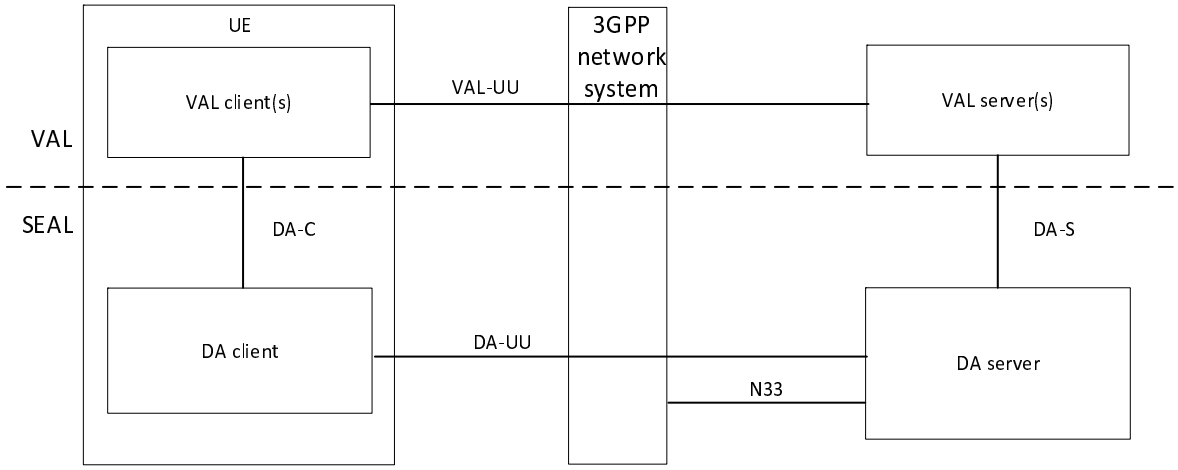

Figure 6.2-1: Digital asset service architecture to support Metaverse services using SEAL architecture

The SEAL architecture includes DA client and server which supports the VAL layer. The DA server interacts with the VAL server(s) over the DA-S reference point. The DA client interacts with the VAL client(s) over the DA-C reference point. The interactions between DA client and DA server is over the DA-UU reference point. The DA server may utilize the 5GC services over N33 reference point. The DA client may be located within the VAL client(s) in which case the DA-C reference point will be internal to VAL client(s). The service APIs offered by DA server on DA-UU and DA-S to the VAL layer functions (via DA client) follow the service-based architecture as shown in the figure 6.2-3.

Figure 6.2-2 illustrates the service-based SEAL architecture for digital asset service to support Metaverse services.

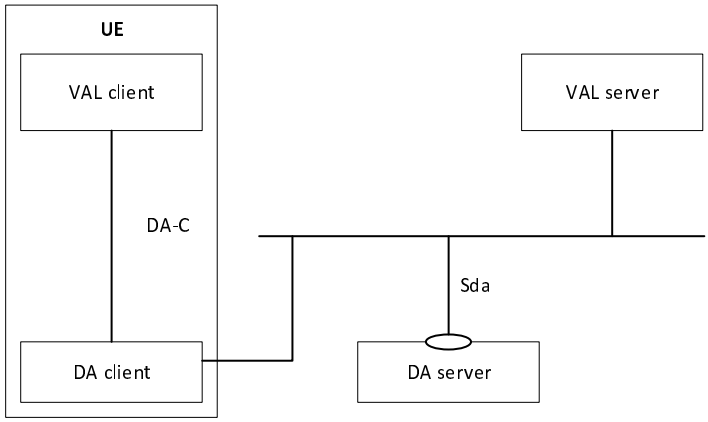

Figure 6.2-2: Service-based SEAL architecture for digital asset service to support Metaverse services

The DA server exposes the APIs over the Sda interface to the VAL layer. The VAL functions (VAL clients and servers) and the DA client (serving a VAL client) consume the services by interacting on the Sda interface of the DA server. The CAPIF as specified in 3GPP TS 23.222 [3] can be used by VAL functions to discover the services of the DA server.

6.3 Functional elements

6.3.1 DA client

The following capabilities are supported by the DA client:

- Supports the client-side functionalities for digital asset profile create, update, retrieve and delete operations.
- Supports the client-side functionalities for digital asset discovery.

6.3.2 DA server

The following capabilities are supported by the DA server:

- Supports the functionalities for digital asset profile create, update, retrieve and delete operations.
- Supports the functionalities for digital asset discovery.

NOTE: The DA server as specified in this specification supports the Base Avatar Repository (BAR) (related to avatar communications) as specified in 3GPP TS 23.228 [5].

6.4 Reference points

6.4.1 DA-C

This reference point supports the interactions between VAL client(s) and DA client.

6.4.2 DA-UU

This reference point supports the interactions between DA client(s) and DA server. The DA client can consume the digital asset services supported by the DA server as specified in clause 6.3.2.

6.4.3 DA-S

This reference point supports the interactions between VAL server(s) and DA server. The VAL server consumes the digital asset services supported by the DA server as specified in clause 6.3.2.

