**3GPP TSG-CT WG1 Meeting #137-eC1-22xxxx**

**E-Meeting, 18th – 26th August 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **4592** | **rev** | **1** | **Current version:** | **17.7.1** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | EN resolution on use of anonymous SUCI |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2022-08-11 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | About the use of anonymous SUCI in SNPN case, currently in stage 3, it only implemented the required UE configuration as per subscription level and for the per UE-level configuration, there is below EN:"*Editor's note: (WI eNPN, CR 4139) it is FFS whether another UE-level configuration for usage of anonymous SUCI is needed.*".However, when seeing the related stage 2 requirements as follows, there is no any restrictions that such UE configuration has to be per subscription level and cannot be per UE level. On the contrary, the following stage 2 texts are more straightforward to be implemented as per UE level configuration.In TS 33.501 sub I.2.2.2.2 for primary authentication with AAA server of CH:"I.2.2.2 Credentials holder using AAA server for primary authentication *For construction of the SUCI, existing methods in clause 6.12 can be used. Otherwise, if the EAP method supports SUPI privacy, the UE may send an anonymous value SUCI based on configuration.*".In TS 33.501 sub I.9.2.3 for primary authentication with AAA server of DCS:"*I.9.2.3 Primary authentication using DCS**When the primary authentication is performed between the UE and the DCS, the authentication requirements and procedures defined in clause I.2 for Credential Holder shall apply with the DCS taking the role of the Credentials Holder. When the DCS uses AAA Server for primary authentication, AUSF directly selects the NSSAAF as specified in 23.501 [2]. In this case, the UDM is not involved in the procedure defined in clause I.2.2.2.2, and the step 3 to step 5 shall be skipped. When 5G AKA or EAP-AKA’ is used, the DCS shall act as a AUSF/UDM.*"In TS 33.501 sub I.5 for general requirements on SUPI privacy in SNPN:"*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 EAP-method supports privacy, the UE may send an anonymous SUCI based on configuration.**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'.* "In case of primary authentication with AAA server of CH, from protocol implementation perspective, it is a valid and reasonable option for the operatro to choose the UE-level configuration on the use of anonymous SUCI in below very common case:**The single CH provisions different credentials to enable its users to access multiple different non-subscribed SNPNs.**In this case, the CH can have a common policy for all non-subscribed SNPNs on the use of EAP method and anonymous SUCI. If so, the CH can provide a single UE-level configuration here without any further negotiations. All these can be agreed when they assigning the SLA for SNPN accessing using credentials provided by the CH.In case of primary authentication with AAA server of DCS, it is also reasonable to have a UE-level configuration as only one DCS is involved and no any coordination between DCSs is neededThis CR just provides another reasonable option for the operator to choose and it does not mandate any operator has to do so. If some operators believe such UE-level configuration cannot work well in their deployments, then to use credential-level configuration. If some operators believe such UE-level configuration can work well in their deployment, then to use it.All in all, whenever the used EAP method for primary authentication supports SUPI privacy between the UE and the CH or DCS, it could be an option for the operator to have a UE-level configuration for the use of anonymous SUCI. |
|  |  |
| ***Summary of change:*** | It proposes to resolve an EN by adding a NOTE to indicate that in some valid cases, the operator can have a UE-level configuration for the use of anonymous SUCI. |
|  |  |
| ***Consequences if not approved:*** | Stage 2 requirements on the use of anonymous SUCI are not fully implemented in stage 3, i.e. the UE-level configuration for the use of anonymous SUCI is missing. |
|  |  |
| ***Clauses affected:*** | 5.3.2 |
|  |  |
|  | **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:*** |  |

\* \* \* First Change \* \* \* \*

### 5.3.2 Permanent identifiers

A globally unique permanent identity, the 5G subscription permanent identifier (SUPI), is allocated to each subscriber for 5GS-based services. The IMSI, the network specific identifier, the GCI and the GLI are valid SUPI types. When the SUPI contains a network specific identifier, a GCI or a GLI, it shall take the form of a network access identifier (NAI). When the UE performs initial registration for onboarding services in SNPN or is registered for onboarding services in SNPN, the SUPI contains the onboarding SUPI derived from the default UE credentials for primary authentication. The UE derives the onboarding SUPI before or during the initial registration for onboarding services in SNPN and uses the derived onboarding SUPI in the initial registration for onboarding services in SNPN and while registered for onboarding services in SNPN.

The structure of the SUPI and its derivatives are specified in 3GPP TS 23.003 [4].

The UE provides the SUPI to the network in concealed form. The SUCI is a privacy preserving identifier containing the concealed SUPI. When the SUPI contains a network specific identifier, a GCI or a GLI, the SUCI shall take the form of a NAI as specified in 3GPP TS 23.003 [4].

A UE supporting N1 mode includes a SUCI:

a) in the REGISTRATION REQUEST message when the UE is attempting initial registration procedure and a valid 5G-GUTI is not available;

b) in the IDENTITY RESPONSE message, if the SUCI is requested by the network during the identification procedure; and

c) in the DEREGISTRATION REQUEST message when the UE initiates a de-registration procedure and a valid 5G-GUTI is not available.

If the UE uses the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI, the SUCI contains the unconcealed SUPI.

