**3GPP TSG-SA3 Meeting #115 *draft\_S3-240723-r3***

**Athens, Greece, 26th Feb 2024 - 1st Mar 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1904** | **rev** | **3** | **Current version:** | **18.4.0** |  |
|  | | | | | | | | |
| *For* ***HE******LP*** *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:*** | Forcing the UDR-UDM interface to exclusively use 3GPP-defined security protocols in the non co-located deployment case | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | BSI (DE), Ericsson, China Mobile | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI18 | | | | |  | ***Date:*** | | | 2024-02-16 |
|  |  | | | |  | |  | | |  |
| ***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. | | | | | | | | *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:*** | | The implementation of specific algorithms for the transmission of long-term persistent keys carries the risk of using unverified algorithms that could be vulnerable to attacks. However, the use of the TLS protocol, as defined by TS 33.501 in section 13.1.0, allows for better transparency and interoperability. Adding a note about the different deployment cases will distinguish between the co-located and the non co-located case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Limit the UDR-UDM interface to exclusively use 3GPP-defined security protocols in the non co-located case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | It is possible that vendors may not implement a security mechanism for transporting long-term keys between the UDM and UDR. In such cases, if an attacker has network access, he can intercept the long-term keys and compromise the overall security of the network. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.8.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

### 5.8.1 Generic requirements

The long-term key(s) used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM/ARPF unprotected. If the long term key is transferred between UDR and UDM/ARPF, it shall be transferred in encrypted form. The security mechanisms defined in clause 13.1, e.g. TLS or NDS/IP shall be supported to protect the transfer of the encrypted long-term key over the Nudr interface.

NOTE 1: Security mechanisms for protection of subscription credentials in ARPF are left to implementation.

NOTE 2: Security mechanisms for storage of subscription credentials in the UDR are left to implementation.

### \*\*\*\*\*\*\*\*\*\* END OF CHANGE \*\*\*\*\*\*\*\*\*\*