6.5 Service-based interface

6.5.1 Sda

This interface supports the interactions between VAL function (VAL servers) and DA server. The VAL function consumes the digital asset service as specified in clause 6.3.2.

7 Identities and commonly used information

7.1 General

This clause specifies details about the identifiers and common values used for digital asset service.

7.2 Digital asset profile

The digital asset profile includes the information elements about the attributes of a single digital asset. Table 7.2-1 shows the information elements for the digital asset profile.

NOTE 1: In this release, the digital asset profile is specified considering Avatar as a digital asset of the user.

Table 7.2-1: Digital asset profile

Information element	Status	Description
Digital asset ID	M	Identifier of the digital asset profile
Digital asset type	M	Type of the digital asset. (For this release, it contains "Avatar").
List of owners	M	List of identity of the owner user(s) who created the digital asset.
Digital asset name	O	The name of the digital asset
Digital asset description	O	The description on the digital asset
List of service provider identifiers	O	List of service providers for the digital asset.
access control list	O	List of tuples indicating the requestors allowed to perform operations with this digital asset and the allowed operation types.
> allowed user list	O	List of users allowed to access this digital asset
>> allowed operations	O	List of operations allowed by this user. Possible operations are (one or more of) : Discovery, Retrieve, Update, Delete
>> list of predictive models	O	For each allowed user, list of one or more predictive model for the user, in order to predict user's behaviour.
current status	O	Current status (in use or not) of the profile
spatial conditions	O	List of spatial conditions (e.g. locations) where this digital asset profile is allowed to be accessed
> current location	O	Current location where the profile is being used
allowed application list	O	List of application IDs which are allowed to use this digital asset profile
associated accessories identifiers	O	List of digital asset identifiers which are accessories (e.g. Hat, watch, shoes) purchased for this digital asset profile
expiry time	O	Time until this digital asset profile is valid
History information	O	Usage history for this digital asset profile
> list of locations	O	List of locations where the digital asset profile is used.
> time of use	O	Time information when the digital asset profile is used
> list of applications	O	List of the application IDs which used this digital asset profile.
List of digital asset media	O	List of digital asset media
> Media URI	O (NOTE 1)	URI where the media is stored
> Media object	O (NOTE 1)	Media object (e.g. JPG file)
Digital signature	O	The digital signature of this digital asset, signed by the DA server
NOTE 1: One of the IE shall be included NOTE 2: The provisioning of the certificate of the DA server and generation and usage of the digital signature at DA server are left for implementation		

7.3 Void

7.4 Identities

7.4.1 General

Following identifies as defined in clause 7 of 3GPP TS 23.434 [4] are applicable for this specification too.

- User ID
- VAL user ID

- VAL UE ID
- VAL service ID

7.4.2 Identities related to digital asset

7.4.2.1 Digital asset identifier (Digital asset ID)

A unique identifier to identify digital asset. A digital asset has only one digital asset profile, the digital asset identifier is also used to uniquely identify the digital asset profile of the digital asset. It is assigned by SEAL DA server. The identity is globally unique.

7.4.2.2 Void

8 Procedures and information flows

8.1 General

8.2 Digital asset profile management

8.2.1 General

The following clauses specify procedures, information flows, and APIs for digital asset profile management.

8.2.2 Procedures

8.2.2.1 Digital asset profile create

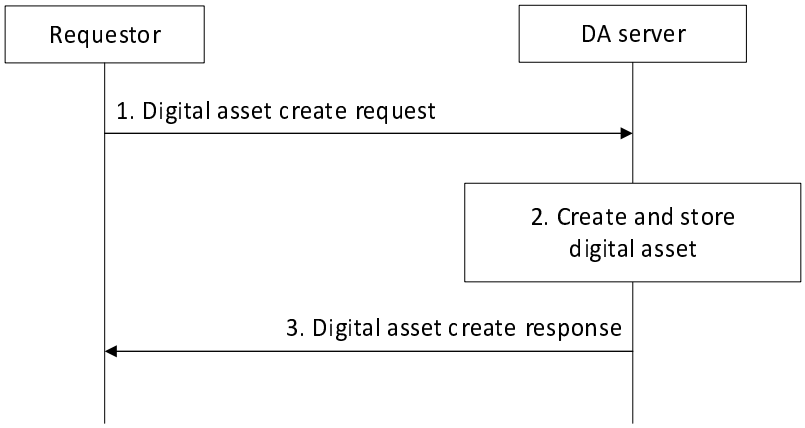

Figure 8.2.2.1-1: Digital asset profile create

1. A requestor (e.g. DA client) sends a digital asset create request to the DA server. The request includes information listed in Table 8.2.3.1-1.
2. The DA server authenticates and authorizes the request. If authorized, the DA server creates the digital asset profile (as per clause 7.2), assigns globally unique digital asset identifier and stores the information about the digital asset profile in a local repository.
3. The DA server generates and sends a response to the requestor. The response includes information listed in Table 8.2.3.2-1.

