**3GPP TSG-SA WG6 Meeting #62 S6-243358**

**Maastricht, Netherlands, 19th – 23rd August 2024 (revision of S6a240295, 3330)**

**Source: Nokia**

**Title: Solution for Consent Management**

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

**Agenda item: 8.7**

**Document for: Approval**

**Contact: Diego Preciado (****diego.preciado\_rojas@nokia.com****)**

**1. Introduction**

This contribution provides a proposal for solution of KI#1 and KI#6 on Consent Management.

**2. Reason for Change**

KI#1 states that it is needed to study “*How consent of the resource owner can be managed through communication between the resource owner and authorization function in the CAPIF core function”*. This solution proposes the service operations and related information flows to capture the consent from the resource owner.

The Rel.18 status is that the CAPIF-8 interactions are not specified by SA3. So, CCF and ROF interactions are to be addressed in Rel.19 via this study in SA6 and also now SA3 also has SI.

On CAPIF-8, when CCF (AuthF) is triggered for service API authorization by API invoker, the OAuth 2.0 framework can be used which enables CCF to interact with ROF to obtain the user consent.

Several scenarios could take place:

1. For every API invocation, the CCF (AuthF) can initiate an interaction with the corresponding ROF. (Rel.18 work). There is no restriction on time when the RO can be asked for explicit opt-in.

2. There could be scenarios in which the RO can not provide the opt-in (e.g., duting Night time). For API invocations (requesting Consent capture) on those time frames, the CCF (AuthF) can initiate a combined interaction with ROF as soon as a suitable time frame is found. The preferences for notification periods can be provided by the ROF while subscribing to CAPIF events. Additionally, as stated in clause 5.6.2 of 3GPP TR 23.700-22 v0.4.0, the unwanted interactions with the RO user need to be minimized.

This contribution aims to solve (2) which is an enhancement on the Rel.18 mechanism.

**3. Proposal**

It is proposed to agree the new key issue for 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#Y | X |  |  |  |  | X |  |

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

## 6.z Solution #Y: Capturing resource owner consent

### 6.z.1 Solution description

#### 6.z.1.1 General

Even though consent can be captured through a variety of methods and techniques (e.g., ticking a box on a website or writing/accepting a letter confirming the grant for processing personal data), having the consent captured during runtime is a well-established approach for some scenarios in which the resource owner grants or denies the API invoker’s access request.

While capturing the consent during runtime, the RO is presented the purpose (of data processing), indicating what the API invoker intends to do with the personal information resources of the RO (e.g., read location for spatial analytics or read network activity for fraud detection). In turn, the RO may grant access to personal information resources based on the purpose, for instance: grant access to personal information resources for fraud detection but deny access for other purposes (e.g., advertising).

#### 6.z.1.2 Procedure for capturing resource owner consent

Figure 6.z.1-1 presents the procedure for capturing and storing the consent using RNAA.

Pre-condition:

1. The API invoker is onboarded as in clause 8.1 in 3GPP TS 23.222 [2] and has received an API invoker identity.



Figure 6.z.1-1: Procedure for capturing resource owner consent

1. ROF subscribes with the CCF providing Identity and Security information for CAPIF events about consent requests (see Table 8.8.6-1) including relevant Event Criteria and Notification reception information (containing a callback URI). Optional information as time or zone constraints for notifying the RO or subscription duration could be present while subscribing.

NOTE 1: The details of the ROF subscription procedure can be specified in normative work.

1. The API invoker(s) send Obtain service API authorization request(s) to the CAPIF core function for obtaining permission(s) to access the service API(s) by including the API invoker(s) identity information and any information required for authentication of the API invoker(s). The API invoker(s) include in the request information about the purpose and the targeted resources and operations to be performed on those resources.

NOTE 2: Authorization details will be specified by SA3.

1. The CCF validates the authentication of the API invoker(s) (using authentication information) and checks whether the API invoker is permitted to access the requested resources, i.e., checks if a consent record for the signalled purpose is already in place. If the consent for accessing the requested resources for the signalled purpose is already granted, the information flow continues in step 5 of Figure 6.z.1-1.

NOTE 3: The authentication process is specified in clause 6.5.2 of 3GPP TS 33.122 [3].

NOTE 4: Whether the CCF is allowed to hold/cache consent records depends on local regulations.

4 If the consent needs to be captured from the RO, the bulk processing of pending requests takes place as soon as the notification criteria are met. The bulk processing may include the CCF sending one event notification to the ROF (aggregating the multiple requests from the API invoker(s)) and consent capture from RO.

NOTE 5: The details of the interaction between RO and ROF for capturing the consent are considered out-of-scope of 3GPP.

1. If the RO grants the consent for accessing personal information resources, the authorization information to access the service APIs is sent to the API invoker(s) in the obtain service API authorization response(s).
2. The service API invocation(s) take place considering the authorization information received in the previous step.

#### 6.z.1.3 Enhancement to clauses in 3GPP TS 23.222

Potential changes to clauses 8.8.1, 8.8.6, 10.4.1 (among others) in 3GPP TS 23.222 will be based on SA3 solution for procedures on CAPIF-8 ad further elaborated during the normative phase.

### 6.z.2 Architecture Impacts

None.

### 6.z.3 Corresponding APIs

NOTE: Whether new or enhanced APIs are required in support of this solution is in scope of SA3.

### 6.z.4 Solution evaluation

This solution addresses the following open issue in KI#1:

1. How consent of the resource owner can be managed through communication between the resource owner and authorization function in the CAPIF core function

This solution provides a feasible solution for managing user consent using subscribe-notify methods where the CCF can combine one or more pending user consent events and notify the ROF. This approach saves multiple communications between ROF and CCF (AuthF) in scenarios where too many user consent interactions are triggered to the end user’s application interactions.

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