**3GPP TSG-SA WG6 Meeting #62 S6-243447**

**[Maastricht](https://www.3gpp.org//Specification-Groups/" \t "https://www.3gpp.org/_blank), Netherlands, 19th Aug-23rd Aug 2024 Rivision of S6-243104**

Source: China Mobile

Title: Solution for permission control of digital assets

Spec: 3GPP TR 23.700-21

Agenda item: 8.4

Document for: Approval

Contact: Jingwen Liu (liujingwen@chinamobile.com), Yue Liu (liuyueyjy@chinamobile.com)

**1. Introduction**

This pCR provides solution to solve KI#9 (Permission control of digital assets).

**2. Reason for Change**

There is a open issue in KI#9 as following：

- Whether and how to manage the permission control for digital asset, including in across multiple metaverses use case.

It is required to provide solution for above open issues.

**3. Proposal**

It is proposed to agree the following changes to TR 23.700-21 v1.1.0.

\* \* \* First Change \* \* \* \*

## 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 control mode:** In the context of this TR, digital asset control mode is the way in which restricts the consumer operation when they use the digital assets in metaverse services. There are three modes according to different using scenario: strict control, general control, and loose control. Strict control is used for private use, and other users are not allowed to operate them; General control is the situation that some people are allowed to use, it needs to get the owner's authorization before others operate; Loose control is the case of public use, all the consumer can operate digital assets without applying for permission.

\* \* \* Next Change \* \* \* \*

## 7.x Solution #x: Support for permission control of digital assets

### 7.x.1 Solution description

This solution maps to KI#9, achieves permission control on digital assets in the case of digital assets sharing. VAL user uses VAL server to upload a digital asset to A-DACM function. When the other user wants to use the digital asset which is in the A-DACM. Enabler layer controls the operation to the digital asset base on the owner’s consent by DAPM function. The architectural impacts and procedures are described in clause 7.x.2 and clause 7.x.3 respectively.

A-DACM and DAPM are different logical functionalities and have different roles. They may be provided by one provider or different providers. They may be deployed in the a single server or seperate servers. If they are deployed in the same server, the interaction procedure between A-DACM function and DAPM function could be ignored.

### 7.x.2 Architecture Impacts

The solution utilizes the architecture specified in clause 6.4, Option#4. In the architecture DAPM function exposes the APIs to the Vertical Application Layer for service providing.

### 7.x.3 Procedures

#### 7.x.3.1 Digital asset control mode registration

Figure 7.x.3.1-1 illustrates the precedure of digital asset control mode registration. The registration procedure is initiated by the digital asset uploaded. Some digital assets are created for public use, so set up control mode in advance is avoid management costs for public products. The same as the private assets.



Figure 7.x.3.1-1: Procedure for digital asset control mode regristration

1-2. Follow step 1-2 of the procedure in 7.7.1.3. The user, i.e. owner of the digital asset, may creat digital assets(e.g. avatar) on the VAL server, and then the VAL server sends Digital asset upload request to the A-DACM function. The A-DACM processes the necessary authentication and authorization procedures, and stores the digital asset and/or relative information.

3. The A-DACM sends digital asset relative information to DAPM function, including digital asset identifier, owner information.

4. DAPM function stores the information and sends the response to A-DACM.

5. A-DACM function sends upload response to VAL server, include the DAPM address information. The VAL server may forward the response to the user.

6. The owner of the digital asset sends the control mode register request to DAPM via VAL server. The control mode includes user identifier, digital asset ID, control mode information(e.g. strict control or general control or loose control.

7. After necessary authentication and authorization procedures, DAPM function stores the control mode of digital asset operation set by the owner.

8. DAPM function sends control mode setting result to the owner of the digital asset via VAL server to indicate success or failure of the operation. The response includes the result of control mode setting.

Note: If A-DACM and DAPM are realized in the same server, step 3,4 are internal interactions and could be skipped.

#### 7.x.3.2 control mode update

Figure 7.x.3.2-1 illustrates the procedure for update the digital asset control mode. Owner may update the contorl mode of digital asset operation via VAL server or DAPM client.