8.2.2.2 Digital asset profile retrieve

The digital asset retrieve procedure obtains information about the digital asset and is different from digital asset discovery.

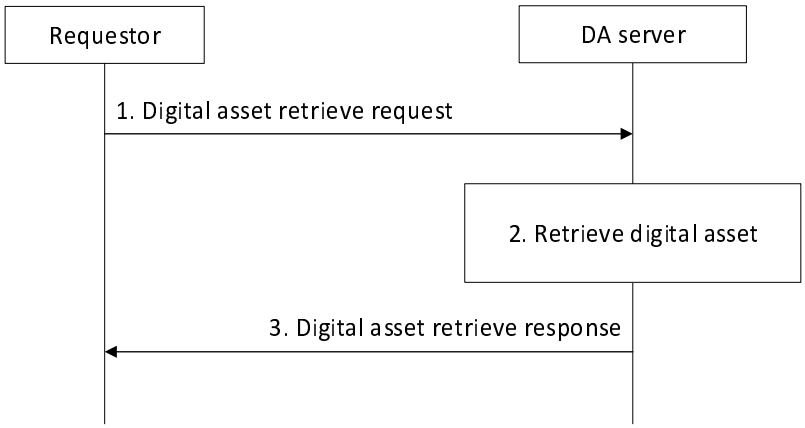

Figure 8.2.2.2-1: Digital asset profile retrieve

1. A requestor (e.g. DA client) sends a digital asset retrieve request to the DA server. The request includes information listed in Table 8.2.3.3-1.
2. The DA server authenticates and authorizes the request. If authorized, the DA server retrieves the digital asset from the local repository.
3. The DA server generates and sends a response to the requestor. The response includes information listed in Table 8.2.3.4-1.

8.2.2.3 Digital asset profile update

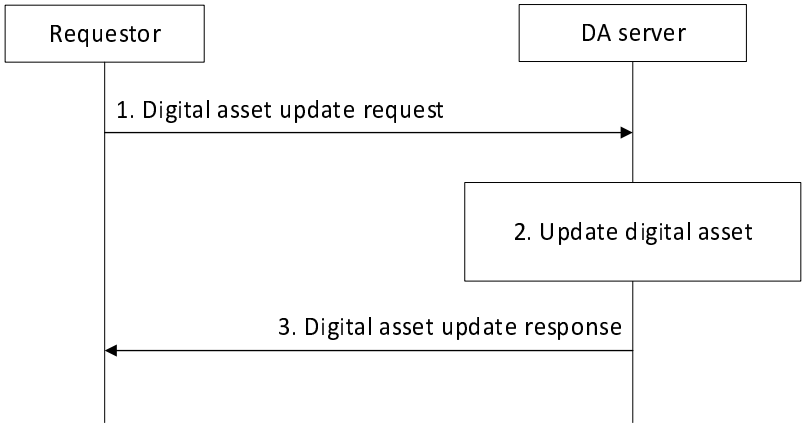

Figure 8.2.2.3-1: Digital asset profile update

1. A requestor (e.g. DA client) sends a digital asset update request to the DA server. The request includes information listed in Table 8.2.3.5-1.
2. The DA server authenticates and authorizes the request. If authorized, the DA server updates information about the digital asset in the local repository.
3. The DA server generates and sends a response to the requestor. The response includes information listed in Table 8.2.3.6-1.

8.2.2.4 Digital asset profile delete

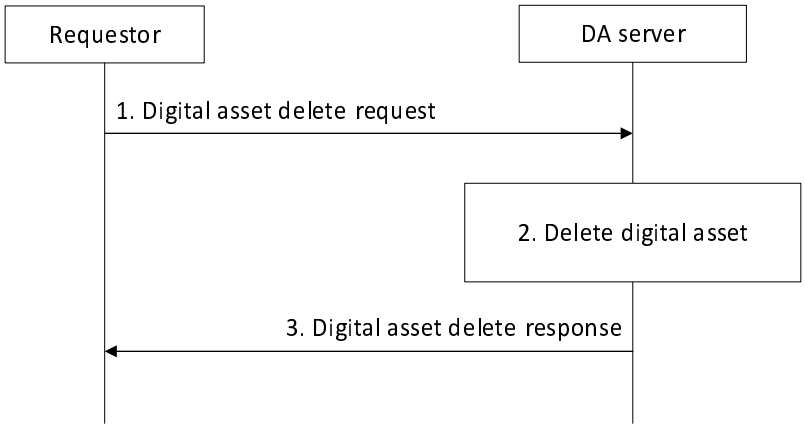

Figure 8.2.2.4-1: Digital asset profile delete

1. A requestor (e.g. DA client) sends a digital asset delete request to the DA server. The request includes information listed in Table 8.2.3.7-1.
2. The DA server authenticates and authorizes the request. If authorized, the DA server deletes the digital asset from the local repository.
3. The DA server generates and sends a response to the requestor. The response includes information listed in Table 8.2.3.8-1.

