**3GPP TSG-SA3 Meeting #115 *draft\_S3-240954***

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

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0198** | **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 | **X** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  |  |
|  |  |
| ***Source to WG:*** | , Ericsson, AT&T, Telecom Italy |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***Work item code:*** | 9 |  | ***Date:*** | 6 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | 9 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | As described in the discussion paper S3-234551, the proposal is intended to solve the lack of automation in the deployment of additional required Root CA certificates in BTSs, and also addresses the security issues in the use of extraCerts field for transporting Root CA certificates. |
|  |  |
| ***Summary of change:*** | The change consists of two proposals to update the CMPv2 profile for BTS defined in clause 9 of TS 33.310. 1) To extend the usage of ‘extraCerts’ field to transport Root CA certificates, including the support of CMP over TLS. 2) To use ‘caPubs’ as an secure alternative to transport self-signed root CA certificates.  |
|  |  |
| ***Consequences if not approved:*** | The configuration of additional trust anchor root CA certificates required in scenarios like RAN sharing or when multiple CA hierarchies are involved will continue to be manual. The actual configuration of additional self-signed root CA certificates is on the non-secure extraCerts field, leading to potential MitM attacks. |
|  |  |
| ***Clauses affected:*** | 9.5.4.3 |
|  |  |
|  | **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:*** | S3-234552 |

\* \* \* First Change \* \* \* \*

#### 9.5.4.3 Initialization Response

The Initialization Response as specified in [4] shall contain exactly one generated base station certificate, i.e. the size of the sequence for CertResponse shall be 1 in all cases.

The following profile shall be applied to the CertRepMessage field and its sub-fields:

- The generated certificate shall be transferred to the base station in the certifiedKeyPair field of the CertResponse field. The transfer shall not be encrypted (i.e. the certificate field in CertorEncCert shall be mandatory).

The extraCerts field of the PKIMessage carrying the initialization response shall be mandatory and shall contain the operator root certificate and the RA/CA certificate (or certificates if separate private keys are used for signing of certificates and CMP messages). If the RA/CA certificate(s) are not signed by the operator root CA, also the intermediate certificates for the chain(s) up to the operator root certificate shall be included in the extraCerts field. If additional (self-signed) Root CA certificates are required, they shall be carried in the extraCerts field or caPubs field of the PKIMessage. Since extraCerts field is not under CMP message integrity protection, CMP over TLS should be used as a security transport mechanism. Since CMP already supports integrity protection for caPubs field, the use of security transport mechanisms is optional.

\* \* \* End of First Change \* \* \* \*