**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_S3-230176-r4***

**Electronic meeting, 16 - 20 January 2023** Revision of S3-23xxxx

**Source: Huawei, HiSilicon**

**Title: New Solution on OAuth2.0 Token Revocation**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***The contribution*** ***proposes a new solution for key issue 2 in TR 33.884.***

# 2 References

# 3 Rationale

This solution addresses the requirement Authz-5-Revoke in KI#2.

This solution proposes to use short expire time for issued token. The authorization can be revoked automatically if API invoker does not refresh the issued token. There is no impact on AEF.

# 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 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[3] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

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

[5] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[6] IETF RFC 7519: "JSON Web Token (JWT)".

[7] IETF RFC 7515: "JSON Web Signature (JWS)".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[9] Void

[10] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[xx] 3GPP TR 23.222: “Common API Framework for 3GPP Northbound APIs”

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

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

## 6.X Solution #X: OAuth 2.0 Token Revocation

### 6.X.1 Introduction

This solution addresses the requirement Authz-5-Revoke in KI#2.

This solution proposes to use a short expiry time for an issued token. The authorization can be revoked automatically if an API invoker does not refresh the issued token. There is no impact on the AEF.

### 6.X.2 Solution details



Figure 6.X.2-1 Procedure of Revocation of OAuth Authorization

1. The API invoker discovers a service API as described in the clause 8.7 in TR 23.222 [xx]. Besides, the API invoker indicates its requirement for revocation to the CCF, the revocation requirement may be required by resource owner.

2. The CCF sends the service API Discovery Response message with information of the discovered API to the API invoker.

3. API Invoker sends the Token Request to the CCF to retrieve a token to access the discovered API.

4. The CCF issues a token with a short expiry time when receiving the requirement for revocation, e.g. 1 hour.

5. The CCF sends the Token Response to the API Invoker. The message includes the issued token. Once revocation is required by the resource owner, e.g. to log out, the API invoker stops refreshing the token, which will be revoked within the short expiry time.

### 6.X.3 Evaluation

This solution partially addresses the requirement Authz-5-Revoke in KI#2.

The solution assumes that API invoker is trusted by resource owner.

The solution has no impact on the AEF.

Editor’s Note: Further evaluation is FFS.

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