8.2.3 Information flows

8.2.3.1 Digital asset profile create request

Table 8.2.3.1-1 describes the information elements for a digital asset profile create request sent from a requestor (e.g. DA client) to a DA server.

Table 8.2.3.1-1: Digital asset profile create request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset profile parameters	M	Parameters to create digital asset profile

Table 8.2.3.1-2: Parameters for digital asset profile

Information element	Status	Description
Digital asset owner identifier(s)	M	A list of identifier(s) for the digital asset owner.
Digital asset type	M	The type of digital asset, e.g. avatar, wallet, etc.
Digital asset name	O	The name of the digital asset
Digital asset description	O	The description on the digital asset
List of service provider identifiers	O	List of service providers for the digital asset.
access control list	O	List of tuples indicating the requestors allowed to perform operations with this digital asset and the allowed operation types.
> allowed user list	O	List of users allowed to access this digital asset
>> allowed operations	O	List of operations allowed by this user. Possible operations are (one or more of) : Discovery, Retrieve, Update, Delete
>> list of predictive models	O	For each allowed user, list of one or more predictive model for the user, in order to predict user's behaviour.
spatial conditions	O	List of spatial conditions (e.g. locations) where this digital asset profile is allowed to be accessed
> current location	O	Current location where the profile is being used
allowed application list	O	List of application IDs which are allowed to use this digital asset profile
associated accessories identifiers	O	List of digital asset identifiers which are accessories (e.g. Hat, watch, shoes) purchased for this digital asset profile
expiry time	O	Time until this digital asset profile is valid

Editor's Note: The association of a subscriber/user identifier for the digital asset is FFS.

8.2.3.2 Digital asset profile create response

Table 8.2.3.2-1 describes the information elements for the digital asset profile create response sent from a DA server to a requestor (e.g. DA client).

Table 8.2.3.2-1: Digital asset profile create response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure code may be provided.
Digital asset identifier	M	An identifier for the digital asset.
Digital asset media upload endpoint	M	The end point provided by DA server at which digital asset media is to be uploaded.

8.2.3.3 Digital asset profile retrieve request

Table 8.2.3.3-1 describes the information elements for the digital asset profile retrieve request sent from a requestor (e.g. DA client) to a DA server.

Table 8.2.3.3-1: Digital asset profile retrieve request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	M	An identifier for the digital asset.

8.2.3.4 Digital asset profile retrieve response

Table 8.2.3.4-1 describes the information elements for the digital asset profile retrieve response sent from a DA server to a requestor (e.g. DA client).

Table 8.2.3.4-1: Digital asset profile retrieve response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure code may be provided.
Digital asset profile	M	The digital asset profile as specified in clause 7.2.

8.2.3.5 Digital asset profile update request

Table 8.2.3.5-1 describes the information elements for the digital asset profile update request sent from a requestor (e.g. DA client) to a DA server.

Table 8.2.3.5-1: Digital asset profile update request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	M	An identifier for the digital asset.
Digital asset profile parameters	M	The digital asset profile parameters as specified in Table 8.2.3.1-2.

8.2.3.6 Digital asset profile update response

Table 8.2.3.6-1 describes the information elements for the digital asset profile update response sent from a DA server to a requestor (e.g. DA client).

Table 8.2.3.6-1: Digital asset profile update response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure code may be provided.

8.2.3.7 Digital asset profile delete request

Table 8.2.3.7-1 describes the information elements for the digital asset profile delete request sent from a requestor (e.g. DA client) to a DA server.

Table 8.2.3.7-1: Digital asset profile delete request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	M	An identifier for the digital asset.

8.2.3.8 Digital asset profile delete response

Table 8.2.3.8-1 describes the information elements for the digital asset profile delete response sent from a DA server to a requestor (e.g. DA client).

Table 8.2.3.8-1: Digital asset profile delete response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure code may be provided.

8.2.4 APIs

8.2.4.1 General

Table 8.2.4.1-1 illustrates the SEAL APIs for digital asset profile management.

Table 8.2.4.1-1: List of SEAL APIs for digital asset profile management

API Name	API Operations	Known Consumer(s)	Communication Type
SS_DAProfileManagement	Create	DA client, VAL server	Request/Response
	Retrieve	DA client, VAL server	
	Update	DA client, VAL server	
	Delete	DA client, VAL server	

8.2.4.2 SS_DAProfileManagement API

8.2.4.2.1 General

Service description: This API enables a VAL server (or DA client) to manage digital asset profile on a DA server.

8.2.4.2.2 Create operation

API operation name: SS_DAProfileManagement_Create

Description: The consumer requests to create digital asset profiles.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.2.3.1-1.

Outputs: See Table 8.2.3.2-1.

See clause 8.2.2.1 for details of usage of this operation.

8.2.4.2.3 Retrieve operation

API operation name: SS_DAProfileManagement_Retrieve

Description: The consumer requests to retrieve digital asset profiles.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.2.3.3-1.

Outputs: See Table 8.2.3.4-1.

See clause 8.2.2.2 for details of usage of this operation.

