**3GPP TSG-SA3 Meeting #115 *S3-240848***

Athens, Greece, 26th February - 1st March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0193** | **rev** | **-** | **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:*** | Clarify pre-registration in CA/RA for NF instance ID verification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | ACM\_SBA | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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:*** | | As specified in the clause 10.3.3 of TS 33.310:  *Operator RA/CA should be able to verify that the nfinstanceID in the certificate signing request (‘ir’ and ‘cr’ messages in CMP protocol) belongs to the NF instance requesting the certificate.*  *During the set up of initial trust between NF and operator RA/CA, the operator RA/CA gets to know the NF identity (nfInstanceID), that can be verified at the certificate enrolment and renewal procedures.*  But it is not clear how does the operator CA/RA get to know the NF instance ID when an Initial Authentication Key is used to setup initial trust. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify certain NF profile parameters (at least including the NF instance ID) shall be pre-registered in the operator CA/RA by OAM system when an Initial Authentication Key is used to setup initial trust, and the pre-registered information is used by the operator CA/RA to verify the NF instance ID during enrolment procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No clear specification about how does the operator CA/RA get to know the NF instance ID when an Initial Authentication Key is used to setup initial trust. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 10.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* BEGIN OF CHANGES \*\*\*

### 10.2.3 Procedure

Figure 10.2.3-1 depicts the procedure for the set-up of initial trust in 5GC NFs.



Figure 10.2.3-1: Procedure for set up of initial trust

Prerequisites of the procedure:

- If the initial trust has been established by initial digital certificate or OAM signature, the public root certificate of the OAM local CA or the OAM certificate shall be configured as trust anchor for the verification of the initial trust in the operator CA/RA.

- If the initial trust has been established by IAK, the key shall have been securely distributed to the NF by OAM.

- All other necessary parameters to enable the communication with operator CA/RA such as the address shall have been configured by OAM.

1. The OAM system shall configure the initial trust used for the enrolment of the operator certificate in the 5GC NF. If the initial trust is established by an initial certificate during or after the NF initialization, the local CA in the OAM system should issue such initial certificate to the NF as part of its configuration. This certificate shall be configured with the NF Instance Id in SubjectAltName field. The fetching procedure of this certificate by the NF is left to implementation.

If the initial trust has been established by IAK, certain NF profile parameters (at least including the NF instance ID) shall be pre-registered in the operator CA/RA by OAM system.

2. The 5GC NF generates the private-public key pair and the request of an EE operator certificate to the operator CA/RA. The certificate enrollment request shall include the initial trust (initial OAM issued certificate, signature of NF profile parameters, or IAK) fetched in step 1 and the NF Instance Id in SubjectAltName field of the certTemplate. The NF shall sign the request with its private key and includes the digital signature in the request.

If the initial trust is established by an initial certificate, the request shall include the certificate chain of local CA.

If the initial trust is established by IAK, the Operator CA/RA shall validate certificate enrollment request using the IAK.

If the initial trust is established by a signature of NF profile parameters, the operator CA/RA shall verify the signature in the certificate enrollment request .

NOTE: Some 5GC NF implementations may include separate certificate management function(s) acting on behalf of the NF towards the CA/RA. The requirements of this procedure are applicable to those functions.

3. Certificate enrolment request is sent to the operator CA/RA.

4. The operator CA/RA shall verify the initial trust in the request from the NF and the identity of the NF (NF Instance Id). If verified, the operator CA/RA shall generate the EE operator certificate for the NF. Specifically, by checking the digital signature on the certificate enrolment request against the trust anchor configured in step 1, and the proof of possession of the private key for the requested operator certificate. It shall verify as well that the NF Instance Id in the SubjectAltName field of the certTemplate for the Certificate Enrolment Request corresponds to the NF Instance Id of the initial OAM issued certificate, or the NF instance ID signed by the OAM issued signature. If those verifications are successful, the operator CA/RA shall generate an EE certificate for the 5GC NF.

If the initial trust has been established by IAK, the CA/RA shall issue the certificate with the pre-registered NF profile parameters (at least including NF instance ID) after successful verification of the initial trust.

5. The operator CA/RA shall include the EE certificate for the requestor NF in certificate enrolment response.

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