**3GPP TSG-SA3 Meeting #122 S3-25xxxx**

**Fukuoka, Japan, 19 – 23 May 2025**

**Source: Huawei, HiSilicon**

**Title: Pseudo-CR on description of OAuth 2.0**

**Document for: Approval**

**Agenda item: 5.20**

**Spec: 3GPP TR 33.938**

**Version: 0.2.0**

**Work Item: FS\_CryptoInv**

**Comments**

This contribution proposes detailed description for OAuth 2.0 for TR 33.938.

The OAuth 2.0 is an authorization framework. In 3GPP, the bearer token option in JWT format (using JWS) is chosen to address additional security aspects in OAuth 2.0. This option requires uses of cryptography, as in TLS and JWS. Since OAuth 2.0 is widely used in 3GPP specifications, e.g. SBI in TS 33.501 and others for SA6/CT, it is proposed to include its description in this TR although it is a framework, which is potentially impacted by QC and should not be left out in future PQC migration.

\* \* \* First 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 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[3] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[4] 3GPP TS 33.501: “Security architecture and procedures for 5G system”.

[5] IETF RFC 9190: "EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3".

[6] IETF RFC 5216: "The EAP-TLS Authentication Protocol",

[7] SECG SEC 1: “Recommended Elliptic Curve Cryptography”, Version 2.0, 2009. Available at <http://www.secg.org/sec1-v2.pdf>.

[8] SECG SEC 2: “Recommended Elliptic Curve Domain Parameters”, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>.

[9] IETF RFC 9001: "Using TLS to Secure QUIC".

[10] IETF RFC 8152: "CBOR Object Signing and Encryption (COSE)".

[11] 3GPP TS 33.220: “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)”.

[12] IETF RFC 8613: "Object Security for Constrained RESTful Environments (OSCORE)".

[13] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

[14] IETF RFC 6509: ''MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)''.

[15] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[16] 3GPP TS 35.205: "3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*".

[17] 3GPP TS 35.231: "Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*; Document 1: Algorithm specification".

[18] 3GPP TS 35.234: "Specification of the MILENAGE-256 algorithm set; An example set of 256-bit 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5, f5\* and f5\*\*; Document 1: General".

[x1] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[x2] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[x3] IETF RFC 7519: "JSON Web Token (JWT)".

[x4] 3GPP TS 29.500: "Technical Realization of Service Based Architecture".

\* \* \* Next Change \* \* \* \*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

BSF Bootstrapping Server Function

CBOR Concise Binary Object Representation

COSE CBOR Object Signing and Encryption

ECDSA Elliptic Curve Digital Signature Algorithm

JWT JSON Web Token

KDF Key Derivation Function

MPQUIC Multipath QUIC

OAuth Open Authorization

OCSP Online Certificate Status Protocol

OSCORE Object Security for Constrained RESTful Environments

PKI Public Key Infrastructure

QUIC Quick UDP Internet Connections

REST Representational State Transfer

SECG Standards for Efficient Cryptography

SUPI Subscription Permanent Identifier

TLS Transport Layer Security

UDP User Datagram Protocol

\* \* \* Next Change \* \* \* \*

### 4.4.x OAuth 2.0

The OAuth 2.0 protocol is an authorization framework enabling a third-party application to obtain limited access to an HTTP service as specified in RFC 6749 [x1]. The usage of bearer tokens in OAuth 2.0 and JSON Web Token (JWT) are specified in RFC 6750 [x2] and RFC 7519 [x3] respectively. The former requires TLS (see also in the clause 4.4.2) to secure transmission of token whereas the latter uses JSON Web Signature (JWS) (see also in the clause 4.4.17) for integrity protection of token.

OAuth 2.0, using JWT bearer token, is used in 5G system to provide security for the following:

* Authorization of Application Function (clause 12.4 of TS 33.501 [4])
* Authorization for the Service Based Interface (clauses 13 and 14 of TS 33.501 [4] and clause 6.7 of TS 29.500 [x4])
* Authentication for the management service for network slices (clause 15 of TS 33.501 [4])
* Authorization of NF Service for network automation (clause X.2 of TS 33.501 [4])

OAuth 2.0 (JWT bearer token) employs asymmetric cryptography and symmetric cryptography for authentication and key agreement, as in TLS.

OAuth 2.0 (JWT bearer token) employs asymmetric cryptography and symmetric cryptography for authorization based on signatures and message authentication code (MAC), as in JWS.

\* \* \* End of Changes \* \* \* \*