8.2.4.2.4 Update operation

API operation name: SS_DAProfileManagement_Update

Description: The consumer requests to update digital asset profiles.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.2.3.5-1.

Outputs: See Table 8.2.3.6-1.

See clause 8.2.2.3 for details of usage of this operation.

8.2.4.2.5 Delete operation

API operation name: SS_DAProfileManagement_Delete

Description: The consumer requests to delete digital asset profiles.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.2.3.7-1.

Outputs: See Table 8.2.3.8-1.

See clause 8.2.2.4 for details of usage of this operation.

8.3 Digital asset discovery

8.3.1 General

The following clauses specify procedures, information flows, and APIs for digital asset discovery.

8.3.2 Procedure

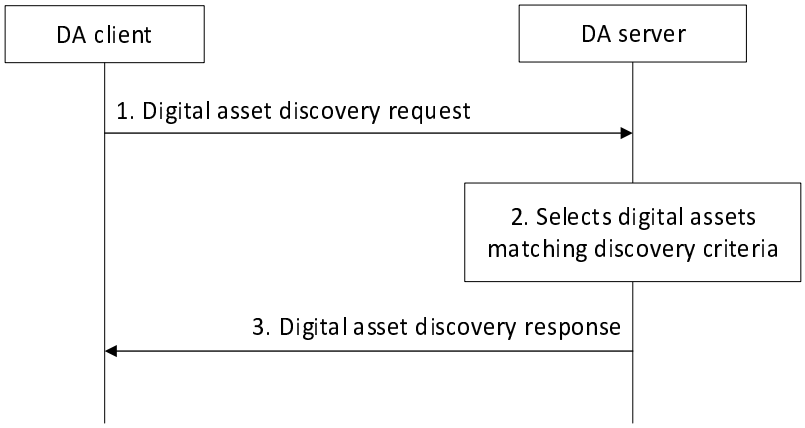

Figure 8.3.2.1-1: Digital asset discovery

1. A DA client sends a digital asset discovery request to the DA server. The request includes information listed in Table 8.3.3.1-1.
2. The DA server authenticates and authorizes the request. If authorized, the DA server applies the discovery criteria to discover digital assets from the local repository.
3. The DA server generates and sends a response to the requestor. The response includes information listed in Table 8.3.3.2-1.

8.3.3 Information flows

8.3.3.1 Digital asset discovery request

Table 8.3.3.1-1 describes the information elements for a digital asset discovery request sent from a requestor (e.g. DA client or VAL server) to a DA server.

Table 8.3.3.1-1: Digital asset discovery request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	O NOTE	The identifier of the digital asset.
Digital asset discovery filters	O NOTE	Set of characteristics to determine matching digital asset (e.g., Digital asset name, Digital asset description, location, Digital asset type, Digital asset owner, Allowed user, Digital asset profile).
NOTE: At least one of the information elements shall be present		

8.3.3.2 Digital asset discovery response

Table 8.3.3.2-1 describes the information elements for the digital asset discovery response sent from a DA server to a requestor (e.g. DA client or VAL server).

Table 8.3.3.2-1: Digital asset discovery response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure code may be provided.
Discovery results	M	List of discovery results matching the discovery criteria.
>Digital asset identifier	O (NOTE)	Identifier of the digital asset matching the discovery criteria.
>Digital asset name	O (NOTE)	Name of the digital asset matching the discovery criteria.
>URL	O	A URL of the service provider the digital asset is associated with.
>Digital asset status	M	Status of the digital asset.
>Digital asset descriptions	O	Description of the digital asset.
NOTE: At least one of the information elements must be present.		

8.3.4 APIs

8.3.4.1 General

Service description: This API enables a DA client to discover digital assets from a DA server.

8.3.4.2 Discovery operation

API operation name: SS_DADiscovery

Description: The consumer requests to discover digital assets.

Known Consumers: DA client.

Inputs: See Table 8.3.3.1-1.

Outputs: See Table 8.3.3.2-1.

See clause 8.3.2 for details of usage of this operation.

8.4 Digital asset media management

8.4.1 General

The following clauses specify procedures, information flows, and APIs for digital asset media management.

