**3GPP TSG-SA WG6 Meeting #62 S6-243361**

**Maastricht, Netherlands, 19th – 23rd August 2024 (revision of S6-243321)**

**Source: Samsung**

**Title: Pseudo-CR on user consent for group**

**Spec: 3GPP TR 23.700-22 V0.4.0**

**Agenda item: 8.7**

**Document for: Approval**

**Contact: Basavaraj (Basu) Pattan, basavarajjp@samsung.com**

**1. Introduction**

This contribution proposes on how resource owner’s consent required within the group is managed.

**2. Reason for Change**

3GPP TS 23.222, clause 8.31, specifies mechanism for API invoker obtaining authorization from resource owner. However, it does not specify how to handle the case of obtaining authorization information with resource owner consent in group communication.

This solution proposes the group member resource owner function involvement with CAPIF Core Function (CCF) to enable the authorization information for API Invoker with resource owner consent to invoke the service API on API exposing function. For example, the VAL server (API invoker) communicates with CAPIF Core Function (CCF) to obtain the authorization information (as described in clause 8.31 of 3GPP TS 23.222) regarding invocation of SEAL SS\_LocationInfoRetrieval API (described in clause 9.4.4 of 3GPP TS 23.434) at the location management server (acting as an API exposing function for the API invoker).

**3. Proposal**

It is proposed to agree the following changes to 3GPP TR 23.700-22 V0.4.0.

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

## 5.1 Key issue #1: Managing resource owner consent

### 5.1.1 Description

With the introduction of support for Subscriber-aware Northbound API access in 3GPP Rel-18 a number of requirements were added at stage 1, one of which was motivated by the desire for a UE to be able to control whether or not to provide information considered private to a 3rd party entity. Specifically, the requirement is that the 5G system shall be able to allow the UE to provide/revoke consent for information (e.g., location, presence) to be shared with the third-party. At stage 2 the CAPIF-8 reference point was introduced to CAPIF where the aspect of consent was highlighted through the statement that the resource owner communicates with the authorization function in the CAPIF core function to manage resource owner consent, with such communication being expected to be performed over CAPIF-8. However, the mechanism for managing such consent was not specified with the functionalities over CAPIF-8 being is FFS and out of scope of the Rel-18 of the specification.

Further, user consent may also be required during group communication to access the information related to the members of the group. For example, the VAL server requesting to create a dynamic platooning group requires to access the location of the members joining the group.

### 5.1.2 Open issues

The CAPIF does not address management of resource owner consent in the context of supporting RNAA. The open issues are:

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

2. Whether (and how) “purpose of data processing” will be captured and where will it be stored.

3. How to align and manage access control that is more granular than simply granted/denied for service API (e.g., service operation level, resource level, service API originator/requestor details) with the provided resource owner consent to ensure appropriate usage of resource owner consent at the enabler layer.

4. How resource owner’s consent required within the group is managed.

NOTE: Aspects pertaining to the definition of resource owner consent/authorization over CAPIF-8 are in the scope of SA3, noting that the R18 security aspects of CAPIF supporting RNAA are specified in 3GPP TS 33.122 [3].

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

## 6.x Solution #x: User consent for group

### 6.x.1 Solution description

#### 6.x.1.1 General

This paper proposes a solution for key issue #1 on enabling user consent within group.

3GPP TS 23.222, clause 8.31, specifies mechanism for API invoker obtaining authorization from resource owner. However, it does not specify how to handle the case of obtaining authorization information with resource owner consent in group communication.

Therefore, this solution proposes the group member resource owner function involvement to enable the authorization information for API Invoker with resource owner consent to invoke the service API on API exposing function. For example, the VAL server (API invoker) communicates with CAPIF Core Function (CCF) to obtain the authorization information (as described in clause 8.31 of 3GPP TS 23.222) regarding invocation of SEAL SS\_LocationInfoRetrieval API (described in clause 9.4.4 of 3GPP TS 23.434) at the location management server (acting as an API exposing function for the API invoker).

