**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-230422-r1***

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

**Source: NTT DOCOMO**

**Title: pCR to 33.884 adding new solution: PKCE flow**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***The contribution*** ***proposes the PKCE flow to authorize UE invoked APIs***

# 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 +++++++++++++++++

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for the 5G system".

[3] 3GPP TR 23.700-95: "Study on application enablement aspects for subscriber-aware northbound API access".

[4] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[5] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[6] openID.net: "OpenID Connect Core 1.0 incorporating errata set 1". Available at: <https://openid.net/specs/openid-connect-core-1_0.html>

[7] IETF RFC 7009: “OAuth 2.0 Token Revocation”.

[8] IETF RFC 7515: “JSON Web Signature (JWS)”.

[xx] IETF RFC 7636: "Proof Key for Code Exchange by OAuth Public Clients"

++++++++++++++++++ Next Change +++++++++++++++++

## 6.Y Solution #Y: Authorizing UE originated API invocation with PKCE flow

### 6.Y.1 Introduction

In case the API invocation can be initiated by an application on the UE without making use of a unique CAPIF client agent per UE, the UE application might not be able to securely store a client credential. For this case, there is the Authorization Code Flow with Proof Key for Code Exchange defined in RFC 7636 [xx].

### 6.Y.2 Solution details

The solution uses the PKCE protocol flow with the following mapping: the client in RFC 7636 is the application on the UE. The authorization server in RFC 7636 is the authorization function in the network.

Editor's note: whether a separate onboarding process is necessary for UE originated API invocation is FFS.

### 6.Y.3 Evaluation

Editor's note: whether the user interaction required for PKCE flow is acceptable for SA6 is FFS.

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