8.4.2 Procedures

8.4.2.1 Upload digital asset media

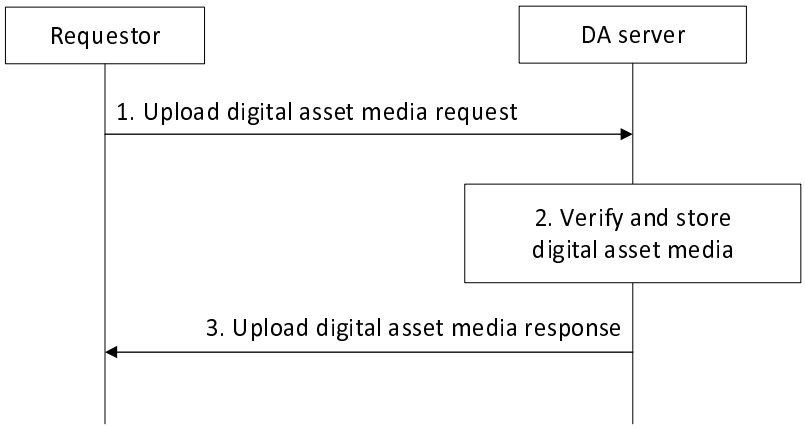

Figure 8.4.2.1-1: Upload digital asset media

1. A requestor (e.g. DA client) sends an upload digital asset media request to the DA server (at the digital asset media upload endpoint). The request includes information listed in Table 8.4.3.1-1.
2. The DA server authenticates and authorizes the request and verifies the digital asset identifier. If authorized, the DA server receives the media object or media URI corresponding to the digital asset profile, stores the media or the information about the digital asset media.
3. The DA server sends an upload digital asset media response to the requestor. The response includes information listed in Table 8.4.3.2-1.

8.4.2.2 Download digital asset media

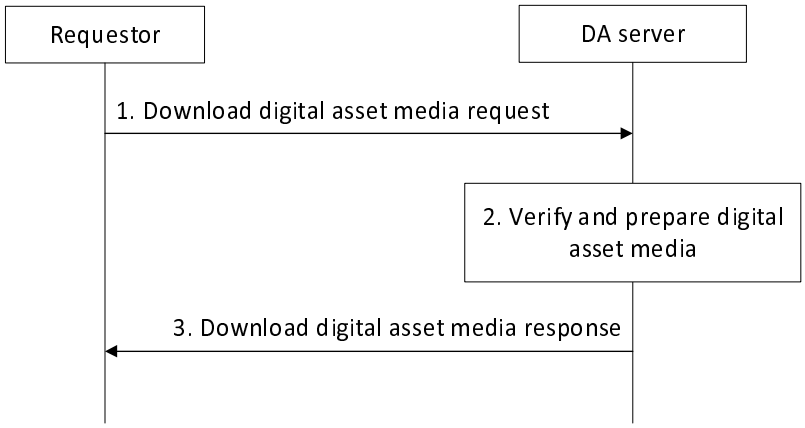

Figure 8.4.2.2-1: Download digital asset media

1. A requestor (e.g. DA client) sends a download digital asset media request to the DA server. The request includes information listed in Table 8.4.3.3-1.

2. The DA server authenticates and authorizes the request and verifies the digital asset identifier. If authorized, the DA server determines the digital asset media as per the information provided in step 1.

3. The DA server sends a download digital asset media response to the requestor. The response includes information listed in Table 8.4.3.4-1.

8.4.2.3 Update digital asset media

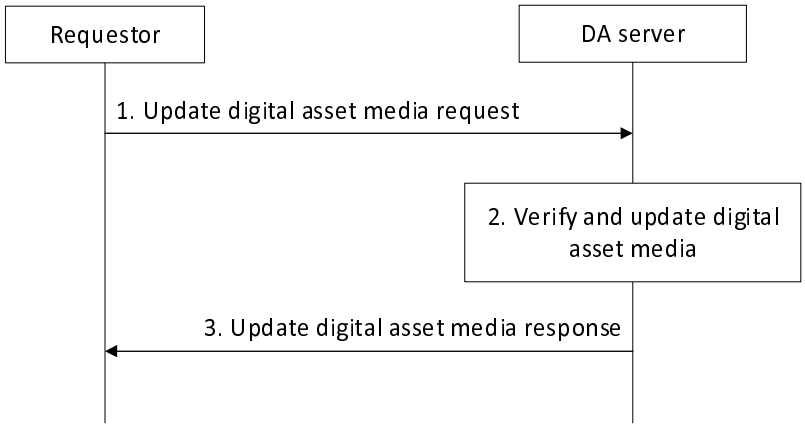

Figure 8.4.2.3-1: Update digital asset media

1. A requestor (e.g. DA client) sends an update digital asset media request to the DA server. The request includes information listed in Table 8.4.3.5-1.

2. The DA server authenticates and authorizes the request and verifies the digital asset identifier. If authorized, the DA server receives the media object or media URI corresponding to the digital asset profile, updates the existing media or the information about the digital asset media corresponding to the digital asset identifier.

3. The DA server sends an update digital asset media response to the requestor. The response includes information listed in Table 8.4.3.6-1.

