**3GPP TSG-SA3 Meeting #99e *S3-201017-r16***

**e-meeting, 11-15 May 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0808** | **rev** | **-** | **Current version:** | **16.2.0** |  |
|  | | | | | | | | |
| *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:*** | Authentication in indirect communication scenarios | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Nokia, Nokia Shanghai Bell, Huawei, Hisilicon, Mavenir, CableLabs | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | | 2020-04-30 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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 can be 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:*** | | At SA3#98bis-e, the following agreement was made: "NF to NRF auth could be based on direct mutual TLS or hop-by-hop TLS." This CR intends to implement the agreement in normative text. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Describes authentication between NF and NRF, and between NFs, in indirect communication scenarios. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Authentication for eSBA indirect communication scenarios not specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.3.1, 13.3.1.1 (new), 13.3.1.2 (new), 13.3.1.3 (new), 13.3.2, 13.3.2.1 (new), 13.3.2.2 (new), 13.3.2.3 (new), 13.3.2.4 (new), 13.3.8 (new), 13.3.8.0 (new), 13.3.8.1 (new), 13.3.8.2 (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... 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:*** | | *S3-201017 merges S3-201129, S3-201130,* S3-201093, S3-201235 | | | | | | | | |

START OF CHANGES

### 13.3.1 Authentication and authorization between network functions and NRF

#### 13.3.1.1 Direct communication

NRF and NF shall authenticate each other during discovery, registration, and access token request.

In direct communication, NF and NRF shall use one of the following methods for authentication:

* If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for mutual authentication of the NRF and NF.
* If the PLMN does not use protection at the transport layer, mutual authentication of NRF and NF may be implicit by NDS/IP or physical security (see clause 13.1).

#### 13.3.1.2 Indirect communication

In indirect communication, NF and the NRF shall use one of the following methods for authentication:

- Mutual authentication between NF and NRF provided by the transport layer protection solution.

- Client credentials assertion and authentication as specified in clause 13.3.8.

NOTE 1a: Client credentials assertion authentication is based on a client credentials assertion sent by the NF Service Consumer to the NRF via an intermediate such as the SCP. It does not provide authentication of the NRF towards the NF Service Consumer or protection of the service request sent by the NF Service Consumer to the NRF.

- Implicit, by relying on authentication between NF Service Consumer and SCP, and between SCP and NRF, provided by the hop-by-hop security protection at the transport layer, NDS/IP , or physical security.

NOTE 1b: Mutual authentication between NF Service Consumer and NRF is not achieved with hop-by-hop security.

NOTE 1c: If only hop-by-hop security is used in a PLMN, the NRF is not able to verify that an access token request sent by SCP on behalf of a certain NF consumer, is actually authorized by this consumer.

#### 13.3.1.3 Authorization of discovery request and error handling

When NRF receives message from unauthenticated NF, NRF shall support error handling, and may send back an error message. The same procedure shall be applied vice versa.

After successful authentication between NRF and NF, the NRF shall decide whether the NF is authorized to perform discovery and registration.

In the non-roaming scenario, the NRF authorizes the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF service and the type of the NF service consumer, as described in clause 4.17.4 of TS23.502 [8].In the roaming scenario, the NRF of the NF Service Provider shall authorize the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF Service, the type of the NF service consumer and the serving network ID.

If the NRF finds NF service consumer is not allowed to discover the expected NF instances(s) as described in clause 4.17.4 of TS 23.502[8], NRF shall support error handling, and may send back an error message.

NOTE 1: When a NF accesses any services (i.e. register, discover or request access token) provided by the NRF , the OAuth 2.0 access token for authorization between the NF and the NRF is not needed.

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

33.501

13.3.2 Authentication and authorization between network functions

#### 13.3.2.1 Direct communication

In direct communication, authentication between network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between NFs.

- If the PLMN does not use protection at the transport layer, authentication between NFs within one PLMN may be implicit by NDS/IP or physical security (see clause 13.1).

If the PLMN uses token-based authorization, the network shall use protection at the transport layer as described in clause 13.1.

#### 13.3.2.2 Indirect communication

In indirect communication scenarios, the NF Service Producer and NF Service Consumer shall use implicit authentication by relying on authentication between NF Service Consumer and SCP, and between SCP and NF Service Producer, provided by the transport layer protection solution, NDS/IP, or physical security.

NOTE 0: Mutual authentication between NF service consumer and NF Service producer is not achieved with hop-by-hop security.

If the PLMN uses token-based authorization as specified by clause 13.4.1.X and the PLMN’s policy mandates that the NRF authenticates the NF Service Consumer before granting an access token, the access token indicates to the NF Service Producer that the NF Service Consumer has been authenticated by the NRF.

If additional authentication of the NF Service Consumer is required, the NF Service Producer authenticates the NF Service Producer at the application layer using Client credentials assertion and authentication as specified in clause 13.3.8.

The NF service consumer authentication based on Client credentials assertion and authentication is optional to use, and based on operator policy.

#### 13.3.2.3 Inter-PLMN NF to NF communication

NOTE 1: void.

NOTE 2: void.

Authentication between network functions in different PLMN is implicit by authentication between NF-SEPP as in clause 13.3.3, SEPP-SEPP as in clause 13.2 and SEPP-NF as in clause 13.3.3, and (for indirect communication scenarios) SCP-SEPP as in clause 13.3.5.

The present document does not provide a standardised solution for binding 5G SBA REST Service Operations between the PLMN V-SMF and H-SMF over N16 / N32 to GTP-U over N9 in roaming scenarios. To prevent injection or spoofing of UP traffic over N9, it is recommended to use a common firewall that can correlate HTTP/2 methods and GTP-U in order to bind and filter out any malicious traffic on N9. Use of a common firewall may place other implementation restrictions (e.g. co-location of SMF, SEPP and UPF) in order to allow use of a common firewall.

#### 13.3.2.4 Error handling

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

### 13.3.8 Client credentials assertion and authentication

#### 13.3.8.0 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.

Client credentials assertion do not provide integrity protection on the full service request. Neither does it 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.

#### 13.3.8.1 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 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.

#### 13.3.8.2 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.

END OF CHANGES