Annex C (normative):  
Protection schemes for concealing the subscription permanent identifier

# C.1 Introduction

The present Annex specifies the protection schemes for concealing the subscription permanent identifier. Each protection scheme is identified by a Protection Scheme Identifier. The Protection Scheme Identifiers are as follows:

null-scheme 0x0;

Profile <A> 0x1;

Profile <B> 0x2.

The values 0x3 - 0xB are reserved for future standardized protection schemes. The values 0xC - 0xF are reserved for proprietary protection schemes specified by the home operator.

Care should be taken when using unique schemes for small groups of users, as this may impact the effectiveness of the privacy scheme for these users.

The size of the Scheme Output of the protection schemes is as follows:

null-scheme size of input, i.e., size of username used in case of NAI format or MSIN in case of IMSI;

Profile <A> total of 256-bit public key, 64-bit MAC, plus size of input;

Profile <B> total of 264-bit public key, 64-bit MAC, plus size of input.

The maximum size of a Scheme Output for proprietary protection schemes shall be total of 3000 octets plus size of input .

NOTE 1: The maximum size of scheme-output was chosen to allow the introduction of quantum-resistant protection schemes.

The UE shall not send, and the network may reject SUCIs larger than the maximum size of scheme-output.

# C.2 Null-scheme

The null-scheme shall be implemented such that it returns the same output as the input, which applies to both encryption and decryption.

When using the null-scheme, the SUCI does not conceal the SUPI and therefore the newly generated SUCIs do not need to be fresh.

NOTE 1: The reason for mentioning the non-freshness is that, normally, in order to attain unlinkability (i.e., to make it infeasible for over-the-air attacker to link SUCIs together), it is necessary for newly generated SUCIs to be fresh. But, in case of the null-scheme, the SUCI does not conceal the SUPI. So unlinkability is irrelevant.

NOTE 2: The null-scheme provides no privacy protection.

# C.3 Elliptic Curve Integrated Encryption Scheme (ECIES)

## C.3.1 General

The use of ECIES for concealment of the SUPI shall adhere to the SECG specifications [29] and [30]. Processing on UE side and home network side are described in high level in clauses C.3.2 and C.3.3.

## C.3.2 Processing on UE side

The ECIES scheme shall be implemented such that for computing a fresh SUCI, the UE shall use the provisioned public key of the home network and freshly generated ECC (elliptic curve cryptography) ephemeral public/private key pair according to the ECIES parameters provisioned by home network. The processing on UE side shall be done according to the encryption operation defined in [29]. with the following changes to Section 3.8 and step 5 and 6 of Section 5.1.3.

- generate keying data K of length *enckeylen + icblen + mackeylen*.

- Parse the leftmost enckeylen octets of K as an encryption key EK, the middle icblen octets of K as an ICB, and  
the rightmost mackeylen octets of K as a MAC key MK.

The final output shall be the concatenation of the ECC ephemeral public key, the ciphertext value, the MAC tag value, and any other parameters, if applicable.

NOTE: The reason for mentioning "any other parameter, if applicable" in the final output is to allow cases, e.g. to enable the sender to send additional sign indication when point compression is used.

The Figure C.3.2-1 illustrates the UE's steps.



Figure C.3.2-1: Encryption based on ECIES at UE

## C.3.3 Processing on home network side

The ECIES scheme shall be implemented such that for deconcealing a SUCI, the home network shall use the received ECC ephemeral public key of the UE and the private key of the home network. The processing on home network side shall be done according to the decryption operation defined in [29]. with the following changes to Section 3.8 and step 6 and 7 of Section 5.1.4.

- generate keying data K of length *enckeylen* + *icblen* + *mackeylen.*

- Parse the leftmost *enckeylen* octets of *K* as an encryption key *EK*, the middle *icblen* octets of *K* as an ICB, and  
the rightmost *mackeylen* octets of *K* as a MAC key *MK*.

NOTE: Unlike the UE, the home network does not need to perform a fresh ephemeral key pair generation for each decryption. How often the home network generates new public/private key pair and how the public key is provisioned to the UE are out of the scope of this clause.

The Figure C.3.3-1 illustrates the home network's steps.



Figure C.3.3-1: Decryption based on ECIES at home network

## 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].

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]).

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 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 : (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 : (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

#### 9.11.3.3 5GS identity type

The purpose of the 5GS identity type information element is to specify which identity is requested.

The 5GS identity type is a type 1 information element.