8.4.2.4 Delete digital asset media

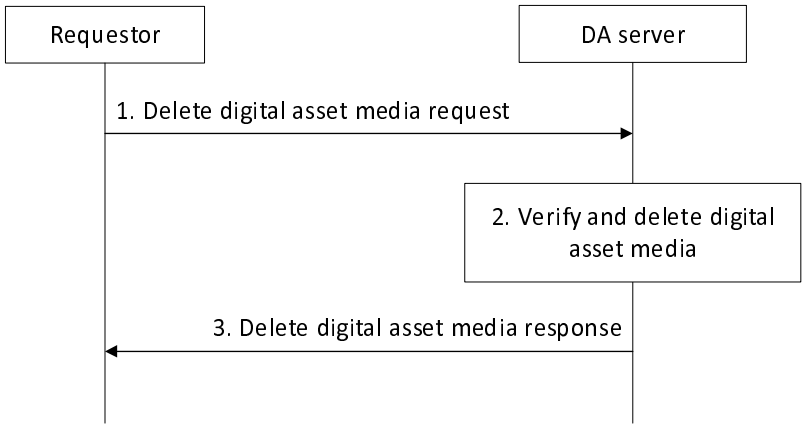

Figure 8.4.2.4-1: Delete digital asset media

1. A requestor (e.g. DA client) sends a delete digital asset media request to the DA server. The request includes information listed in Table 8.4.3.7-1.

2. The DA server authenticates and authorizes the request and verifies the digital asset identifier. If authorized, the DA server deletes the existing media or the information about the digital asset media corresponding to the digital asset identifier.

3. The DA server sends a delete digital asset media response to the requestor. The response includes information listed in Table 8.4.3.8-1.

8.4.3 Information flows

8.4.3.1 Upload digital asset media request

Table 8.4.3.1-1 describes the information elements for an upload digital asset media request sent from a requestor (e.g. DA client) to a DA server.

Table 8.4.3.1-1: Upload digital asset media request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	M	Identifier of the digital asset profile
List of digital asset media	M	List of digital asset media to be uploaded
> Media URI (NOTE)	O	URI where the media is stored
> Media object (NOTE)	O	Media object (e.g. JPG file)
NOTE: One of the IE shall be included		

8.4.3.2 Upload digital asset media response

Table 8.4.3.2-1 describes the information elements for the upload digital asset media response sent from a DA server to a requestor (e.g. DA client).

Table 8.4.3.2-1: Upload digital asset media response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure cause is provided.
Digital asset identifier	M	An identifier for the digital asset.
Cause	O	The cause information when the status is fail.

8.4.3.3 Download digital asset media request

Table 8.4.3.3-1 describes the information elements for the download digital asset media request sent from a requestor (e.g. DA client) to a DA server.

Table 8.4.3.3-1: Download digital asset media request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	M	An identifier for the digital asset.

8.4.3.4 Download digital asset media response

Table 8.4.3.4-1 describes the information elements for the download digital asset media response sent from a DA server to a requestor (e.g. DA client).

Table 8.4.3.4-1: Download digital asset media response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure cause is provided.
Digital asset identifier	M	An identifier for the digital asset.
List of digital asset media	M	List of digital asset media to be downloaded
> Media URI (NOTE)	O	URI where the media is stored
> Media object (NOTE)	O	Media object (e.g. JPG file)
NOTE: One of the IE shall be included		

8.4.3.5 Update digital asset media request

Table 8.4.3.5-1 describes the information elements for an update digital asset media request sent from a requestor (e.g. DA client) to a DA server.

Table 8.4.3.5-1: Update digital asset media request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	M	Identifier of the digital asset profile
List of digital asset media	M	List of digital asset media to be updated
> Media URI (NOTE)	O	URI where the media is stored
> Media object (NOTE)	O	Media object (e.g. JPG file)
NOTE: One of the IE shall be included		

8.4.3.6 Update digital asset media response

Table 8.4.3.6-1 describes the information elements for the update digital asset media response sent from a DA server to a requestor (e.g. DA client).

Table 8.4.3.6-1: Update digital asset media response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure cause is provided.
Digital asset identifier	M	An identifier for the digital asset.
Cause	O	The cause information when the status is fail.

8.4.3.7 Delete digital asset media request

Table 8.4.3.7-1 describes the information elements for a delete digital asset media request sent from a requestor (e.g. DA client) to a DA server.

Table 8.4.3.7-1: Delete digital asset media request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor.
Security credentials	M	Security credentials to authenticate and authorize the requestor.
Digital asset identifier	M	Identifier of the digital asset profile
List of digital asset media	M	List of digital asset media to be deleted
> Media URI	O (NOTE)	URI where the media is stored
> Media object	O (NOTE)	Media object (e.g. JPG file)
NOTE: One of the IE shall be included		

8.4.3.8 Delete digital asset media response

Table 8.4.3.6-1 describes the information elements for the delete digital asset media response sent from a DA server to a requestor (e.g. DA client).

Table 8.4.3.8-1: Delete digital asset media response

Information element	Status	Description
Status	M	A status for the request: success, fail. If the status is fail, a failure cause is provided.
Digital asset identifier	M	An identifier for the digital asset.
Cause	O	The cause information when the status is fail.

8.4.4 APIs

8.4.4.1 General

Table 8.4.4.1-1 illustrates the APIs for managing media related to digital asset profile.

Table 8.4.4.1-1: List of APIs for media management for digital asset

API Name	API Operations	Known Consumer(s)	Communication Type
SS_DAMediaManagement	Upload	DA client, VAL server	Request/Response
	Download	DA client, VAL server	
	Update	DA client, VAL server	
	Delete	DA client, VAL server	

8.4.4.2 SS_DAMediaManagement API

8.4.4.2.1 General

Service description: This API enables a VAL server (or DA client) to manage media related to digital asset profile on a DA server.

