**3GPP TSG-SA3 Meeting #99e *S3-201046-r1***

**e-meeting, 11 – 15 May 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v11.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.210** | **CR** | **0070** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | TLS 1.3 cipher suites | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | CryptPr | | | | |  | | ***Date:*** | | 2020-04-30 |
|  |  | | | |  | | |  | |  |
| ***Category:*** | **F** |  | | | | | | ***Release:*** | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 3GPP should support "TOP SECRET" security and so recommend ecdsa\_secp384r1\_sha384.  Typo "extention" instead of "extension". | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Text added to recommend ecdsa\_secp384r1\_sha384.  Corrected typo. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Critical 3GPP systems might use non-recommended cipher suites leading to weaknesses | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.2.2. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

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

## 6.2.2 Profiling for TLS 1.3

TLS 1.3 shall support the following restrictions and extensions:

**TLS cipher suites and Diffie-Hellman groups**

- The requirements given in section 9.1 of TLS 1.3 RFC 8446 [66] shall be followed. In addition:

- Key exchange with secp384r1 should be supported.

**TLS signature schemes**

- ecdsa\_secp384r1\_sha384 should be supported.

**TLS extensions**

- The requirements given in section 9.2 of TLS 1.3 RFC 8446 [66] shall be followed. In addition:

- The OCSP Status extension (a.k.a. certificate status request), as defined in RFC 6066 [57] and RFC 8466 [66] should be supported.

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