**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211765-r2***

**e-meeting, 17 - 28 May 2021**

**Source:** **Ericsson**

**Title: Update Solution #5****: End-to-end integrity protection of HTTP body and method**

**Document for: Approval**

**Agenda Item: 5.20**

# 1 Decision/action requested

***It is proposed to update the following solution in TR 33.875 [1]***

# 2 References

[1] 3GPP TR 33.875 "Study on enhanced security aspects of the 5G Service Based Architecture (SBA)" Release 17

# 3 Rationale

 This pCR provides two updates to solution #5: End-to-end integrity protection of HTTP body and method**:**

1. Resolve one Editor's Note: "Backwards compatibility with Rel-16 NF producers supporting only existing CCA is ffs.";

 2. Insertion of Hash Algorithm by NF service consumer.

# 4 Detailed proposal

\*\*\*\*\*\*BEGIN 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 33.501: "Security architecture and procedures for 5G System".

[3] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2".

[4] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[x] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3"

[y] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3"

\*\*\*\*\*\*NEXT CHANGE\*\*\*\*\*

## 6.5 Solution #5: End-to-end integrity protection of HTTP body and method

### 6.5.1 Introduction

This solution addresses the key issue #5 (End-to-end integrity protection of HTTP messages).

The core steps of this solution are:

- Use Client credentials assertions (CCAs) based authentication as specified in TS 33.501 [2] Clause 13.3.8 for NF-NRF or/and NF-NF communication.

- Enhance the Client credentials assertions (CCAs) to optionally include a hash of the HTTP body and HTTP method to protect the message itself.

- The receiving node (NRF or NF producer) computes the hash of the HTTP body and HTTP method and validates that it is identical to the hash received in the Client credentials assertions (CCAs).

Since the added hash is an optional field in the ClientCredentialsAssertion as specified in 3GPP TS 29.500 [x] Table 5.2.3.2.11 -1, this solves the backwards compatibility with Rel 16 NF producers supporting only existing CCA. A Rel-16 producer will verify the signature of the CCA correctly but ignore the optional field that it does not recognize. The behaviour is similar to Rel-15 producers' behaviour for IEs in access tokens that were introduced in Rel-16. As specified in TS 29.510 [y], Table 6.3.5.2.4-1 "Definition of type AccessTokenClaims", if an NF service producer receives an IE in the access token that it does not understand, the NF service producer ignores the IE. Similar behaviour can be specified for IEs in the CCA, see Table 6.5.2-1 below.

Editor's Note: It needs to be clarified whether the handling for access tokens is aplicable for CCAs.

Editor's Note: This solution has dependency on CT4 feedback on what SCP exactly needs to modify.

### 6.5.2 Solution details



Figure 6.5.2-1 CCA based Authentication with HTTP hash enhancement

1. NF service consumer sends a service request including a signed Client credentials assertion (CCA) token to authenticate against NF service producer or NRF as described in TS 33.501 [2] Clause 13.3.8. But for this solution it is also proposed to add an optional field in CCA to protect the part of the message itself. The added field is a hash of HTTP body and HTTP method.

2. NF service producer or NRF validates the CCA as described in 3GPP 33.501 Clause 13.3.8.3. But since one optional field is supposed to be added to the CCA, the receiving end point (NF service producer or NRF) also needs to compute the hash of the HTTP body and HTTP method and validates that it is identical to the hash received in the Client credentials assertion.

The updated definition of type ClientCredentialsAssertion in 3GPP 29.500 [x] is (additions in **bold** style):

Table 6.5.2-1: Updated CCA based on Table 5.2.3.2.11 -1: Definition of type ClientCredentialsAssertion

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| sub | NfInstanceId | M | 1 | This IE shall contain the NF instance ID of the NF service consumer, corresponding to the standard "Subject" claim described in IETF RFC 7519 [41], clause 4.1.2. |
| iat | integer | M | 1 | This IE shall indicate the time at which the JWT was issued, corresponding to the standard "Issued At" claim described in IETF RFC 7519 [41], clause 4.1.6. This claim may be used to determine the age of the JWT. |
| exp | integer | M | 1 | This IE shall contain the expiration time after which the client credentials assertion is considered to be expired, corresponding to the standard "Expiration Time" claim described in IETF RFC 7519 [41], clause 4.1.4.  |
| aud | array(NFType) | M | 1..N | This IE shall contain the NF type of the NF service producer and/or "NRF", for which the claim is applicable, corresponding to the standard "Audience" claim described in IETF RFC 7519 [41], clause 4.1.3.  |
| **hash** | **string** | **O** | **0..1** | **This IE contains a hash of the body of the HTTP message and HTTP method. If an NF service producer that receives this IE in the CCA included in the** **3gpp-Sbi-Client-Credentials header does not understand this IE, it shall be ignored.** |
| **halg** | **string or integer** | **O** | **0..1** | **This IE contains the hash algorithm information that is used by NF service consumer to compute the hash of the HTTP message. If an NF service producer that receives this IE in the CCA included in the** **3gpp-Sbi-Client-Credentials header does not understand this IE, it shall be ignored.** |

The details of the hash are proposed to be specified as following:

Option 1: For computation of the hash of the HTTP body and HTTP method for inclusion into the Client credential assertion, the input S to the KDF specified in Annex B of 3GPP TS 33.220 [4] is computed as follows:

 - P0 = HTTP body;

- L0 = length of the HTTP body;

- P1 = HTTP method;

- L1 = length of HTTP method.

The input key KEY is equal to null. Note that the FC value will be allocated in the normative phase.

Option 2: Alternatively to using the fixed KDF as hash function, the choice of hash function can also be done similar as in JWT or JWS. The hash algorithm is chosen by NF service Consumer. The selection of hash algorithm needs to be aligned between HTTP message sender and HTTP message receiver, i.e., mandatory to support algorithms need to be specified in a 3GPP profile. This option provides more crypto agility and is better aligned with JWT and JWS. For ease of implementation in initial deployments, the 3GPP profile for the hash algorithm could mandate the usage of a specific hash function, e.g. SHA256. This is similar to the JOSE profile of PRINS as specified in TS 33.501 [2], clause 13.2.4.9, which specifies the usage of specific AEAD and signature algorithms, but still provides crypto agility if changes should be necessary in the future.

Editor's Note: It needs to be clarified whether the usage of a new hash algorithm can also be indicated by the length.

### 6.5.3 Evaluation

Editor's Note: Provide an analysis of the risks of threats mitigated by this solution. Provide a statement on complexity/impact/backward compatibility if one would follow this solution.

\*\*\*\*\*\*END OF CHANGES\*\*\*\*\*