8.4.4.2.2 Upload operation

API operation name: SS_DAMediaManagement_Upload

Description: The consumer requests to upload media related to digital asset.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.4.3.1-1.

Outputs: See Table 8.4.3.2-1.

See clause 8.4.2.1 for details of usage of this operation.

8.4.4.2.3 Download operation

API operation name: SS_DAMediaManagement_Download

Description: The consumer requests to retrieve media related to digital asset.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.4.3.3-1.

Outputs: See Table 8.4.3.4-1.

See clause 8.4.2.2 for details of usage of this operation.

8.4.4.2.4 Update operation

API operation name: SS_DAMediaManagement_Update

Description: The consumer requests to update media related to digital asset.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.4.3.5-1.

Outputs: See Table 8.4.3.6-1.

See clause 8.4.2.3 for details of usage of this operation.

8.4.4.2.5 Delete operation

API operation name: SS_DAMediaManagement_Delete

Description: The consumer requests to delete media related to digital asset.

Known Consumers: VAL server, DA client.

Inputs: See Table 8.4.3.7-1.

Outputs: See Table 8.4.3.8-1.

See clause 8.4.2.4 for details of usage of this operation.

Annex A (informative): Deployment models

The digital assets service can support the requirements of the SEAL service deployment models specified in clause 4.2 of 3GPP TS 23.434 [4].

The architecture of digital asset service is based on the SEAL functional model. The digital assets service can support the SEAL service deployment models specified in clause 8 of 3GPP TS 23.434 [4].

Annex B (informative): Business relationships

The digital assets service can be hosted by a SEAL provider and the business relationships specified in clause 5 of 3GPP TS 23.434 [4] can apply to the hosting of digital assets service. The SEAL provider agreement between VAL service provider and SEAL providers can include the context of lawful interactions related to digital assets.

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2024-10	SA6#63					TS skeleton (S6-244146)	0.0.0
2024-10	SA6#63					Implemented the following approved pCRs: S6-244574, S6-244575, S6-244577, S6-244579, S6-244691, S6-244721	0.1.0
2024-11	SA6#64					Implemented the following approved pCRs: S6-245275, S6-245530, S6-245531, S6-245542	0.2.0
2024-12	SA#106	SP-241696				Submitted to SA#106 for information	1.0.0
2025-02	SA6#65					Implemented the following approved pCRs: S6-250036, S6-250411, S6-250412, S6-250413, S6-250414, S6-250415, S6-250416, S6-250257, S6-250263	1.1.0
2025-03	SA#107	SP-250195				Submitted to SA#107 for approval	2.0.0
2025-03	SA#107	SP-250195				MCC Editorial update for publication after TSG SA approval	19.0.0
2025-06	SA#108	SP-250610	0001	1	F	Fix for Digital asset media management	19.1.0
2025-06	SA#108	SP-250610	0002		F	Clarification on digital asset	19.1.0
2025-06	SA#108	SP-250610	0003	1	F	Fix for clause 3.1 & 7.4.2.1	19.1.0
2025-06	SA#108	SP-250610	0005		F	Fix for clause 7.2	19.1.0
2025-06	SA#108	SP-250610	0006		F	Fix for clause 8.3.3.2	19.1.0
2025-06	SA#108	SP-250610	0007		F	Remove for clause 7.3 & 7.4.2.2	19.1.0
2025-06	SA#108	SP-250610	0008	1	F	Fix for Upload digital asset media	19.1.0
2025-06	SA#108	SP-250610	0009	1	F	Fix for Download digital asset media	19.1.0
2025-06	SA#108	SP-250610	0010	1	F	Fix for Update digital asset media	19.1.0
2025-06	SA#108	SP-250610	0011	2	F	Fix for Delete digital asset media	19.1.0
2025-06	SA#108	SP-250610	0013	1	F	Clarification on digital assets	19.1.0
2025-09	SA#109	SP-251061	0016		F	Adding APIs for Digital Asset Media Management	19.2.0
2025-09	SA#109	SP-251061	0017		F	Correction in DA Profile	19.2.0
2026-01	SA#110	SP-251485	0020	1	F	CR on digital asset discovery request message	19.3.0
2026-01	SA#110	SP-251485	0021	1	F	CR on digital asset media	19.3.0
2026-01	SA#110	SP-251485	0022		F	CR on digital asset profile	19.3.0
2026-01	SA#110	SP-251485	0023		F	CR on the description of IE allowed operations	19.3.0
2026-01	SA#110	SP-251485	0028	1	F	Resolving ENs	19.3.0
2026-01	SA#110	SP-251485	0031	2	F	CR on digital assets authentication	19.3.0
2026-01	SA#110	SP-251485	0033	1	F	Remove digital assets collection requirement	19.3.0

History

Version	Date	Status
V19.2.0	January 2026	Publication
V19.3.0	February 2026	Publication