**3GPP TSG-SA WG6 Meeting #62 S6-243360**

**Maastricht, Netherlands, 19th – 23rd August 2024 (revision of S6-243323)**

**Source: Samsung**

**Title: New solution for user consent in nested API invocations**

**Spec: 3GPP TR 23.700-22 v0.4.0**

**Agenda item: 8.7**

**Document for: Approval**

**Contact: Basavaraj (Basu) Pattan (**[**basavarajjp@samsung.com**](mailto:basavarajjp@samsung.com)**)**

**1. Introduction**

This contribution proposes new solution for Key Issue #1, for user consent management in nested API invocations, both prior to invocation and upon service API invocation.

**2. Reason for Change**

The open issue#1 in key issue #1 is to address how consent of the resource owner can be managed through communication between the resource owner and authorization function in the CAPIF core function. Obtaining authorization information with resource owner consent upon service API invocation is not handled in CAPIF TS 23.222. And, this is also applicable in the cases of nested API invocations. Also, procedure in clause 8.32, TS 23.222 does not clarify about how to obtain authorization information with resource owner consent in nested API invocation, specifically in step 4.

This pCR proposes new solution for obtaining authorization with resource owner consent upon service API invocation, which is applicable for both nested API invocations and generically when API invoker invokes service API directly on AEF. Also, the contribution clarifes procedure in clause 8.32, TS 23.222 on how the authorization is obtained with resource owner consent during nested API invocation case.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TR 23.700-22 v0.4.0.

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

## 6.1 Mapping of solutions to key issues

Table 6.1-1 Mapping of solutions to key issues

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | KI #1 | KI #2 | KI #3 | KI #4 | KI #5 | KI #6 | KI #7 |
| Sol #1 |  |  | X |  |  |  |  |
| Sol #2 | X |  |  |  |  |  |  |
| Sol #3 | X |  |  |  |  |  |  |
| Sol #4 |  |  |  | X |  |  |  |
| Sol #5 |  |  |  |  | X |  |  |
| Sol #6 |  |  |  |  |  |  | X |
| Sol #7 |  |  |  |  |  |  | X |
| Sol #8 |  |  |  |  |  |  | X |
| Sol #9 | X |  |  |  |  |  |  |
| Sol #10 | X |  |  |  |  |  |  |
| Sol #11 | X |  |  |  |  |  |  |
| Sol #X | X |  |  |  |  |  |  |

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

## 6.X Solution #X: User consent upon nested service API invocation

### 6.X.1 Solution description

#### 6.X.1.1 General

This solution maps to KI#1 on managing the resource owner consent in nested API invocations scenarios. The solutions address the scenario of obtaining authorization information with resource owner / user consent prior and upon nested service API invocations. The solution proposed for obtaining authorization information with resource owner / user consent upon service API invocation is applicable both the cases of API invoker obtaining authorization information with resource owner consent upon service API invocation on AEF or an AEF obtaining authorization information with resource owner consent upon a nested API invocation on another AEF.

For the solution related to obtaining authorization information with resource owner consent upon nested service API invocation, the AEF invokes the service API directly to downstream AEF and the downstream AEF responds with a message that authorization information with user consent is required. Based on the message from downstream AEF the requesting AEF obtains the required authorization information with resource owner consent using the procedure specified in clause 8.31, TS 23.222 [2]. This solution proposes new procedure based on the procedure in clause 8.32 of 3GPP TS 23.222 [2] that is for obtaining authorization with resource owner consent prior to service API invocation. Also, the procedure in clause 8.16, TS 23.222 [2] is updated to handle the case for obtaining authorization with resource owner consent upon service API invocation.

For the solution related to obtaining authorization information with resource owner consent prior to nested service API invocation, the step 4 of clause 8.32 procedure, TS 23.222 [2] is updated to clarify that AEF obtains authorization with resource owner consent using the procedure specified in clause 8.31 of 3GPP TS 23.222 [2].

#### 6.X.1.2 Obtain authorization with user consent upon service API invocation

This solution illustrates the procedure for obtaining authorization with resource owner consent in a nested API invocation, where an AEF to invoke the downstream service APIs, obtains authorization upon the downstream service API invocation. This new solution is an alternative to procedure specified in clause 8.32 of 3GPP TS 23.222 [2] (Reducing authorization information inquiry in a nested API invocation). Clause 8.32, TS 23.222 [2], handles the case of obtaining authorization with user consent prior to nested API invocation. This solution handles the case of obtaining authorization with user consent upon nested API invocation. The modifications needed to clause 8.32 in the new solution are highlighted (**in bold**).

Figure 6.X.1.2-1: Obtaining authorization information during the API invocation in nested API invocation

As shown in Figure 6.X.1.2-1, is the modified clause 8.32 of 3GPP TS 23.222 [2] (Reducing authorization information inquiry in a nested API invocation) procedure, to obtain authorization information in a nested API invocation, in which an API exposing function receiving the service API invocation request interacts with another API exposing function to provide the service.

1. API invoker obtains the authorization information to invoke the service API on API exposing function 1, with involvement of resource owner function in issuing resource owner consent to the API invoker.
2. API invoker invokes the service API in API exposing function 1 using the authorization information in step 1.
3. To fulfil the API invoker’s request, the API exposing function 1 decides to invoke service API in API exposing function 2.
4. **The API exposing function 1 invokes with service API directly on API exposing function 2 without the authorization information (including resource owner consent), as specified in clause 8.16, 3GPP TS 23.222** [2]**.**
5. **The API exposing function 2, triggers procedure to obtain the authorization information for API exposing function 1 with resource owner consent involving resource owner function and CCF.**
6. **After the API exposing function 1 obtains the required authorization information with resource owner consent, as in step 5**, the API exposing function 1 invokes the service API on API exposing function 2 with the authorization information, as specified in clause 8.31, 3GPP TS 23.222 [2].
7. The API exposing function 2, **validates the service API request and the authorization information with resource owner consent**. **If it is valid and matching the context of the service API request, then the API exposing function,** executes the service API request and
8. Responds to the API exposing function 1 appropriate Service API response message.
9. The API exposing function 1, based on the service API response message from API exposing function 2, responds to the API invoker with appropriate service API response message.

