**3GPP TSG-SA3 Meeting #115 *S3-240583***

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **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:***  | Correction to validation of usage of X.509 certificate procedure |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2024-02-26 |
|  |  |  |  |  |
| ***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 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:*** | There is no purpose defined for certificates used in the initial trust phase either in IETF RFC 5280 or in IETF draft-ietf-lamps-nf-eku-05. The initial certificate is intended only for authentication purposes of the certificate requestor to the operator CA.  |
|  |  |
| ***Summary of change:*** | Removal of the paragraph introduced in SP-231325 |
|  |  |
| ***Consequences if not approved:*** | The actual validation of the purpose of the initial certificate cannot be implemented, as there is no purpose defined for certificates used in initial trust phase.  |
|  |  |
| ***Clauses affected:*** | 10.4 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

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

## 10.4 Validation of usage of X.509 certificate

The 5G Core NFs in SBA might need to support multiple operator certificates for different purposes, such as TLS authentication, JSON signing and JSON encryption (e.g., for signing access tokens for service access authorization, signing CCA tokens, etc.).

The Extended Key Usage (EKU) extension of the X.509 certificate as defined in IETF RFC 5280 [14] and IETF draft-ietf-lamps-nf-eku-01 [63] can be used to indicate the purpose of the X.509 certificates used in SBA. Accordingly, the CA is expected to be configured with policies to validate the purpose of the certificate and add it to the issued certificate, thus the usage of the certificate can be further verified in corresponding procedures (e.g., TLS authentication).

NOTE: RFC 5280 [14] specifies several extended key purpose identifiers (KeyPurposeIds) for X.509 certificates, but there are not extended key purpose identifiers explicitly assigned for JSON Web Signature (JWS) and JSON Web Encryption, used in 5GC. IETF draft-ietf-lamps-nf-eku-01 [63] defines extended key purpose identifiers for JWS, JWE. This is work in progress in IETF at the time of writing, therefore the procedure of validation of usage of X.509 certificate is currently applicable only to TLS authentication.

If the initial trust is set up by an initial certificate and the NF communicates with the operator CA directly, the initial certificate may also carry the Extended Key Usage extension.

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