The 5GS identity type information element is coded as shown in figure 9.11.3.3.1 and table 9.11.3.3.1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | | 2 | 1 |  |
| 5GS identity type  IEI | | | | 0  spare | | | Type of  identity | | | octet 1 |

Figure 9.11.3.3.1: 5GS identity type information element

Table 9.11.3.3.1: 5GS identity type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of identity (octet 1) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 1 |  | SUCI |
| 0 | 1 | 0 |  | 5G-GUTI |
| 0 | 1 | 1 |  | IMEI |
| 1 | 0 | 0 |  | 5G-S-TMSI |
| 1 | 0 | 1 |  | IMEISV |
| 1 | 1 | 0 |  | MAC address |
| 1 | 1 | 1 |  | EUI-64 |
|  | | | | |
| All other values are unused and shall be interpreted as "SUCI", if received by the UE. | | | | |

#### 9.11.3.4 5GS mobile identity

The purpose of the 5GS mobile identity information element is to provide either the SUCI, the 5G-GUTI, the IMEI, the IMEISV, the 5G-S-TMSI or the MAC address.

The 5GS mobile identity information element is coded as shown in figures 9.11.3.4.1, 9.11.3.4.2, 9.11.3.4.3, 9.11.3.4.4, 9.11.3.4.5, 9.11.3.4.6, 9.11.3.4.8 and 9.11.3.4.7, and table 9.11.3.4.1.

The 5GS mobile identity is a type 6 information element with a minimum length of 4.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet2  octet 3 |
| 1 | 1 | 1 | 1 | 0  spare | Type of identity | | | octet 4 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 5 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 6 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 7 |
| AMF Region ID | | | | | | | | octet 8 |
| AMF Set ID | | | | | | | | octet 9 |
| AMF Set ID (continued) | | AMF Pointer | | | | | | octet 10 |
| 5G-TMSI | | | | | | | | octet 11 |
| 5G-TMSI (continued) | | | | | | | | octet 12 |
| 5G-TMSI (continued) | | | | | | | | octet 13 |
| 5G-TMSI (continued) | | | | | | | | octet 14 |

Figure 9.11.3.4.1: 5GS mobile identity information element for type of identity "5G-GUTI"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| Identity digit 1 | | | | odd/  even  indic | Type of identity | | | octet 4 |
| Identity digit p+1 | | | | Identity digit p | | | | octet 5\* |

Figure 9.11.3.4.2: 5GS mobile identity information element for type of identity or "IMEI" or "IMEISV"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0  spare | SUPI format | | | 0  spare | Type of identity | | | octet 4 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 5 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 6 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 7 |
| Routing indicator digit 2 | | | | Routing indicator digit 1 | | | | octet 8 |
| Routing indicator digit 4 | | | | Routing indicator digit 3 | | | | octet 9 |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | Protection scheme Id | | | | octet 10 |
| Home network public key identifier | | | | | | | | octet 11 |
| Scheme output | | | | | | | | octet 12 - x |

Figure 9.11.3.4.3: 5GS mobile identity information element for type of identity "SUCI" and SUPI format "IMSI"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MSIN digit 2 | | | | MSIN digit 1 | | | | octet 12 |
| … | | | | | | | |  |
| MSIN digit n+1 | | | | MSIN digit n | | | | octet x |

Figure 9.11.3.4.3a: Scheme output for type of identity "SUCI", SUPI format "IMSI" and Protection scheme Id "Null scheme"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0  Spare | SUPI format | | | 0  Spare | Type of identity | | | octet 4 |
| SUCI NAI | | | | | | | | octet 5 - y |

Figure 9.11.3.4.4: 5GS mobile identity information element for type of identity "SUCI" and SUPI format "Network specific identifier"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 1 | 1 | 1 | 1 | 0  spare | Type of identity | | | octet 4 |
| AMF Set ID | | | | | | | | octet 5 |
| AMF Set ID (continued) | | AMF Pointer | | | | | | octet 6 |
| 5G-TMSI | | | | | | | | octet 7 |
| 5G-TMSI (continued) | | | | | | | | octet 8 |
| 5G-TMSI (continued) | | | | | | | | octet 9 |
| 5G-TMSI (continued) | | | | | | | | octet 10 |

Figure 9.11.3.4.5: 5GS mobile identity information element for type of identity "5G-S-TMSI"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0 | 0 | 0 | 0 | 0 | Type of identity | | | octet 4 |
| spare | | | | |

Figure 9.11.3.4.6: 5GS mobile identity information element for type of identity "No identity"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0  spare | 0  spare | 0  spare | 0  spare | MAURI | Type of identity | | | octet 4 |
| MAC address | | | | | | | | octet 5  octet 10 |

