**3GPP TSG-SA3 Meeting #99e *S3-201045-r1***

**e-meeting, 11 – 15 May 2020**

|  |
| --- |
| *CR-Form-v11.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.210** | **CR** | **0069** | **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:***  | Elliptic Curve Group Size |
|  |  |
| ***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 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | The formulation "Elliptic curve groups of less than 255 bits shall not be supported" seems to be unclear. The intention is to allow usage of curve-25519/ed25519/W-25519 while preventing usage of other curves having less than 256 bits.3GPP should support a higher security level and so recommend ecdsa\_secp384r1\_sha384. Typo "extention" instead of "extension". |
|  |  |
| ***Summary of change:*** | Clarified text about elliptic curve group size Text added to recommend ecdsa\_secp384r1\_sha384Corrected typo |
|  |  |
| ***Consequences if not approved:*** | Critical 3GPP systems might use non-recommended elliptic curve groups leading to weaknesses. Unclear specification. |
|  |  |
| ***Clauses affected:*** | 6.2.3. |
|  |  |
|  | **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:*** |  |

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

## 6.2.3 Profiling for TLS 1.2

TLS 1.2 (RFC 5246 [50]) shall support the following restrictions and extensions:

**TLS cipher suites**

- The rules on allowed cipher suites given in TLS 1.2 (RFC 5246 [50]) shall be followed.

- In addition, the following cipher suites are mandatory to support and recommended to use:

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289 [55]

- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288 [54]

- Support of the following cipher suites is recommended:

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289 [55]

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289 [55]

- Only cipher suites with AEAD (e.g. GCM) and PFS (e.g. ECDHE, DHE) shall be supported.

**Diffie-Hellman groups**

- For ECDHE, the curve secp256r1 (P-256) as defined in RFC 8422 [71] shall be supported, secp384r1 (P-384) as defined in RFC 8422 [71] should be supported. Except curve25519, ed25519, and W-25519, elliptic curve groups of less than 256 bits shall not be supported.

- For DHE, Diffie-Hellman groups of at least 4096 bits should be supported. Diffie-Hellman groups smaller than 2048 bits shall not be supported.

**TLS hash algorithms and signature algorithms**

- Hash algorithms: SHA-256 shall be supported. SHA-384 should be supported. MD5 and SHA-1 shall not be supported.

- Signature algorithms: ecdsa, rsa\_pss\_rsae, and rsa\_pkcs1 shall be supported. Usage of rsa\_pkcs1 is not recommended.

- ecdsa\_secp384r1\_sha384 should be supported.

**TLS compression**

- The “null” compression method as specified in TLS 1.2 RFC 5246 [50] is mandatory to support. All other compression methods shall not be supported.

**TLS extensions**

- If TLS Extensions are used in conjunction with TLS, then for RFC 6066 [57] shall apply.

- The Server Name Indication (SNI) extension defined in RFC 6066 [57] shall be supported.

- The Truncated HMAC extension, defined in RFC 6066 [57] shall not be supported.

- TLS Session Resumption based on RFC 5246 [50] or RFC 5077 [59] should be supported.

- TLS servers and TLS clients shall support RFC 5746 [60]. The server shall accept client-initiated renegotiation only if secured according to RFC 5746 [60].

* The Extended Master Secret extension, defined in RFC 7627 [61] shall be supported.
* Signature Algorithms, defined in RFC 5246 [50] shall be supported.

- The Supported Groups extension, defined in RFC 8422 [71] and RFC 7919 [62] shall be supported.

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

**PSK cipher suites**

- If pre-shared key (psk) cipher suites are implemented in TLS, then RFC 4279 [63] and RFC 5489 [64] shall apply and the following cipher suites are mandatory to support and recommended to use:

- TLS\_DHE\_PSK\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5487 [65].

- TLS\_ECDHE\_PSK\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 8442 [51].

- Support of the following cipher suite is recommended:

- TLS\_ECDHE\_PSK\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 8442 [51].

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