**3GPP TSG-SA3 Meeting #100e *S3-201801-r1***

**e-meeting, 17 - 28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **0906** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Integrity protection of service request in indirect communication |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 7.8.2020 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-16 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | With the introduction of indirect communication hop by hop security is achieved by mandating TLS between NFs, NF and SCP, and SCP and NRF at transport layer. Thus, due to the nature of SBA messages, there is no end-to-end integrity protection of the service request messages, when SCP forwards a consumer request to the producer or requests an authorization token on behalf of the consumer. This is captured in clause 13.3.8.1 by the following sentence: “Client credentials assertion do not provide integrity protection on the full service request.”Hoever, it is better, if Rel-16 clarifies how end-to-end integrity protection of the service request in indirect communication is to be done, since this may lead to attacks by Man in the Middle. For instance, a Man in the Middle can intercept the service request and try to modify the content of the message or HTTP (custom) header, which causes communication failure or could lead to DoS attack. Further, if SCP or MitM intercept the service request, modify/add the claims and send the request then to NRF, the NFc may due to this attack potentially get authorized for additional/modified claims which the attacker has entered. The MitM (e.g.SCP) would receive from NRF an OAuth access token for the modified claims, which was originally not intended by NFc. |
|  |  |
| ***Summary of change:*** | To clarify integrity protection in model C/D, when CCA token is used, an additional field for service request verification in the payload is added. Thus, since CCA is digitally signed by NFc, the receipient can verify that the service request received from SCP is the original one provided by NFc. This can be done at the same time as verifying the authenticity of NFc and therefore provides integrity protection of the service request.R1: Adding clarification on full service request, it is just a service request. Need to be specific on header part, if integrity protection is needed. |
|  |  |
| ***Consequences if not approved:*** | If the service request is not integrity protected, even thought NFc gets authenticated, CCA fails its purpose and integrity protection of the service request in indirect communication is missing. |
|  |  |
| ***Clauses affected:*** | 13.3.8.1, 13.3.8.2, 13.3.8.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **x** |  |  Other core specifications  | TS/TR 29.5XX... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*START OF CHANGES

13.3.8.1 General

Client credentials assertions are tokens signed by the NF Service Consumer. It enables the NF Service Consumer to authenticate towards the receiving end point (NRF, NF Service Producer) by including the signed token in a service request.

It includes the NF Service Consumer’s NF Instance ID that can be checked against the certificate by the NF Service Producer. The assertion includes a timestamp as basis for restriction of the lifetime of the assertion.

Client credentials assertions are expected to be more short-lived than NRF generated access tokens. So, they can be used in deployments with requirements for tokens with shorter lifetime for NF-NF communication. There is a trade-off that when the lifetime of the assertion is too short, it requires the consumer to generate a new assertion for every new service request.

Client credentials assertion cannot be used in the roaming case, as the NF Service Producer in the home PLMN will not be able to verify the signature of the NF Service Producer in the visited PLMN unless cross-certification process is established between the two PLMNs through one of the mechanisms specified in TS 33.310.

CCA may provide integrity protection of the service request.

CCA does not provide a mechanism for the NF Service Consumer to authenticate the NF Service Producer.

In this clause, Client credentials assertions are described generally for both NF-NRF communication and NF-NF communication.

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

13.3.8.2 Client credentials assertion

Client credentials assertions shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures based on JSON Web Signature (JWS) as described in RFC 7515 [45].

The Client credentials assertion shall include:

- the NF instance ID of the NF Service Consumer (subject);

- A timestamp (iat) and an expiration time (exp), and

- The NF type of the expected audience (audience), i.e. the type "NRF", "NF service Producer", or "NRF" and "NF Service Producer".

The Client credentials assertion may include:

* a service request verification, i.e. including the service request message as one of the payload values.
* a protected header list, i.e. custom headers that shall be integrity protected and not be modified by SCP.

The NF Service consumer shall digitally sign the generated Client credentials assertion based on its private key as described in RFC 7515 [45]. The signed Client credentials assertion shall include one of the following fields:

- the X.509 URL (x5u) to refer to a resource for the X.509 public key certificate or certificate chain used for signing the client authentication assertion, or

- the X.509 Certificate Chain (x5c) include the X.509 public key certificate or certificate chain used for signing the client authentication assertion.

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

13.3.8.3 Verification of Client credentials assertion

The verification of the Client credentials assertion shall be performed by the receiving node, i.e., NRF or NF Service Producer in the following way:

* It validates the signature of the JWS as described in RFC 7515 [45].
* If validates the timestamp (iat) and/or the expiration time (exp) as specified in RFC 7519 [44].

If the receiving node is the NRF, the NRF validates the timestamp (iat) and the expiration time (exp).

If the receiving node is the NF Service Producer, the NF service Producer validates the expiration time and it may validate the timestamp.

* It checks that the audience claim in the the client credentials assertion matches its own type.
* It verifies that the NF instance ID in the client credentials assertion matches the NF instance ID in the public key certificate used for signing the assertion.
* If service request verification is part of CCA, it verifies that the data included in this field is matching the service request received together with the CCA. The receiver shall also verify that the headers in the protected header list are not modified.

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