**3GPP TSG-SA3 Meeting #108Adhoc-e *draft\_S3-222496-r2***

**e-meeting, 10th – 14th October, 2022** Revision of S3-22xxxx

**Source: Huawei, HiSilicon**

**Title: New Solution on Resource Owner Authorization in API Invocation using OAuth Token**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***The contribution proposes a new solution for key issue for obtaining resource owner authorization in API invocation*** ***using OAuth token.***

# 2 References

# 3 Rationale

The contribution proposes a new solution for obtaining resource owner authorization in API invocation using OAuth 2.0.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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".

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

[yy] IETF RFC 6749: “The OAuth 2.0 Authorization Framework”.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.X Solution #X: Resource Owner Authorization in API Invocation using OAuth Token

### 6.X.1 Introduction

This solution addresses the requirement in KI#Y.

This solution proposes to reuse OAuth 2.0 with authorization code grant model to obtain resource owner’s authorization in case that an API invocation of network exposure is to process the resource owner’s data.

### 6.X.2 Solution details

### 6.X.2.1 Architecture



Figure 6.X.2.1-1 architecture for CAPIF with SNA enhancement

The architecture is derived from solution 2 in TR 23.700-95 [xx]. Definition of the authorization function, CAPIF-8, CAPIF-10, and CAPIF-10e is the same. Triggerer has the same definition of resource owner client(s).

It is proposed that the authorization function is collocated with the CCF.

However, the difference is that CAPIF-9 is not needed in this solution because there is no communication with AEF. CAPIF-8 is application layer, which is out of 3GPP

### 6.X.2.2 Procedure



Figure 6.X.2.2-1 Procedure of Obtaining Resource owner Authorization

As shown in the Figure 6.X.2.2-1, the details of obtaining resource owner authorization in API invocation is summarized as following:

1. API invoker obtains authorization method (e.g. method 1: TLS-PSK, or method 2: PKI, or method 3: TLS with OAuth token) as specified in clause 6.1 in TS 33.122 [zz].

2. API invoker discovers service API as specified in clause 6.3.1.3 in TS 33.122 [zz].

3. Resource owner triggers the API invocation. If resource owner authorization is needed for the invoked API and the method 3: TLS with OAuth token is selected, then the API invoker obtains tokenCAPIF via OAuth 2.0 with authorization code grant model as depicted in clasue 6.X.2.3.

Editor’s Note: If methods other than TLS with OAuth token is selected, how the resource owner authorizes the API invoker is ffs.

4. The API invoker invokes nouthbound API to the AEF as depicted in clause 6.5.2.1 or 6.5.2.2 in TS 33.122 [zz]. The API Invocation message includes tokenCAPIF.

5. The AEF verifies the tokenCAPIF in the message. The AEF verifies the integrity of tokenCAPIF and shall check whether IDs in the scope are align with the IDs in the API invocation message. If the verification is successful, it means the CCF has authorized the API Invoker to access the API and the resource owner has authorized the API invoker to access its resource.

Editor’s Note: Details of content and verification of token is ffs.

6. The AEF may update subscription data in UDM for user consent based on the resource owner’s authorization.

### 6.X.2.3 OAuth 2.0 role mapping

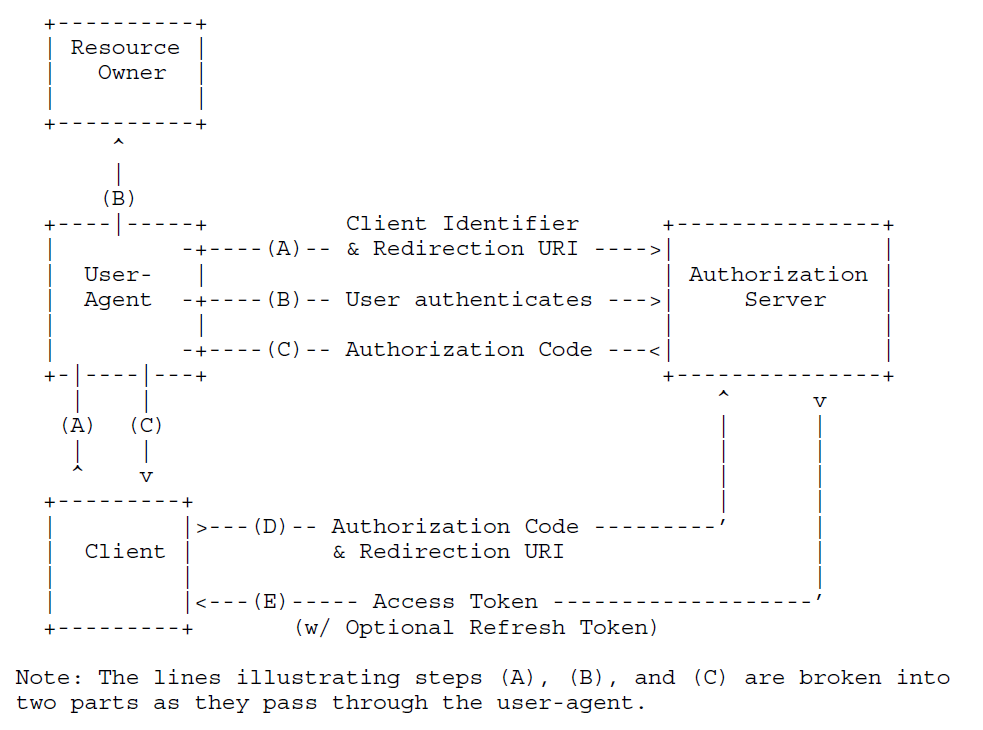


Figure 6.X.2.3-1 Procedure of Obtaining Resource owner Authorization

OAuth 2.0 with authorization code grant model is depicted in clasue 4.1 in RFC 6749 [yy]. In this solution, the API invoker endorses the role of client, the triggerer endorses the role of user-agent. The Authentication Function authenticates the resource owner in step B. The API invoker (i.e. client) retrieves tokenCAPIF from the Authorization function in CCF. The scope of the tokenCAPIF includes API invoker ID, service API ID and resource owner ID (i.e. GPSI).

### 6.X.3 Evaluation

TBD

Editor’s Note: Revocation of authorization is FFS.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*