Figure 9.11.3.4.7: 5GS mobile identity information element for type of identity "MAC address"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0  spare | 0  spare | 0  spare | 0  spare | 0  spare | Type of identity | | | octet 4 |
| EUI-64 | | | | | | | | octet 5  octet 12 |

Figure 9.11.3.4.8: 5GS mobile identity information element for type of identity "EUI-64"

Table 9.11.3.4.1: 5GS mobile identity information element

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Type of identity (octet 4)  Bits | | | | | | | | | | | | | |
| 3 | 2 | 1 | |  | | | | | | | | | |
| 0 | 0 | 0 | | No identity (see NOTE 1) | | | | | | | | | |
| 0 | 0 | 1 | | SUCI | | | | | | | | | |
| 0 | 1 | 0 | | 5G-GUTI | | | | | | | | | |
| 0 | 1 | 1 | | IMEI | | | | | | | | | |
| 1 | 0 | 0 | | 5G-S-TMSI | | | | | | | | | |
| 1 | 0 | 1 | | IMEISV | | | | | | | | | |
| 1 | 1 | 0 | | MAC address | | | | | | | | | |
| 1 | 1 | 1 | | EUI-64 | | | | | | | | | |
| All other values are reserved. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Odd/even indication (octet 4)  Bit | | | | | | | | | | | | | |
| 4 |  |  | |  | | | | | | | | | |
| 0 |  |  | | even number of identity digits | | | | | | | | | |
| 1 |  |  | | odd number of identity digits | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the 5G-GUTI, then bits 5 to 8 of octet 4 are coded as "1111", octet 5 through 7 contain the MCC and MNC values as specified below, octet 8 through 10 contain the AMF Region ID, the AMF Set ID and the AMF Pointer values and octet 11 through 14 contain the 5G-TMSI as defined in 3GPP TS 23.003 [4]. | | | | | | | | | | | | | |
| MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | | | | | | | | | |
| MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)  The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111".  The contents of the MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| AMF Region ID (octet 8)  This field contains the binary encoding of the AMF Region ID. Bit 8 of octet 7 is the most significant bit and bit 1 of octet 7 is the least significant bit.  AMF Set ID (octet 9, octet 10 bits 7 to 8)  This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 9 is the most significant bit and bit 7 of octet 10 is the least significant bit.  AMF Pointer (octet 10 bits 1 to 6)  This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 9 is the most significant bit and bit 1 of octet 9 is the least significant bit.  5G-TMSI (octet 11 to 14)  Bit 8 of octet 11 is the most significant bit and bit 1 of octet 14 is the least significant bit. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Identity digit (octet 4 bits 5 to 8, octet 5 etc.) | | | | | | | | | | | | | |
| For the IMEI, Identity digit field is coded using BCD coding. If the number of identity digits is even then bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEI is described in 3GPP TS 23.003 [4]. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the IMEISV, Identity digit field is coded using BCD coding. Bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEISV is described in 3GPP TS 23.003 [4]. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the SUCI, bit 8 of octet 4 is spare and shall be coded as zero. Bits 5-7 of octet 4 contain the SUPI format and are coded as shown below. | | | | | | | | | | | | | |
| SUPI format (octet 4, bits 5-7)  Bits | | | | | | | | | | | | | |
| 7 | 6 | 5 | |  | |  | | | | | | | |
| 0 | 0 | 0 | |  | | IMSI | | | | | | | |
| 0 | 0 | 1 | |  | | Network Specific Identifier | | | | | | | |
| All other values are interpreted as IMSI by this version of the protocol. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the SUCI with SUPI format "IMSI", octets 5 through 7 contain the MCC and MNC values as specified below. For subsequent fields, bit 8 of octet 8 is the most significant bit and bit 1 of the last octet the least significant bit. The required fields for the SUCI are as defined in 3GPP TS 23.003 [4]. | | | | | | | | | | | | | |
| MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | | | | | | | | | |
| MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)  The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111".  The contents of the MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Routing indicator (octets 8-9)  Routing Indicator shall consist of 1 to 4 digits. The coding of this field is the responsibility of home network operator but BCD coding shall be used. If a network operator decides to assign less than 4 digits to Routing Indicator, the remaining digits shall be coded as "1111" to fill the 4 digits coding of Routing Indicator (see NOTE 2). If no Routing Indicator is configured in the USIM, the UE shall code bits 1 to 4 of octet 8 of the Routing Indicator as "0000" and the remaining digits as “1111". | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Protection scheme identifier (octet 10 bits 1 to 4) | | | | | | | | | | | | | |
