**3GPP TSG-SA3 Meeting #116 *S3-242630***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | Split between authentication and authorization | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA\_Ph2 | | | | |  | ***Date:*** | | | 2024-05-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 33.501 specification text evolved over time. It started with authentication and authorization in clause 13.3. But later on a specific clause 13.4 on authorization was introduced. The headlines of 13.3 and 13.4 led several times to discussion. This CR fixes this by referencing to 13.4 where references are missing, because indeed, at some places 13.3 also talks about authorization. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Referencing clause 13.4 for authorization, where missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Continuous misunderstandings when arguing about authentication and authorizations. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.3.1.1, 13.3.1.2, 13.3.2.1, 13.3.2.2, 13.3.3, 13.3.5 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | ***S3-241860*** | | | | | | | | |

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

13.3 Authentication and static authorization

13.3.0 Static authorization

Static authorization is based on local authorization policy at the NRF and the NF Service Producer. It can be used when token-based authorization is not used.

During the Nnrf\_NFDiscovery procedure, the NRF ensures that the NF Service Consumer is authorized to discover the NF Service Producer service(s) as specified in clause 13.3.1.3 of this document.

If token-based authorization is not used within one PLMN and the NF Service Producer receives a service request, the NF Service Producer shall check authorization of the NF Service Consumer based on its local policy. If the NF Service Consumer is authorized to receive the service requested, the NF Service Producer shall grant the NF Service Consumer access to the service API.

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 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 (CCA) based authentication as specified in clause 13.3.8.

NOTE 1: Client credentials assertion authentication is based on a CCA token sent by the NF Service Consumer to the NRF via an intermediate such as the SCP. CCA based authentication 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, i.e. 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 2: Mutual authentication between NF Service Consumer and NRF is not achieved with hop-by-hop security.

NOTE 3: 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 Service 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 Producer 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: Void.

When a NF consumes the Nnrf\_NFManagement or the Nnrf\_NFDiscovery services provided by the NRF, the usage of the OAuth 2.0 access token for authorization between the NF and the NRF is optional.

13.3.2 Authentication 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 13.4.1.2 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 Consumer at the application layer using CCA based authentication as specified in clause 13.3.8.

The NF Service Consumer authentication based on CCA based 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

The Inter-PLMN UP Security functionality (IPUPS) as described in clauses 4.2.2 and 5.9.3.4 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.

13.3.2.4 Error handling

When an NF receives a message from an unauthenticated NF, the receiving NF shall support error handling, and may send back an error message.

13.3.3 Authentication between SEPP and network functions

NOTE 1: This clause also describes authentication between SEPP and NRF, because the NRF is a network function.

Authentication between SEPP and network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between SEPP and NFs.

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

A network function and the SEPP shall mutually authenticate before the SEPP forwards messages sent by the network function to network functions in other PLMN, and before the SEPP forwards messages sent by other network functions in other PLMN to the network function.

13.3.4 Authentication and authorization between SEPPs

Authentication and authorization between SEPPs in different PLMNs is defined in clause 13.2.

13.3.5 Authentication between SEPP and SCP

Authentication between SEPP and SCP within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between SEPP and SCP.

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

A SCP and the SEPP shall mutually authenticate before forwarding incoming or outgoing requests.

13.3.6 Authentication and static authorization between SCP and network functions

The SCP and network functions shall use one of the following methods described in clause 13.1 to mutually authenticate each other before service layer messages can be exchanged on that interface:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for mutual authentication of the SCP and the network functions.

- If the PLMN does not use protection at the transport layer, mutual authentication of the SCP and network functions may be implicit by NDS/IP or physical security.

Authentication between the SCP and the Network Function may be implicit by co-location.

Authorization between the SCP and NFs is based on local authorization policy. Regarding the authorization of access token requests sent by an SCP on behalf of an NF Service Consumer, NOTE 3 in clause 13.3.1.2 applies.

13.3.7 Authentication and static authorization between SCPs

SCPs shall use one of the following methods as described in 13.1 to mutually authenticate each other before service layer messages can be exchanged on that interface:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for mutual authentication of the SCPs.

- If the PLMN does not use protection at the transport layer, mutual authentication of the two SCPs may be implicit by NDS/IP or physical security.

Authorization between SCPs is based on local authorization policy.

13.3.8 Client credentials assertion based authentication

13.3.8.1 General

The Client credentials assertion (CCA) is a token 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 CCA includes a timestamp as basis for restriction of its lifetime.

CCAs 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 CCA is too short, it requires the NF Service Consumer to generate a new CCA for every new service request.

The CCA 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 Consumer 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 does 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, CCAs are described generally for both NF-NRF communication and NF-NF communication.

13.3.8.2 Client credentials assertion

CCAs 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 CCA 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" and/or the NF type of the NF Service Producer.

The NF Service Consumer shall digitally sign the generated CCA based on its private key as described in RFC 7515 [45]. The signed CCA 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.

13.3.8.3 Verification of Client credentials assertion

The verification of the CCA 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].
* It 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 CCA matches its own type.
* It verifies that the NF instance ID of the NFc in the CCA matches the NF instance ID in the public key certificate used for signing the CCA.

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