**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-230423-r1***

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

**Source: NTT DOCOMO**

**Title: pCR to 33.884 adding new solution: token validation**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***The contribution*** ***proposes a solution for validating OAuth access tokens***

# 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.Y Solution #Y: Validation of OAuth Token

### 6.Y.1 Introduction

If an OAuth token used for authorization, the API exposing function needs to verify the validity of the token. In this solution, this is done by token introspection RFC 7662 [yy]. The revocation procedure between authorization server and resource owner is out of scope of this solution.

### 6.Y.2 Solution details



Figure 6.Y.2-1: validation of OAuth 2.0 token

All messages containing a tokens shall be protected using TLS. The API invoker shall authenticate the API exposing function by verifying the API exposing function's certificate. The API exposing function shall authenticate the authorization function by validating the authorization function's certificate

Editor's Note: contents of the certificates and which CAs are acceptable is FFS.

The oAuth access token shall contain:

- a unique random string,

- which API the token applies to (the scope),

- who is the resource owner,

- the API invoker ID, and

- expiry time.

Editor's Note: how that information is encoded in the OAuth access token is for stage 3.

1. The API call shall contain the OAuth access token.

2. The API exposing function shall verify that the access token is applicable to the desired API call and if yes, send the access token to the authorization function for validation. Otherwise the API call shall fail and a new authorization may be requested.

3. The authorization function shall verify the validity of the access token and return whether the token is valid.

4. If the access token is valid, the API exposing function shall execute the API call.

The API exposing function may cache the result of validation. In that case, the API exposing function shall subscribe to receive a notification in case the token is revoked. This subscription may be included in step 2, e.g. by accessing a different endpoint for validate and subscribe than for validate only.

The authorization function shall offer a notification service to inform the API exposing function of revokation of a token. Subscription shall be on a per token basis.

The authorization function may store information about validity of tokens locally.

### Editor's Note: whether caching is required is FFS.6.Y.3 Evaluation

This solution addresses Authz-4-Scope and Authz-5-Revoke. This solution deviates from the existing CAPIF solution in clause 6.5.2.3 in TS33.122 [xx]. It can avoid the impact of signature generation and verification and of relying on synchronized time and short lived tokens at the expense of backend communication between AEF and authorization function.

Editor's Note: whether token introspection provides benefits over signature verification is FFS.

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