| Bits | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| 4 | 3 | 2 | 1 | |  | | | | | | |
| 0 | 0 | 0 | 0 | | Null scheme | | | | | | |
| 0 | 0 | 0 | 1 | | ECIES scheme profile A | | | | | | |
| 0 | 0 | 1 | 0 | | ECIES scheme profile B | | | | | | |
| 0 | 0 | 1 | 1 | |  | | | | | | |
| to | | | | | Reserved | | | | | | |
| 1 | 0 | 1 | 1 | |  | | | | | | |
| 1 | 1 | 0 | 0 | |  | | | | | | |
| to | | | | | Operator-specific protection scheme | | | | | | |
| 1 | 1 | 1 | 1 | |  | | | | | | |
|  | | | | | | | | | | | |
| Bits 5-8 of octet 10 are spare and shall be coded as zero. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Home network public key identifier (octet 10) | | | | | | | | | | | | | |
| The Home network public key identifier (PKI) field is coded as defined in 3GPP TS 23.003 [4]. Home network public key identifier shall be coded as "00000000" when Protection scheme identifier is set to "0000" (i.e. Null scheme). | | | | | | | | | | | | | |
| Bits | | | | | | | | | | | | | |
| 8 | 7 | 6 | | 5 | | 4 | 3 | 2 | 1 |  |  | |
| 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 0 |  | Home network PKI value 0 | |
| 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 1 |  |  | |
| to | | | | | | | | | |  | Home network PKI value (1-254) | |
| 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | 0 |  |  | |
| 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | 1 |  | Reserved | |
|  | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Scheme output (octets 12 to x)  The Scheme output field consists of a string of characters with a variable length or hexadecimal digits as specified in 3GPP TS 23.003 [4]. If Protection scheme identifier is set to "0000" (i.e. Null scheme), then the Scheme output consists of the MSIN and is coded using BCD coding with each digit of the MSIN coded over 4 bits. If the MSIN includes an odd number of digits, bits 5 to 8 of octet x shall be coded as "1111". If Protection scheme identifier is not "0000" (i.e. ECIES scheme profile A, ECIES scheme profile B or Operator-specific protection scheme), then Scheme output is coded as hexadecimal digits. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the SUCI with SUPI format set to "Network specific identifier", the SUCI NAI field contains an NAI constructed as specified in subclause 28.7.3 of 3GPP TS 23.003 [4] and encoded as UTF-8 string. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the 5G-S-TMSI, bits 5 to 8 of octet 4 are coded as "1111". The coding of the 5G-S-TMSI is left open for each administration. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| AMF Set ID (octet 5, octet 6 bits 7 to 8)  This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 5 is the most significant bit and bit 7 of octet 6 is the least significant bit.  AMF Pointer (octet 6 bits 1 to 6)  This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 6 is the most significant bit and bit 1 of octet 6 is the least significant bit.  5G-TMSI (octet 7 to 10)  Bit 8 of octet 7 is the most significant bit and bit 1 of octet 10 is the least significant bit. | | | | | | | | | | | | | |
| MAC address (octets 5 to 10)  This field contains the MAC address as defined in subclause 8 of IEEE Std 802 [43].  Bit 8 of octet 5 is the most significant bit and bit 1 of octet 10 is the least significant bit.  EUI-64 (octets 5 to12)  This field contains an EUI-64 as defined in [x].  Bit 8 of octet 5 is the most significant bit and bit 1 of octet 10 is the least significant bit. | | | | | | | | | | | | | |
| MAC address usage restriction indication (MAURI) (octet 4 bit 4) | | | | | | | | | | | | | |
| Bit | | | | | | | | | | | | | |
| 4 |  |  | |  | |  | | | | | | | |
| 0 |  |  | |  | | No restrictions | | | | | | | |
| 1 |  |  | |  | | MAC address is not usable as an equipment identifier | | | | | | | |
|  | | | | | | | | | | | | | |
| For Type of identity "No identity", the length of mobile identity contents parameter shall be set to 1 and the bits 4-8 of octet 4 are spare and shall be coded as zero. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| NOTE 1: This can be used when the requested identity is not available at the UE during the identification procedure.  NOTE 2: For a 3-digit Routing Indicator, e.g "567", bits 1 to 4 of octet 8 are coded as "0101", bits 5 to 8 of octet 8 are coded as "0110", bits 1 to 4 of octet 9 are coded as "0111", bits 5 to 8 of octet 9 are coded as "1111". | | | | | | | | | | | | | |

## C.4.2 Null-scheme

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.4.3 ECIES Profile A

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'

sec

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.4.4 ECIES Profile B

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'