**3GPP TSG-SA3 Meeting #100e *S3-201798-r5***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0903** | **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:*** | Authentication and static authorization | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | | 27.8.2020 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | Clarifications needed related to which model is in use, consistant usage of accronyms CAA, NFp, NFc to avoid misspellings and allow better reading.  Some wrong or not clarified NFp/NFc needs to be corrected  Clause 13.3.1.3 NOTE 1 is not fitting.  General clause missing.  In 13.3.8.1 wrong name: NF Producer -> NFc  In 13.3.8.3 missing clarification that NF Instance ID in the public key certificate as specified in 3GPP TS 33.310 needs to be present for the verification of NF instance ID in CCA.  Revision 1: reverting the short names NFp/NFc to full names, reverting 13.3 to full title  Revision 2: addressing e-meeting comments, moving intro to 13.3.0 to 13.0 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarifications added related to which model is in use.  Consistant usage of NF Service Producer / NF Service Consumer and CAA acronym, intro in abreviation clause.  In 13.3.1.2 NF -> NFc; further NOTE 1 clarification/rewrite; also NOTE 3  In 13.3.1.3 Provider -> Producer corrected; -> NFp used  NOTE 1 deleted,cause not fitting here.  Reference to model A and B in direct comm.  13.3.8 - corrections NF & missing clarification added as NOTE that NF Instance ID in the public key certificate as specified in 3GPP TS 33.310 needs to be present for the verification of NF instance ID in CCA. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misunderstanding of spec | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.2, 13.0 (new), 13.3.1.1, 13.3.1.2, 13.3.1.3, 13.3.2.1, 13.3.2.2, 13.3.4, 13.3.8, 13.3.8.1, 13.3.8.2, 13.3.8.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Revision of S3-201798 | | | | | | | | |

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

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

5GC 5G Core Network

5G-AN 5G Access Network

5G-RG 5G Residential Gateway

NG-RAN 5G Radio Access Network

5G AV 5G Authentication Vector

5G HE AV 5G Home Environment Authentication Vector

5G SE AV 5G Serving Environment Authentication Vector

ABBAAnti-Bidding down Between Architectures

AEAD Authenticated Encryption with Associated Data

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

AMF Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF Authentication credential Repository and Processing Function

AUSF Authentication Server Function

AUTN AUthentication TokeN

AV Authentication Vector

AV' transformed Authentication Vector

BAP Backhaul Adaptation Protocol

BH Backhaul

CCA Client Credentials Assertion

Cell-ID Cell Identity as used in TS 38.331 [22]

CHO Conditional Handover

CIoT Cellular Internet of Things

cIPX consumer's IPX

CKSRVCC Cipher Key for Single Radio Voice Continuity

CP Control Plane

cSEPP consumer's SEPP

CTR Counter (mode)

CU Central Unit

DN Data Network

DNN Data Network Name

DU Distributed Unit

EAP Extensible Authentication Protocol

EDT Early Data Transmission

EMSK Extended Master Session Key

EPS Evolved Packet System

FN-RG Fixed Network RG

gNB NR Node B

GUTI Globally Unique Temporary UE Identity

HRES Hash RESponse

HXRES Hash eXpected RESponse

IAB Integrated Access and Backhaul

IKE Internet Key Exchange

IKSRVCC Integrity Key for Single Radio Voice Continuity

IPUPS Inter-PLMN UP Security

IPX IP exchange service

KSI Key Set Identifier

KSISRVCC Key Set Identifier for Single Radio Voice Continuity

LI Lawful Intercept

MN Master Node

MO-EDT Mobile Originated Early Data Transmission

MT-EDT Mobile Terminated Early Data Transmission

MR-DC Multi-Radio Dual Connectivity

MSK Master Session Key

N3IWF Non-3GPP access InterWorking Function

NAI Network Access Identifier

NAS Non Access Stratum

NDS Network Domain Security

NEA Encryption Algorithm for 5G

NF Network Function

NG Next Generation

ng-eNB Next Generation Evolved Node-B

ngKSI Key Set Identifier in 5G

N5CW Non-5G-Capable over WLAN

N5GC Non-5G-Capable

NIA Integrity Algorithm for 5G

NR New Radio

NR-DC NR-NR Dual Connectivity

NSSAI Network Slice Selection Assistance Information

PDN Packet Data Network

PEI Permanent Equipment Identifier

pIPX producer's IPX

PRINS PRotocol for N32 INterconnect Security

pSEPP producer's SEPP

PUR Preconfigured Uplink Resource

QoS Quality of Service

RES RESponse

SCG Secondary Cell Group

SEAF SEcurity Anchor Function

SCP Service Communication Proxy

NOTE: Void. Security Gateway

SEPP Security Edge Protection Proxy

SIDF Subscription Identifier De-concealing Function

SMC Security Mode Command

SMF Session Management Function

SN Secondary Node

SN Id Serving Network Identifier

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TLS Transport Layer Security

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TWAP Trusted WLAN Access Point

TWIF Trusted WLAN Interworking Function

TSC Time Sensitive Communication

UE User Equipment

UEA UMTS Encryption Algorithm

UDM Unified Data Management

UDR Unified Data Repository

UIA UMTS Integrity Algorithm

ULR Update Location Request

UP User Plane

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

USIM Universal Subscriber Identity Module

XRES eXpected RESponse

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

## 13.0 General

This clause describes the different aspects of service based interfaces.

Clause 13.1 describes the protection at the network or transport layer addressing TLS protection between NF and SEPP (clause 13.1.1), protection between SEPPs (clause 13.1.2).

Clause 13.2 describes the application layer security on the N32 interface addressing for N32-c connection between SEPPs (clause 13.2.2) key agreement and parameter exchange (clause 13.2.2.2) and error detection and handling in the SEPP (clause 13.2.2.3). Clause 13.2 further describes N32-f context clause 13.2.2.4), while clause 13.2.3 addresses the protection policies for N32 application layer solution and clause 13.2.4 the N32-f connection between SEPPs.

Clause 13.3. describes authentication and static authorization between NFs and NRF (clause 13.3.1), between NFs (clause 13.3.2), between SEPP and NFs (clause 13.3.3), between SEPPs (clause 13.3.4), between SEPP and SCP (clause 13.3.5), between SCP and NFs (clause 13.3.6), and between SCPs (clause 13.3.7). Clause 13.3.8 introduces client credentials assertion (CCA).

Clause 13.4 focus is on authorization of the NF service access.

Clause 13.5 addresses the aspects of security capability negotiation between SEPPs.

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

13.3 Authentication and static authorization

13.3.1 Authentication and authorization between network functions and NRF

13.3.1.1 Direct communication

NF and NRF 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 since it is not mutually authenticated. It also does not provide protection of the service request sent by the NF Service Consumer to the NRF since no integrity protection is applied as explained in 13.3.8.

- 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: 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.

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 13.4.1.2 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 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

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

13.3.3 Authentication and authorization between SEPP and network functions

NOTE 1: This clause also describes authentication and authorization 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 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.

Editor's Note: Authoriziation between SCP and NFs is ffs.

13.3.7 Authentication and 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.

Editor's Note: Authorization between SCPs is ffs.

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

CCA tokens 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", "NF Service Producer", or "NRF" and "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.

NOTE: NF Instance ID in the public key certificate as specified in 3GPP TS 33.310 needs to be present for the verification of NF instance ID in CCA.

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