**3GPP TSG-SA3 Meeting #100-e *S3-201655***

**E-meeting, 17- 28 Aug 2020** Revision of S3-20xxxx

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | 885 | **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 | **x** | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Clarification of ECIES Profile B uncompressed mode text |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Verizon  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  5GS\_Ph1-SEC |  | ***Date:*** |  4-8-2020 |
|  |  |  |  |  |
| ***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:*** | TS 33.501 contains confusing text regarding Home Network Public Key and the generated Ephemeral Public Key for Profile B. While clause C.3.4 specifies, “Profile B shall use point compression to save overhead and shall use the Elliptic Curve Cofactor Diffie-Hellman Primitive (section 3.3.2 of [29]) to enable future addition of profiles with cofactor h ≠ 1. For curves with cofactor h = 1 the two primitives (section 3.3.1 and 3.3.2 of [29]) are equal “. It does not mention whether this is for the shared secret (ephemeral public key) or for the Home Network Public Key. The Home Network Public Key for Profile B, configured in the USIM, can be in compressed format or uncompressed format. References to the RFCs, especially for Profile B, are missing from Annex C.In Annex C.4.4.1 for Implemeter’s test data for profile B, there is test data showing both compressed and uncompressed Ephemeral Public Keys, giving the wrong impression that for the shared secret (ephemeral public key) generation both compressed and uncompressed are allowed. Points listed above are confusing to implementers and deployment engineers.  |
|  |  |
| ***Summary of change:*** | 1) In C.3.4.0 add text that Profile B shall use point compression while generating shared secret ephemeral public key to save overhead and shall use the Elliptic Curve Cofactor Diffie-Hellman Primitive (section 3.3.2 of [29]) to enable future addition of profiles with cofactor h ≠ 1.2) In C.3.4.0 add text related to The Home Network Public Key coding and reference to RFC 5480 for Profile B.3) For the Eph. Public Key, delete the “If” from the “If compressed:” sentence under clause C.4.4.1 IMSI-based SUPI .Add additional text “Eph. Public Key (Profile B always uses point compression to generate scheme output) and delete “ Otherwised uncompressed: '049AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D1D1F44EA1C87AA7478B954537BDE79951E748A43294A4F4CF86EAFF1789C9C81F”4) For the Eph. Public Key under C.4.4.2 Network specific identifier-based SUPI, delete the “If” from the “If compressed:” sentence.Add additional text "Eph. Public Key(Profile B always uses point compression to generate scheme output).”5) Reference for IETF RFC 5480 added in clause 2.  |
|  |  |
| ***Consequences if not approved:*** | Causes implementation misalignment between UDM and USIM, SUPI encryption/decryption will fail, and authentication will not succeed. |
|  |  |
| ***Clauses affected:*** | 2, C.3.4.0, C.4.4.1, C.4.4.2,  |
|  |  |
|  | **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:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

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

## C.3.4 ECIES profiles

### C.3.4.0 General

Unless otherwise stated, the ECIES profiles follow the terminology and processing specified in SECG version 2 [29] and [30]. The profiles shall use "named curves" over prime fields.

For generating successive counter blocks from the initial counter block (ICB) in CTR mode, the profiles shall use the standard incrementing function in section B.1 of NIST Special Publication 800-38A [16] with m = 32 bits. The ICB corresponds to T1 in section 6.5 of [16].

The value of the *MAC tag* in ECIES, shall be the *L* most significant octets of the output generated by the HMAC function, where *L* equals to the maclen.

Profile A shall use its own standardized processing for key generation (section 6 of RFC 7748 [46]) and shared secret calculation (section 5 of RFC 7748 [46]). The Diffie-Hellman primitive X25519 (section 5 of RFC 7748 [46]) takes two random octet strings as input, decodes them as scalar and coordinate, performs multiplication, and encodes the result as an octet string. The shared secret output octet string from X25519 shall be used as the input Z in the ECIES KDF (section 3.6.1 of [29]). As the point compression is not applied for profile A, the prefix rule for compression type defined in [29] section 5.1.3 shall not be used in profile A, i.e., there shall be no prefix for the ephemeral public key of Profile A.

Profile B shall use point compression to save overhead and shall use the Elliptic Curve Cofactor Diffie-Hellman Primitive (section 3.3.2 of [29]) to enable future addition of profiles with cofactor h ≠ 1. For curves with cofactor h = 1 the two primitives (section 3.3.1 and 3.3.2 of [29]) are equal.

The Home Network Public Key is coded in hexadecimal digits as described in IETF RFC 7748 [46] for protection Scheme Profile A. For protection scheme Profile B, the Home Network Public Key is coded as described in IETF RFC 5480 [xx]. The length of the Home Network Public Key depends on the Protection Scheme and the form of the Home Network Public Key (e.g. compressed or uncompressed).

The profiles shall not use backwards compatibility mode (therefore are not compatible with version 1 of SECG).

