**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220243-r1***

**e-meeting, 14 - 25 February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST**  |
|  |
|  | **33.310** | **CR** | **draft-CR** | **rev** |  | **Current version:** | **16.8.0** |  |
|  |
| *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:***  |  Clarification on the certificate profile for SCP and SEPP |
|  |  |
| ***Source to WG:*** | Ericsson, Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 2022-02-07 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Clarify the certificate profile for SCP and SEPP. |
|  |  |
| ***Summary of change:*** | Editorial change to replace SECOP to SCP.Add one clause to clarify that NF certificate profile requirements are applicable to SCP certificate profile with some deviations.Add one clause to clarify that separate TLS entity certificate profile requirements may be applied for SEPP used for different use cases, and NF certificate profile requirements are applicable to SEPP intraconnect and interconnect certificate profile with some deviations. |
|  |  |
| ***Consequences if not approved:*** | Inconsistent implementation which may cause interoperability problems. |
|  |  |
| ***Clauses affected:*** | 6.1.3c.1, 6.1.3c.2, 6.1.3c.x (new), 6.1.3c.y (new), 6.1.3c.y.1 (new), 6.1.3c.y.2 (new), 6.1.3c.y.3 (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:*** | S3-214290 |

### \*\*\* BEGIN CHANGES 1 \*\*\*

### 6.1.3c SBA Certificate profile

#### 6.1.3c.1 Introduction

Clause 6.1.3c profiles the certificates to be used for 5GC Service Based Architecture (SBA).

Different TLS entity certificate profile requirements may be applied to intra-domain and/or inter-domain SBA for NF producers, NF consumers and NRF instances, Service Communication Proxy (SCP) nodes, and Security Edge Protection Proxy (SEPP) nodes applicable to 3GPP 5GC roaming. A separate TLS entity certificate profile is also needed to cover the usage of the certificates issued by the InterconnectionCA(s) for inter-domain SBA context for TLS connections between SEPP nodes. Furthermore, separate TLS entity certificate profile requirements may be applied for Service Communication Proxy (SCP) needed for 3GPP 5GC SBA Indirect Communication model architectural Options C and D.

#### 6.1.3c.2 General SBA Certificate profile

The following additions and deviations to the common profiles shall hold for all SBA-related entities (NFs, SCPs, SEPPs):

- Signature algorithm: RSAEncryption need not be supported.

- ECDSA is recommended for TLS entity certificates with 5GC Service Based Architecture (SBA).

### \*\*\* END CHANGES 1 \*\*\*

### \*\*\* BEGIN CHANGES 2 \*\*\*

#### 6.1.3c.x SCP certificate profile

TLS certificates shall be directly signed by the CA in the operator domain that the SCP entity belongs to.

The same requirements to the NF certificate profile as listed in clause 6.1.3c.3 apply, except for the following requirements that are not applicable to the SCP certificate profile:

- The following requirement does not need to be supported: "subjectAltName should (in TLS server certificates) contain URI-ID with the HTTPS URI(s) for the apiRoot of a Network Function producer instance for the NF service API(s) that it provides; using wildcard URIs should be avoided";

- The following requirement does not need to be supported: "subjectAltName should (in TLS server certificates) contain URI-IDs with the HTTPS URI(s) for the apiRoot of a Network Function consumer instance for the NF service callback URI(s) that it provides; using wildcard URIs should be avoided".

### \*\*\* END CHANGES 2 \*\*\*

### \*\*\* BEGIN CHANGES 3 \*\*\*

#### 6.1.3c.y SEPP certificate profiles

##### 6.1.3c.y.1 Introduction

Separate TLS entity certificate profile requirements may be applied for SEPP during different use cases.

SEPP intraconnect certificate profile requirements are applied for SEPP when connecting to other NFs/SCPs in the same operator domain.

SEPP interconnect certificate profile requirements are applied for SEPP when connecting to other SEPPs in different domains.

NF certificate profile requirements are applied for SEPP when providing the Nsepp\_Telescopic\_FQDN\_Mapping service to the NFs in the same operator domain.

##### 6.1.3c.y.2 SEPP intraconnect certificate profile

TLS certificates used between a SEPP and other NFs/SCPs in the same domain shall be directly signed by the CA in the operator domain that the SEPP entity belongs to.

The same requirements to the NF certificate profile as listed in clause 6.1.3c.3 apply, except for the following requirements that are not applicable to the SEPP intraconnect certificate profile:

- The following requirement does not need to be supported: "subjectAltName should (in TLS server certificates) contain URI-IDs with the HTTPS URI(s) for the apiRoot of a Network Function producer instance for the NF service API(s) that it provides; using wildcard URIs should be avoided";

- The following requirement does not need to be supported: "subjectAltName should (in TLS server certificates) contain URI-IDs with the HTTPS URI(s) for the apiRoot of a Network Function consumer instance for the NF service callback URI(s) that it provides; using wildcard URIs should be avoided".

##### 6.1.3c.y.3 SEPP interconnect certificate profile

The same requirements to the NF certificate profile as listed in clause 6.1.3c.3 apply, except for the following requirements that are not applicable to the SEPP interconnect certificate profile:

- The following requirement does not need to be supported: "subjectAltName should (in TLS server certificates) contain URI-IDs with the HTTPS URI(s) for the apiRoot of a Network Function producer instance for the NF service API(s) that it provides; using wildcard URIs should be avoided";

- The following requirement does not need to be supported: "subjectAltName should (in TLS server certificates) contain URI-IDs with the HTTPS URI(s) for the apiRoot of a Network Function consumer instance for the NF service callback URI(s) that it provides; using wildcard URIs should be avoided".

The following additions to the NF certificate profile shall hold for the SEPP interconnect certificate profile:

- subjectAltName shall (in TLS client and server certificates) contain the PLMN-ID(s) or SNPN-ID(s) as DNS-ID(s) (that is, using dNSName subjectAltName) of the same PLMN or same SNPN where the SEPP is located, using the PlmnId as a string according to clause 5.4.4.3 of TS 29.571 [57] or PlmnIdNid according to clause 5.4.4.33 of TS 29.571 [57].

### \*\*\* END CHANGES 3 \*\*\*