**3GPP TSG-SA3 Meeting #119 S3-245226**

Orlando, US 11 – 15 November 2024 *revision of* S3-244928

**Source: Nokia**

**Title: Addressing EN’s on RO permission management in solution 7**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

Update to solution for RO consent management.

# 2 References

[1] 3GPP TS 23.700-22

[2] 3GPP TS 33.700-22

# 3 Rationale

The solution addresses how to collect and manage resource owner permissions from the ROF over CAPIF-8 interface.

The solution is a sketch of relevant service operations related to security.

The solution is refined.

ENs are resolved.

Evaluation is added.

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\* START OF CHANGES*

## 6.7 Solution #7: RO permission management

### 6.7.1 Introduction

This solution is addressing KI#1.2.

CAPIF-8 interface between UE and CCF is being introduced by TS 23.122. ROF is handling this interface.

This solution addresses how to collect and manage permission notifications for resource owner authorization from the ROF over CAPIF-8 interface by subscribe to and unsubscribe from CAPIF events and by receive notifications from the CAPIF core function.

### 6.7.2 Solution details

RO authorization management needs a set of service operations to allow the ROF to collect and manage the permissions. The following sketches them and are additions to TS 23.222 clause 10.4.1 for CAPIF-8.

In general, the following can be added:

* Subscribe for permissions: allows ROF to subscribe for requests from Authorization Function (in CCF) to ask for permission on receiving RO details.
* Get pending permission: allows the ROF to obtain from the Authorization Function (in CCF) the pending permission requests associated with it, potentially based on being notified before and receiving information where to obtain it from.
* Notify event: allows the authorization function (in CCF) to notify the ROF about pending permissions.
* Wakeup: allows the Authorization Function (in CCF) to wake up the resource owner function (ROF) in the UE via AMF NAS operation which allows the UE to obtain pending permissions.
* Unsubscribe: allows a ROF to unsubscribe pending perrmissions events from Authorization function (in CCF).
* Report permission: allows ROF to post permissions to the Authorization Function URI based on permission requests received beforehand.
* Retrieve permission: allows ROF to retrieve the permission records that have been granted by it earlier.

#### 6.7.3.1 Notifications for permissions / wakeup

EN: Flows to be added.

When ROF is waiting for notifications, different approaches can be envisioned.

**Triggering for RO permission via subscription notification**

- ROF subscribes for the pending permission requests with Authorization Function and waits.

- Upon Access Token Request from API Invoker (and based on optional notification criteria set by the resource owner), the Authorization Function (CCF) notifies ROF.

- The notification optionally includes the consent/permission information of API Invoker. If the notification does not contain this information, ROF explicitly fetches the details from Authorization Function and posts the consent responses to the URI provided by Authorization Function. CCF can store the information locally or at a repository service and then provide the access token to the API invoker.

Editor's Note: How the CCF can send notification to an application (ROF) on the UE is FFS.

**Triggering for RO permission via NAS**

- service operation to allow the Authorization Function (in CCF) to wake up the resource owner function in the UE (taking into account notification restrictions provided by the resource owner during the subscription procedure) via AMF (NAS signalling). This service operation can be supported by AMF.

- ROF subscribes for the pending consent/permission request with Authorization Function.

- Upon Access Token Request from API Invoker, Authorization Function wakes up ROF via AMF using NAS signalling message, which can include the consent/pemission information of API Invoker. If the NAS message does not contain consent information, ROF explicitly fetches the consent requests from Authorization Function and posts the consent responses to the URI provided by Authorization Function.

### 6.7.3 Evaluation

This solution covers a management aspect necessary for the RO authorization/permission process, ie. how to ensure reachability of the ROF for authentication and authorization. In particular, how can the resource owner subscribe for the notifications.

In ROF and CCF new APIs need to be supported for subscription notifications.

For NAS based notifications, AMF and UE need to support new NAS IEs to support wakeup.

The NAS based solution has access network impact.

The solution needs to keep ROF (e.g., the web browser on UE) online to provide authorization information to CCF.

Editor's Note: Further evaluation TBD.

*\*\*\*\*\*\*\*\*\*\* END OF CHANGES*