The procedure for step 5 in the solution illustrated above (Figure 6.X.1.2-1) in detailed below. This solution is an enhancement to clause 8.16, TS 23.222 [2] (Service API invocation with AEF authorization) or the solution can be new a procedure alternative to clause 8.16, TS 23.222 [2] to handle the case of obtaining authorization with resource owner consent upon service API invocation.



**Figure 6.X.1.2-2: Procedure for obtaining authorization information upon service API invocation**

Figure 6.X.1.2-2 illustrates the steps for obtaining authorization information upon service API invocation, as given below:

1. The API exposing function 1 invokes with service API directly on API exposing function 2 without the authorization information, as specified in step 1 of clause 8.16.3, 3GPP TS 23.222 [2].
2. API exposing function 2, determines that the required authorization information with resource owner consent is not available to authorize the service API request from API exposing function 1.
3. **API exposing function 2 responds to API exposing function 1, with response message indicating the failure status of the request message, and indicates the reason of failure that the Authorization information with resource owner consent is not available for resource owner (s) in the service API request. The information included in the response message is shown in Table 6.X.1.2-1.**

Table 6.X.1.2-1: Response message

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| **Request status** | **M** | **Indicates that the request message has failed.** |
| **Authorization information with resource owner consent required** | **M** | **Indicates that the required authorization information with resource owner consent is required.** |
| **Resource Owner (s)** | **M** | **Identifiers or other information related to the resource owners for which the authorization information with resource owner consent is needed.** |
| **CCF Information** | **O** | **Information related to the CCF. For example, CCF URL, Identifier of the CCF, etc.**  **If this information is not present, the API exposing function 1 may contact the CCF that it is configured with.** |

1. **Based on the information received from API exposing function 2, the API exposing function 1 obtains the authorization information with resource owner consent for the required resource owners, using the procedure in clause 8.31 of 3GPP TS 23.222** [2]**.**
2. After obtaining authorization with resource owner consent, the API exposing function 1 invokes the service API on API exposing function 2 using procedure in clause 8.32 of TS 23.222 [2].

In the above solution related to Figure 6.X.1.2-1, API exposing function can be API invoker and the API exposing function 2 can be API exposing function 1. In such case, the API invoker can use this procedure to directly invoke the service API on API exposing function and solution in Figure 6.X.1.2-1 can be used to obtain the resource owner consent upon service API invocation.

#### 6.X.1.3 Obtain authorization with user consent prior service API invocation

This solution is related to obtaining authorization information with resource owner consent prior to nested service API invocation. The step 4 of clause 8.32 procedure, TS 23.222 [2] is updated to clarify that AEF obtains authorization with resource owner consent using the procedure specified in clause 8.31 of 3GPP TS 23.222 [2]. The modifications needed to clause 8.32 in the new solution are highlighted (**in bold**).



Figure 6.X.1.3-1. Procedure for obtaining authorization information prior to API invocation in a nested API invocation

1. The API invoker obtains the authorization information to invoke the service API on API exposing function 1, with involvement of resource owner function in issuing resource owner consent to the API invoker, using the procedures specified in clause 8.31 of 3GPP TS 23.222 [2].
2. API invoker invokes the service API in API exposing function 1 using the authorization information.
3. To fulfil the API invoker’s request, the API exposing function 1 decides to invoke service API in API exposing function 2.
4. **The API exposing function 1, obtains the authorization information to invoke the service API on API exposing function 2, with the involvement of resource owner function in issuing resource owner consent to the API exposing function 1. The procedures specified in clause 8.31 of 3GPP TS 23.222** [2] **is used in this step, to obtain the authorization information with involvement of resource owner function.**
5. The API exposing function 1 invokes the required service API on API exposing function 2 using the authorization information obtained in step 4.
6. The API exposing function 1 receives the service API response from API exposing function 2, and
7. The the API exposing function 1 responds to API invoker with appropriate Service API response message.

The main update is in step 4, where resource owner function is involved in obtaining the resource owner consent to issue the authorization to API exposing function 1 to invoke service API on API exposing function 2.

### 6.X.2 Architecture Impacts

The existing CAPIF architecture as specified in 3GPP TS 23.222 [2], is used for the interactions between API Invoker and CCF defined in this solution. No new functional entities or interfaces are proposed in this solution.

### 6.X.3 Corresponding APIs

The solutions proposed impact the procedures and the related APIs, specified in clause 8.32, clause 8.16 of 3GPP TS 23.222 [2]. During normative phase, if new procedures are agreed as way forward than updating the existing APIs and procedures, then correspondingly new APIs may need to be specified.

### 6.X.4 Solution evaluation

This solution addresses the open issue #1 of key issue #1 by enabling for obtaining authorization with resource owner consent upon service API invocation, which is applicable for both nested API invocations and generically when API invoker invokes service API directly on AEF. The solution proposes new response message from AEF, to the entity invoking service API where authorization (with resource owner consent) is required. This response triggers for obtaining the authorization with user consent based on existing procedures in TS 23.222 [2]. Also, the solution clarifes procedure in clause 8.32, TS 23.222 [2] on how the authorization is obtained with resource owner consent during nested API invocation case. Thus, the solution enhancements cover both the cases of obtaining authorization information with resource owner consent prior and upon service API invocation.

\* \* \* End of Changes \* \* \* \*