#### 6.x.1.2 Procedure

The following text captures the solution by describing the neccesary changes in bold font compared with 3GPP TS 23.434 v19.2.0 as shown below:

|  |
| --- |
| \* \* \* Enhancement based on 3GPP TS 23.434 v19.2.0 \* \* \* \* 10.3.8 Group announcement and join10.3.8.1 General This subclause describes the procedures for establishing group communication from the group management server to the group management clients. 10.3.8.2 Procedure Pre-conditions:  1. The group management client, group management server, VAL server and the VAL clients belong to the same VAL system.  2. The VAL server is aware of the users' identities and is authorized to form a VAL group.    Figure 10.3.8.2-1: Procedure for establishing VAL group communication between the group management server and group management client with user consent.  1. The VAL server determines group information and the identity list to which the group announcement shall be sent. The decision can be based on the list of authorized UEs and other criteria (e.g. user consent, service, or vehicle driving profile).  2. The VAL server configures VAL group for Uu communication defined by VAL Group ID for one or more VAL services with list of VAL Service ID with the group management server.  3. The group management server creates an empty group based on the information provided in the Configure VAL group request. The group management server stores the mapping between the VAL group ID and the external Group Id in the VAL group document, along with a list of GPSIs corresponding to the identity list provided by the VAL server. The group management server also determines whether the group is for 5G LAN-Type communication and whether Ethernet or IP (IPv4 and/or IPv6) transport shall be used for the 5G LAN-Type communication.  4. If 5G LAN-Type communication is to be used, the group management server creates a 5GVN group in the 5GS via N33 using the create group procedure specified in 3GPP TS 23.501 [10] clause 5.29.2 and 3GPP TS 23.502 [11] clause 4.15.6. The group management server creates the 5GVN group data and the 5GVN group membership data defined in 3GPP TS 23.502 [11] clause 4.15.6.3b to be configured in the 5GS. To create the 5GVN group data the group management server uses the 5G LAN-Type communication type information provided by the VAL server to set the PDU session type (Ethernet or IP) and maps the VAL service IDs to Application descriptors. To create the 5GVN group membership data the group management server maps the VAL group ID to the External Group ID and makes a list of GPSIs corresponding to the identity list provided by the VAL server.  NOTE 1: This step is skipped for the case that a 5G LAN-Type communication is not being used.  NOTE 2: The PDU session type, DNN, S-NSSAI provided within 5GVN group data cannot be modified in the 5GS after the create procedure.  NOTE 3: The 5GS supports only a 1:1 mapping between DNN/S-NSSAI combination and 5GVN group.  NOTE 4: The group management server maintains a mapping between DNN and S-NSSAI of the 5GVN group and the VAL server requester identity based on operator policy. How such mapping is configured is implementation specific and out of the scope of this specification.  5. The group management server announces the VAL group to the group management clients. For a 5GVN group the announcement includes the communication type (IP or Ethernet), DNN, and S-NSSAI corresponding to the 5GVN group. **For group creation requiring user consent, the announcement includes the user consent information (e.g. subject, scope). Subject may include VAL server related to VAL service IDs, group management server, other group members etc and Scope includes e.g. location, service APIs etc.**  **5a. The group management client requests Resource Owner Function (ROF), the group user consent including the group ID, subject (e.g. VAL server, group management server, other group members) and scope (e.g. location, service APIs).**  **5b.** **The Resource owner function (ROF) and CAPI Core Function (CCF) communication communicate for managing provisioning of resource owner consent. The security details of this step is in the scope of SA3.**  **5c. Based on the result in step 5b, the Resource owner function (ROF) indicates the user consent success or failure, for e.g. success if the user has given consent for the requested information in full or partial.**  6. The group management client registers to VAL group communication using the VAL Group ID. **When user consent is requested in step 5, based on the result of group user consent the group management client registers to VAL group communication using the VAL Group ID. For example, the group management client may not send the registration request to the group if the user consent is not issued.**  7. The group management server records the users who have registered to be the members of the group.  8. The group management server sends a VAL group registration response to the group management client.  9. The group management server sends a configure VAL group response to the VAL server.  NOTE 5: Step 9 may occur any time after step 5, **except for the case when the user consent is requested in step 5**.  10. The group management server sends identity list notification about the newly registered users to the other members of the group and VAL server, whose subscription to receive notifications of newly registered VAL UE IDs is successful in step 8 and step 9 respectively.  11. The group management client may inform VAL client about the updated identity list. |

When a group member is leaving the group by de-registering (as described in clause 10.3.9 of 3GPP TS 23.434), subsequent to step 2, the group management server records de-registration of a group member including any previous user consents associated with it. The VAL server is also notified about the updates to the user consent information.