### C.3.4.1 Profile A

The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following:

- EC domain parameters : Curve25519 [46]

- EC Diffie-Hellman primitive : X25519 [46]

- point compression : N/A

- KDF : ANSI-X9.63-KDF [29]

- Hash : SHA-256

- SharedInfo1 : $\overline{R}$(the ephemeral public key octet string – see [29] section 5.1.3)

- MAC : HMAC–SHA-256

- mackeylen : 32 octets (256 bits)

- maclen : 8 octets (64 bits)

- SharedInfo2 : the empty string

- ENC : AES–128 in CTR mode

- enckeylen : 16 octets (128 bits)

- icblen : 16 octets (128 bits)

- backwards compatibility mode : false

### C.3.4.2 Profile B

The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following:

- EC domain parameters : secp256r1 [30]

- EC Diffie-Hellman primitive : Elliptic Curve Cofactor Diffie-Hellman Primitive [29]

- point compression : true

- KDF : ANSI-X9.63-KDF [29]

- Hash : SHA-256

- SharedInfo1 : $\overline{R}$ (the ephemeral public key octet string – see [29] section 5.1.3)

- MAC : HMAC–SHA-256

- mackeylen : 32 octets (256 bits)

- maclen : 8 octets (64 bits)

- SharedInfo2 : the empty string

- ENC : AES–128 in CTR mode

- enckeylen : 16 octets (128 bits)

- icblen : 16 octets (128 bits)

##  - backwards compatibility mode : false

## \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## C.4.4 ECIES Profile B

### C.4.4.1 IMSI-based SUPI

The following test data set corresponds to ECIES-based encryption in the UE for IMSI-based SUPI and ECIES Profile B.

IMSI consists of MCC|MNC: '274012' and MSIN: '001002086'

**ECIES test data**

The Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with following data:

Home Network Public Key:

if compressed: '0272DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD1',

otherwise uncompressed: '0472DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD15A7DED52FCBB097A4ED250E036C7B9C8C7004C4EEDC4F068CD7BF8D3F900E3B4'

Home Network Private Key (Not available in the UE): 'F1AB1074477EBCC7F554EA1C5FC368B1616730155E0041AC447D6301975FECDA'

Eph. Public Key (Scheme output for Profile B always includes compressed form of Eph. public key):

compressed: '039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D1'

Eph. Private Key: '99798858A1DC6A2C68637149A4B1DBFD1FDFF5ADDD62A2142F06699ED7602529'

Eph. Shared Key: '6C7E6518980025B982FBB2FF746E3C2E85A196D252099A7AD23EA7B4C0959CAE'

Eph. Enc. Key: ' 8A65C3AED80295C12BD55087E965702A'

ICB: 'EF285B4061C3BAEE858AB6EC68487DAE'

Scheme-input corresponding to the plaintext-block: '00012080F6'

Cipher-text vaue: '46A33FC271'

Eph. mac key: : 'A5EBAC0BC48D9CF7AE5CE39CD840AC6C761AEC04078FAB954D634F923E901C64'

MAC-tag value: '6AC7DAE96AA30A4D'

Scheme Output:

'039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D146A33FC2716AC7DAE96AA30A4D'

### C.4.4.2 Network specific identifier-based SUPI

The following test data set corresponds to ECIES-based encryption in the UE for network specific identifier-based SUPI and ECIES Profile B.

SUPI is: verylongusername1@3gpp.com

**ECIES test data**

The Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with following data:

Home Network Public Key:

if compressed: '0272DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD1',

otherwise uncompressed: '0472DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD15A7DED52FCBB097A4ED250E036C7B9C8C7004C4EEDC4F068CD7BF8D3F900E3B4'

Home Network Private Key (Not available in the UE): 'F1AB1074477EBCC7F554EA1C5FC368B1616730155E0041AC447D6301975FECDA'

Eph. Public Key (Scheme output for Profile B always includes compressed form of Eph. public key):

compressed: '03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B39399218B244B'

Eph. Private Key: '90A5898BD29FFA3F261E00E980067C70A2B1B992A21F5B4FEF6D4DF69FE804AD'

Eph. Shared Key: 'BC3529ED79541CF8C007CE9806330F4A5FF15064D7CF4B16943EF8F007597872'

Eph. Enc. Key: '84F9A78995D39E6968047547ECC12C4F'

Scheme-input corresponding to the plaintext-block: '766572796C6F6E67757365726E616D6531'

Cipher-text value: 'BE22D8B9F856A52ED381CD7EAF4CF2D525'

Eph. mac key: '39D5517E965F8E1252B61345ED45226C5F1A8C69F03D6C91437591F0B8E48FA0'

MAC-tag value: '3CDDC61A0A7882EB'

Scheme Output:

ecckey03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B39399218B244B.cipBE22D8B9F856A52ED381CD7EAF4CF2D525.mac3CDDC61A0A7882EB

\*\*\*\* END of 2nd CHANGE \*\*\*\*

## \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

………………….

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[xx] IETF RFC 5480: “Elliptic Curve Cryptography Subject Public Key Information”.

**\*\*\*\* END of 3rd  CHANGE \*\*\*\***