**3GPP TSG-SA3 Meeting #115 *S3-240893-r2***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0279** | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HELP***](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 | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Certificate validation on IMS access interface | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, CableLabs | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI18 | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | According to the GSMA incoming LS (CVD-2023-0075 – Certificate validation on IMS access interface), the GSMA Co-ordinated Vulnerability Disclosure (CVD) programme’s Panel of Experts (PoE) has reviewed a submission from a group of researchers from Tsinghua University, Carleton University and CableLabs.  Some Rich Communication Services (RCS) clients use TLS to secure the IMS access interface, but do not validate that the domain name in the certificate matches the FQDN of the P-CSCF. GSMA’s RCS specifications do not specify certificate validation requirements, but instead refer to 3GPP TS 33.203. 3GPP TS 33.203 does not explicitly require the User Equipment (UE) to check the name in the certificate against the FQDN of the P-CSCF.  GSMA CVD PoE has asked 3GPP to consider updating TS 33.203 to make it clearer that UEs must check that the name in the certificate matches the FQDN of the P-CSCF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The UE shall check if the FQDN contained in the subjectAltName of the P-CSCF’s TLS certificate matches the FQDN of the P-CSCF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | A malicious P-CSCF can impersonate a legitimate P-CSCF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex O.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

## \*\*\*\*\*\*\* FIRST CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*

## O.2.1 TLS Profile for TLS based access security

When the UE and the P-CSCF implement and use TLS as specified in the present Annex O, TLS shall be implemented and used according to the TLS profile specified in TS 33.310 [24], Annex E. For all TLS versions the provisions on ciphersuites given in TS 33.310 [24], Annex E, shall apply.

NOTE 0: Void.

- Authentication of the P-CSCF

- The P-CSCF shall be authenticated by the UE by presenting a valid server certificate. The P-CSCF certificate profile shall be based on TLS certificates as presented in clause O.5.1. UEs shall validate the P-CSCF server certificate based on clause O.5.2. The UE shall check the FQDN of the P-CSCF against the subjectAltName of the TLS certificate. If they do not match, the UE shall fail the authentication of the P-CSCF.

- Authentication of the UE

- The P-CSCF shall not request a certificate in a Server Hello Message from the UE. The HN shall authenticate the UE as specified in Annex N of this specification.

- Verification of the TLS session endpoints

- In order for the UE to be able to trust the TLS session endpoint, the P-CSCF certificate shall be used during the authentication procedure.

- In order for the P-CSCF to be able to trust that the UE, which was authenticated according to Annex N, is the TLS session endpoint, the P-CSCF shall use the mechanism for associating the TLS Session ID with registration parameters IP address, port, IMPI, IMPU(s), specified in clause O.2.2, and shall have assurance that man-in-the-middle attacks can be mitigated, e.g. by following the rules in the NOTE in clause O.1.1.

- TLS session parameters

* The TLS Handshake Protocol negotiates a session, which is identified by a Session ID.

- The lifetime of a Session ID is subject to local policies of the UE and the P-CSCF. A recommended lifetime is one hour (or at least more than the re-REGISTRATION time out). The procedure for TLS session re-negotiation in IMS is specified in clauses O.4.1 and O.4.2.

- Ports

- The P-CSCF shall be prepared to accept TLS session requests on port 5061 or on a port published by the operator.

- Forwarding requests

- The procedures for forwarding requests by the edge proxy in RFC 5626 [32] shall apply to the P-CSCF when managing TLS connections.

NOTE 1: The use of RFC 5626 [32] in conjunction with TLS is needed so that terminating requests can re-use an existing TLS connection.

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