**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-230421-r1***

**Electronic meeting, 16 - 20 January 2023**

**Source: NTT DOCOMO**

**Title: pCR to 33.884 updating solution #2**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***The contribution*** ***proposes to allow differentiation between user and subscriber authentication***

# 2 References

# 3 Rationale

For the case the UE application can't securely store a client credential, IETF defined the PKCE flow. This pCR adds the PKCE flow as a potential solution.

# 4 Detailed proposal

++++++++++++++++++ Start Changes +++++++++++++++++

### 6.2.2 Solution details



Figure 6.2.2-1: OpenID Connect for SNAAPP AFs

The flow follows the authorization code flow of OpenID Connect [6]. All communication is over TLS secured connections.

1. Prior to any interaction, AZF should be registered with ANF, giving information that will be provided to the UE when requesting authentication.

2. The UE accesses the AZF without identity token

3. The AZF shall redirect the UE to the ANF\_URI, with the type set to code (to indicate authorization code flow), scope set to openid (to indicate that this is an openID request), client\_ID set to its own ID, redirect\_URI set to the URL to be used in step 8, and may set state to some state that can be used by AZF to reduce its internal state. Because sometimes it is necessary to authenticate the subscriber, and sometimes authentication of user is sufficient, the ANF shall offer separate endpoints for user and for subscriber authentication. The AZF shall be aware of which entity shall be authenticated based on configuration. Which authentication method is then chosen is between negotiated between UE/user and ANF and is out of scope of this solution.

4. The UE shall access the ANF at the redirected to ANF\_URI, including the parameters of step 3.

5. The ANF shall authenticate the UE. This can be done in the usual way the home network authenticates the user, which may be GBA, AKMA, or using a proprietary method such as username/password.

6. The ANF should request authorization to release the required personal information to the AZF from the user. In this setup, the ANF presents to the user the information that was made available to the ANF about the AZF in the enrolment.

7. The ANF shall redirect the UE back to the AZF at the AZF\_URI, including as code a single use token, which shall be specific to the AF, and as state the state that was set in step 3.

8.-9. The AZF shall request the identity token from the ANF at its token endpoint. The ANF shall verify that the identity token is indeed being requested by the correct AZF, and, if correct, return the identity token to the AZF.

10. The AZF shall verify the validity of the identity token according to RFC 6749, especially Sections 4.1.2 and 10.12.

Editor's Note: which identifiers are to be used is FFS.

### 6.2.3 Evaluation

This solution can be used to address Authn-1-ResOwner.

Editor's Note: further evaluation is FFS

+++++++++++++++++++ End Changes +++++++++++++++++