**3GPP TSG-SA3 Meeting #99e *S3-201304***

**e-meeting, 11 -15 May 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0847** | **rev** |  | **Current version:** | **16.2.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | SUCI computation: implementers' test data for network specific identifier-based SUPI | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Thales | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 2020-05-01 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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:*** | | Test data for network specific identifier-based SUPI are missing to verify that protection scheme for subscriber privacy is well implemented. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of test data for specific identifier-based SUPI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No test data are available to verify that the SUCI computation is correctly implemented in case of specific identifier-based SUPI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex C.4.2, Annex C.4.3, Annex C.4.4. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

# C.4 Implementers’ test data

## C.4.1 General

The test data sets presented here are for encryption based on ECIES at UE with protection schemes defined in this clause.

## C.4.2 Null-scheme

C.4.2.1 IMSI-based SUPI

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

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

**ECIES Scheme Input**

Scheme Input: '00012080F6'

**ECIES Scheme Output**

Scheme Output: '00012080F6'

### C.4.2.2 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 null-scheme.

SUPI is: verylongusername1@3gpp.com

**ECIES Scheme Input**

Scheme Input: '766572796C6F6E67757365726E616D6531'

**ECIES Scheme Output**

Scheme Output: ~~' 766572796C6F6E67757365726E616D6531'~~ useridverylongusername1

## C.4.3 ECIES Profile A

### C.4.3.1 IMSI-based SUPI

The following test data set corresponds to SUCI computation in the UE for IMSI-based SUPI and ECIES Profile A.

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

**ECIES test data**

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

Home Network Private Key:

'c53c22208b61860b06c62e5406a7b330c2b577aa5558981510d128247d38bd1d'

Home Network Public Key:

'5a8d38864820197c3394b92613b20b91633cbd897119273bf8e4a6f4eec0a650'

Eph. Private Key:

'c80949f13ebe61af4ebdbd293ea4f942696b9e815d7e8f0096bbf6ed7de62256'

Eph. Public Key:

'b2e92f836055a255837debf850b528997ce0201cb82adfe4be1f587d07d8457d'

Eph. Shared Key:

'028ddf890ec83cdf163947ce45f6ec1a0e3070ea5fe57e2b1f05139f3e82422a'

Eph. Enc. Key:

'2ba342cabd2b3b1e5e4e890da11b65f6'

ICB:

'e2622cb0cdd08204e721c8ea9b95a7c6'

Plaintext block:

'00012080f6'

Cipher-text vaue:

'cb02352410'

Eph. mac key:

'd9846966fb7cf5fcf11266c5957dea60b83fff2b7c940690a4bfe57b1eb52bd2'

MAC-tag value:

'cddd9e730ef3fa87'

Scheme Output:

'b2e92f836055a255837debf850b528997ce0201cb82adfe4be1f587d07d8457dcb02352410cddd9e730ef3fa87’

### C.4.3.2 Network specific identifier-based SUPI

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

SUPI is: [verylongusername1@3gpp.com](mailto:verylongusername1@3gpp.com)

**ECIES test data**

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

Home Network Private Key:

'C53C22208B61860B06C62E5406A7B330C2B577AA5558981510D128247D38BD1D'

Home Network Public Key:

'5A8D38864820197C3394B92613B20B91633CBD897119273BF8e4A6f4EEC0A650'

Eph. Private Key:

'BE9EFF3E9F22A4B42A3D236E7A6C500B3F2E7E0C7449988BA800D664BF4FCD97'

Eph. Public Key:

'977D8B2FDAA7B64AA700D04227D5B440630EA4EC50F9082273A26BB678C92222'

Eph. Shared Key:

'511C1DF473BB88317F923501F8BA944FD3B667D25699DCB552DBCEF60BBDC56D'

Eph. Enc. Key:

'FE77B87D87F40428EDD71BCA69D79059'

Plaintext block:

'766572796C6F6E67757365726E616D6531'

Cipher-text vaue:

'8E358A1582ADB15322C10E515141D2039A'

Eph. mac key:

'D87B69F4FE8CD6B211264EA5E69F682F151A82252684CDB15A047E6EF0595028'

MAC-tag value:

'12E1D7783A97F1AC'

Scheme Output:

~~'977D8B2FDAA7B64AA700D04227D5B440630EA4EC50F9082273A26BB678C922228E358A1582ADB15322C10E515141D2039A12E1D7783A97F1AC’~~

ecckey977D8B2FDAA7B64AA700D04227D5B440630EA4EC50F9082273A26BB678C92222.cip8E358A1582ADB15322C10E515141D2039A.mac12E1D7783A97F1AC

## 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: 'F1AB1074477EBCC7F554EA1C5FC368B1616730155E0041AC447D6301975FECDA'

Eph. Public Key:

If compressed: '039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D1'

Otherwised uncompressed: '049AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D1D1F44EA1C87AA7478B954537BDE79951E748A43294A4F4CF86EAFF1789C9C81F'

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 identifer-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: 'F1AB1074477EBCC7F554EA1C5FC368B1616730155E0041AC447D6301975FECDA'

Eph. Public Key:

If compressed: '03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B39399218B244B'

Eph. Private Key: '90A5898BD29FFA3F261E00E980067C70A2B1B992A21F5B4FEF6D4DF69FE804AD'

Eph. Shared Key: 'BC3529ED79541CF8C007CE9806330F4A5FF15064D7CF4B16943EF8F007597872'

Eph. Enc. Key: '84F9A78995D39E6968047547ECC12C4F'

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

Cipher-text vaue: 'BE22D8B9F856A52ED381CD7EAF4CF2D525'

Eph. mac key: '39D5517E965F8E1252B61345ED45226C5F1A8C69F03D6C91437591F0B8E48FA0'

MAC-tag value: '3CDDC61A0A7882EB'

Scheme Output:

'~~03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B39399218B244BBE22D8B9F856A52ED381CD7EAF4CF2D5253CDDC61A0A7882EB'~~

ecckey03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B39399218B244B.cipBE22D8B9F856A52ED381CD7EAF4CF2D525.mac3CDDC61A0A7882EB