Pre-condition: The DAPM address has been pre-configured to the owner of digital asset, or obtained by the owner of digital asset from the digital asset upload response



Figure 7.x.3.2-1: Procedure for control mode update

1. Owner of the digital asset sends control mode update request to DAPM by using VAL server or DAPM client to update the control mode of the digital asset. The request includes digital asset ID and control mode.
2. DAPM verifies the owner of the digital asset. If successful, DAPM stores the latest control mode information of the digital asset.
3. DAPM sends control mode update response to the owner of digital asset to indicate success or failure of the setting.

#### 7.x.3.3 Obtain the permission for digital asset operation piror to the service

Figure 7.x.3.3-1 illustrates procedure for obtain the permission for digital asset operation piror to the service. DAPM may authorize the consumer to operate the digital asset based on the owner consent before the service.

Pre-condition: The DAPM address has been pre-configured to the Consmer VAL Server or DAPM client.



Figure 7.x.3.3-1: Obtain the permission for digital asset operation piror to the service

1. Consmer VAL Server or DAPM client sends DAPM function request for the digital asset operation permission. The request includes the digital asset information(e.g. digital asset identifier), consumer information(e.g. consumer identifier), specific operation(e.g. access, update/modification, download etc) and time limitation.

2. DAPM function checks whether owner’s consent is needed for this request. If needed, the DAPM searches the owner information of the digital asset. Otherwise jump to step 7.

3. DAPM sends an Owner consent request to the the VAL server serves the owner of digital asset for the owner’s consent.

4. The VAL Server serves the owner of digital asset gets owner’s consent.

NOTE: The interactions between the the owner of digital asset and the VAL Server serves the owner of digital asset are implementation specific and out of scope of the present document.

5. VAL server serves the owner of digital asset sends the Owner consent response to DAPM to indicate agree or deny of the operation permission. If the request is agreed, the time limitation of the digital asset operation is also included in the response.

6. DAPM stores the consumer’s permission of the digital asset based on the owner’s consent.

7. DAPM sends response to the Consmer VAL server or DAPM client. The response includes the result of the permission request.

#### 7.x.3.4 Permission control of digital asset operation

Figure 7.x.3.4-1 illustrates the procedure to permission control of digital assets operation.

Pre-condition: The DAPM address has been pre-configured to the Consmer VAL Server or DAPM client.



Figure 7.x.3.4-1: Permission control of digital asset operation

1. The consumer VAL Server sends Digital asset operation request to A-DACM function. The request includes digital asset information(e.g. digital asset identifier), consumer information(e.g. consumer identifier), specific operation(e.g. access, update/modification, download etc).

2. A-DACM function sends Authenticate permission request to DAPM to check whether the consumer has the permission.

3. DAPM function checks whether the control mode is general control. If not, jump to step 9.

4. DAPM function verifies the user permition. If successed, jumps to step 9. Otherwise the DAPM searches the owner.

5. DAPM sends Owner consent request to the the VAL server serves the owner of digital asset to request the owner’s consent. The request includes digital asset information, consumer identifier, required operation and time limit.

6. Owner VAL Server serves the owner of digital asset gets owner’s consent.

NOTE: The interactions between the the owner of digital asset and the VAL Server serves the owner of digital asset are implementation specific and out of scope of the present document.

7. VALserver serves the owner of digital asset sends owner’s consent to DAPM to indicate agree or deny of the application for operation permission. If the request is agreed, the time limitation of the digital asset operation is also included in the response.

8. Based on the owner consent response, DAPM stores the authorization record, the record includes the information about digital asset identifier and authorized operation.

9. DAPM sends Authenticate permission response to A-DACM to notify whether the consumer is allowed to operate the digital asset.

10. A-DACM records the agreed operation and related time limitation of this digital asset for this consumer VAL Server.

11. A-DACM sends Digital asset operation response to VAL Server.

NOTE: If A-DACM and DAPM are realized in the same server, step 2 and step 9 could be skipped.

### 7.x.4 Solution evaluation

This solution addresses KI#9.

\* \* \* End of Change \* \* \* \*