**3GPP TSG-SA3 Meeting #107-e *S3-220912***

e-meeting, 16 – 20 May 2022

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **1380** | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | Definition of Anonymous SUCI | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Qualcomm | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-05-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | |  |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Annex B and Annex O provide the possibility to use something called anonymous SUCI. These Annexes are informative and details of anonymous SUCI has previously been left to implementation. Now in Annex I (normative), anonymous SUCI is needed for non-public networks, especially in the cases of Credential Holder and onboarding where there might not be a HN public key available but still need to conceal UE identifier. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This CR proposes a definition of anonymous SUPI/SUCI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete specification | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.12.2, , Annex I.5 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

## \*\*\*\*\*\*\* FIRST CHANGE \*\*\*\*\*\*\*\*\*\*\*\*

### 6.12.2 Subscription concealed identifier

The SUbscription Concealed Identifier, called SUCI, is a privacy preserving identifier containing the concealed SUPI.

The UE shall generate a SUCI using a protection scheme with the raw public key, i.e. the Home Network Public Key, that was securely provisioned in control of the home network. The protection schemes shall be the ones specified in Annex C of this document or the ones specified by the HPLMN.

The UE shall construct a scheme-input from the subscription identifier part of the SUPI as follows:

* For SUPIs containing IMSI, the subscription identifier part of the SUPI includes the MSIN of the IMSI as defined in TS 23.003 [19].
* For SUPIs taking the form of a NAI, the subscription identifier part of the SUPI includes the "username" portion of the NAI as defined in NAI RFC 7542 [57].

The UE shall execute the protection scheme with the constructed scheme-input as input and take the output as the Scheme Output.

The UE shall not conceal the Home Network Identifier and the Routing Indicator.

For SUPIs containing IMSI, the UE shall construct the SUCI with the following data fields:

- The SUPI Type as defined in TS 23.003 [19] identifies the type of the SUPI concealed in the SUCI.

- The Home Network Identifier is set to the MCC and MNC of the IMSI as specified in 23.003 [19].

- The Routing Indicator as specified in TS 23.003 [19].

- The Protection Scheme Identifier as specified in Annex C of this specification.

- The Home Network Public Key Identifier as specified in this document and detailed in TS 23.003 [19].

- The Scheme Output as specified in this document and detailed in TS 23.003 [19].

For SUPIs containing Network Specific Identifier, the UE shall construct the SUCI in NAI format with the following data fields:

- realm part of the SUCI is set to the realm part of the SUPI.

- username part of the SUCI is formatted as specified in TS 23.003 [19] using the SUPI Type, Routing Indicator, the Protection Scheme Identifier, the Home Network Public Key Identifier and the Scheme Output.

NOTE 1: The format of the SUPI protection scheme identifiers is defined in Annex C.

NOTE 2: The identifier and the format of the Scheme Output are defined by the protection schemes in Annex C. In case of non-null-schemes, the freshness and randomness of the SUCI will be taken care of by the corresponding SUPI protection schemes.

NOTE 2a: In case of null-scheme being used, the Home Network Public Key Identifier is set to a default value as described in TS 23.003 [19].

The UE shall include a SUCI only in the following 5G NAS messages:

- if the UE is sending a Registration Request message of type "initial registration" to a PLMN for which the UE does not already have a 5G-GUTI, the UE shall include a SUCI to the Registration Request message, or

- if the UE responds to an Identity Request message by which the network requests the UE to provide its permanent identifier, the UE includes a SUCI in the Identity Response message as specified in clause 6.12.4.

- if the UE is sending a De-Registration Request message to a PLMN during an initial registration procedure for which the UE did not receive the registration accept message with 5G-GUTI, the UE shall include the SUCI used in the initial registration to the De-Registration Request message.

NOTE 3: In response to the Identity Request message, the UE never sends the SUPI.

The UE shall generate a SUCI using "null-scheme" only in the following cases:

- if the UE is making an unauthenticated emergency session and it does not have a 5G-GUTI to the chosen PLMN, or

- if the home network has configured "null-scheme" to be used, or

- if the home network has not provisioned the public key needed to generate a SUCI.

If the operator's decision, indicated by the USIM, is that the USIM shall calculate the SUCI, then the USIM shall not give the ME any parameter for the calculation of the SUCI including the Home Network Public Key Identifier, the Home Network Public Key, and the Protection Scheme Identifier. If the ME determines that the calculation of the SUCI, indicated by the USIM, shall be performed by the USIM, the ME shall delete any previously received or locally cached parameters for the calculation of the SUCI including the SUPI Type, the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the Protection Scheme Identifier. The operator should use proprietary identifier for protection schemes if the operator chooses that the calculation of the SUCI shall be done in USIM.

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision in the USIM an ordered priority list of the protection scheme identifiers that the operator allows. The priority list of protection scheme identifiers in the USIM shall only contain protection scheme identifiers specified in Annex C, and the list may contain one or more protection schemes identifiers. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the SUPI Type, the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the list of protection scheme identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list are obtained from the USIM.

The ME shall calculate the SUCI using the null-scheme if the Home Network Public Key or the priority list are not provisioned in the USIM.

NOTE 4: The above feature is introduced since additional protection schemes could be specified in the future for a release newer than the ME release. In this case, the protection scheme selected by older MEs may not be the protection scheme with the highest priority in the list of the USIM.

## \*\*\*\*\*\*\* NEXT CHANGE \*\*\*\*\*\*\*\*\*\*\*\*

## \*\*\*\*\*\*\* NEXT CHANGE \*\*\*\*\*\*\*\*\*\*\*\*

# I.5 SUPI privacy for standalone non-public networks

The UE shall support SUPI privacy as defined in clause 6.12 with the following exception. When using an authentication method other than 5G AKA or EAP-AKA', the location of the functionality related to SUPI privacy in the UE is out of scope.

In scenarios where the subscription identifier privacy protection mechanism using non-null scheme as described in clause 6.12.2 cannot be used and when the EAP-method supports privacy, the ME may generate an anonymous SUCI as defined in 3GPP TS 23.003 [19] (i.e. using a subscription identifier in NAI format for which the "username" part of the SUPI is "anonymous" or omitted). The UE generates the anonymous SUCI based on configuration.

The anonymous SUCI is transported over NAS layer and managed within the 5GC as a regular SUCI until de-concealment at the corresponding 5GC NF. The de-concealment of an anonymous SUCI results on an anonymous SUPI in NAI format for which the "username" part of the SUPI is "anonymous".

Furthermore, the privacy considerations for EAP TLS (given in Annex B.2.1.2) should be taken into account when using an authentication method other than 5G AKA or EAP-AKA'.

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