### 6.x.2 Architecture Impacts

This solution is presented based on the CAPIF architecture in 3GPP TS 23.222 and SEAL architecture in 3GPP TS 23.434 and would need enhancements for GMC to ROF interactions.

### 6.x.3 Corresponding APIs

This solution is based on the following APIs:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \* \* \* Enhancement based on 3GPP TS 23.434 v19.2.0 \* \* \* \* 10.3.2.28 Group announcement Table 10.3.2.28-1 describes the information flow for a group management server to announce a VAL group to the group management clients.  Table 10.3.2.28-1: Group announcement   |  |  |  | | --- | --- | --- | | Information element | Status | Description | | VAL group ID | M | The group ID used for the VAL group. | | VAL group description (see NOTE 3) | M | Information related to the VAL group e.g. group definition including communication type and connection parameters, policy, group size, group leader. | | VAL service ID list  (see NOTE 1) | O | List of VAL services whose service communications are to be enabled on the group. | | Geo ID list  (see NOTE 1) | O | List of geographical areas to be addressed by the group. | | Identity list  (see NOTE 1, NOTE 2) | O | List of VAL UE IDs who are invited to be member of the group. | | **User consent information** | **O** | **List of subject (e.g. VAL server related to VAL service IDs, group management server, other group members) and scope (e.g. location, service APIs) that requires user consent** | | NOTE 1: At least one of these IEs shall be present.  NOTE 2: This element is not present if it results in privacy concerns.  NOTE 3: Group communication type may indicate 5G LAN-Type communication using either Ethernet or IP (IPv4 and/or IPv6) transport. Group connection parameters may include DNN and S-NSSAI. | | |  10.3.2.29 Group registration request Table 10.3.2.29-1 describes the information flow for a group management client to register to a VAL group in response to a group announcement from the group management server. Message filters for throttling messages and notifications is included in this request e.g. for limiting message exchange on a constrained UE, for receiving only improtant group communication.  Table 10.3.2.29-1: Group registration request   |  |  |  | | --- | --- | --- | | Information element | Status | Description | | VAL UE ID | M | Identity of the VAL UE registering to the VAL group. | | VAL Group ID | M | The group ID to be registered by the VAL UE for the VAL group. | | Identity list subscription | M | Indicates interest to receive notifications of newly registered or de-registered VAL UE IDs | | Message filters | O | Group message communication will be sent to the VAL UE after applying message filters as described in Table 10.3.2.29-2. | | **User consent information** | **O** | **List of subject and scope for user consent** | |

API corresponding to step 5a:

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| VAL group ID | M | The group ID used for the VAL group. |
| VAL group description (see NOTE 1) | M | Information related to the VAL group e.g. group definition including communication type and connection parameters, policy, group size, group leader. |
| **User consent information** | **O** | **List of subject and scope for user consent** |
| NOTE 1: Group communication type may indicate 5G LAN-Type communication using either Ethernet or IP (IPv4 and/or IPv6) transport. Group connection parameters may include DNN and S-NSSAI. | | |

API corresponding to step 5c:

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| VAL group ID | M | The group ID used for the VAL group. |
| **User consent result** | **M** | **User consent result as success if the user has given consent for the requested information in full or partial, otherwise failure.** |
| **User consent information (NOTE 1)** | **O** | **List of subject and scope for user consent** |
| NOTE 1: This IE is present only if the result in User consent result is success. | | |

### 6.x.4 Solution evaluation

This solution solves the open issue in key issue#1 related to managing resource owner’s consent required within the group. This solution proposes mechanism where group member resource owner function is involved with CCF to enable the authorization information (with resource owner consent) for API Invoker to invoke the service API on API exposing function.

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

<Proposed change in revision marks>