When:

- not operating in SNPN access operation mode; or

- operating in SNPN access operation mode but not performing initial registration for onboarding services and not registered for onboarding services;

the UE shall use the "null-scheme" if:

a) the home network has not provisioned the public key needed to generate a SUCI;

b) the home network has configured "null-scheme" to be used for the UE;

c) the UE needs to perform a registration procedure for emergency services after the failure of authentication procedure or after reception of a REGISTRATION REJECT message with the 5GMM cause #3 "Illegal UE", or to initiate a de-registration procedure before the registration procedure for emergency services was completed successfully, and the UE does not have a valid 5G-GUTI for the selected PLMN; or

d) the UE receives an identity request for SUCI during a registration procedure for emergency services or during a de-registration procedure that was initiated before the registration procedure for emergency services was completed successfully.

When operating in SNPN access operation mode and:

- performing initial registration for onboarding services; or

- registered for onboarding services;

the UE shall use the "null-scheme" if:

a) the public key needed to generate a SUCI is not configured as part of the default UE credentials for primary authentication; or

b) "null-scheme" usage is configured as part of the default UE credentials.

If:

a) the UE uses the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI;

b) the UE operates in SNPN access operation mode and:

1) an indication to use anonymous SUCI which is associated with the selected entry of the "list of subscriber data", is configured in the ME, if the UE is not registering or registered for onboarding services in SNPN; or

2) an indication to use anonymous SUCI which is associated with the default UE credentials, is configured in the ME, if the UE is registering or registered for onboarding services in SNPN;

NOTE 1: The ME can be configured with an indication to use anonymous SUCI associated with an entry of "list of subscriber data" when the EAP method associated with the credentials of the entry supports SUPI privacy at the EAP layer, or can be configured with an indication to use anonymous SUCI associated with the default UE credentials when the EAP method associated with the default UE credentials supports SUPI privacy at the EAP layer, or both.

NOTE 1a: As an alternative option, the ME can be configured with a UE-level indication to use anonymous SUCI when the EAP method used by the UE supports SUPI privacy at the EAP layer, e.g. in case of a CH has a common policy to use anonymous SUCI for all entries of the "list of subscriber data".

c) the UE does not need to perform a registration procedure for emergency services, or to initiate a de-registration procedure before the registration procedure for emergency services was completed successfully; and

d) the UE does not receive an identity request for SUCI during a registration procedure for emergency services or during a de-registration procedure that was initiated before the registration procedure for emergency services was completed successfully;

then the UE shall use anonymous SUCI as specified in 3GPP TS 23.003 [4].

A W-AGF acting on behalf of an FN-RG shall use the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI.

A W-AGF acting on behalf of an N5GC device shall use the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI.

If a UE is a MUSIM UE, the UE shall use a separate permanent equipment identifier (PEI) for each USIM, if any, and each entry of "list of subscriber data", if any, the UE operates for accessing 5GS-based services; otherwise, a UE contains and uses a permanent equipment identifier (PEI) for accessing 5GS-based services. When the UE is registered with a network by using a PEI, the UE shall not use that PEI to register with another network until the UE is de-registered from the network.

In this release of the specification, the IMEI, the IMEISV, the MAC address together with the MAC address usage restriction indication and the EUI-64 are the only PEI formats supported by 5GS. The structure of the PEI and its formats are specified in 3GPP TS 23.003 [4].

Each UE supporting at least one 3GPP access technology (i.e. satellite NG-RAN, NG-RAN, E-UTRAN, UTRAN or GERAN) contains a PEI in the IMEI format and shall be able to provide an IMEI and an IMEISV upon request from the network.

Each UE not supporting any 3GPP access technologies and supporting NAS over untrusted or trusted non-3GPP access shall have a PEI in the form of the Extended Unique Identifier EUI-64 [48] of the access technology the UE uses to connect to the 5GC.

A UE supporting N1 mode includes a PEI:

a) when neither SUPI nor valid 5G-GUTI is available to use for emergency services in the REGISTRATION REQUEST message with 5GS registration type IE set to "emergency registration";

b) when the network requests the PEI by using the identification procedure, in the IDENTITY RESPONSE message; and

c) when the network requests the IMEISV by using the security mode control procedure, in the SECURITY MODE COMPLETE message.

Each 5G-RG supporting only wireline access and each FN-RG shall have a permanent MAC address configured by the manufacturer. For 5G-CRG, the permanent MAC address configured by the manufacturer shall be a cable modem MAC address.

When the 5G-RG contains neither an IMEI nor an IMEISV, the 5G-RG shall use as a PEI the 5G-RG's permanent MAC address configured by the manufacturer and the MAC address usage restriction indication set to "no restrictions".

The W-AGF acting on behalf of the FN-RG shall use as a PEI the MAC address provided by the FN-RG and if the MAC address provided by the FN-RG is not unique or does not correspond to the FN-RG's permanent MAC address according to W-AGF's configuration, the MAC address usage restriction indication set to "MAC address is not usable as an equipment identifier" otherwise the MAC address usage restriction indication set to "no restrictions".

The 5G-RG containing neither an IMEI nor an IMEISV shall include the PEI containing the MAC address together with the MAC address usage restriction indication:

a) when neither SUPI nor valid 5G-GUTI is available to use for emergency services in the REGISTRATION REQUEST message with 5GS registration type IE set to "emergency registration";

b) when the network requests the PEI by using the identification procedure, in the IDENTIFICATION RESPONSE message; and

c) when the network requests the IMEISV by using the security mode control procedure, in the SECURITY MODE COMPLETE message.

NOTE 2: In case c) above, the MAC address is provided even though AMF requests the IMEISV.

The W-AGF acting on behalf of the FN-RG shall include the PEI containing the MAC address together with the MAC address usage restriction indication:

a) when the network requests the PEI by using the identification procedure, in the IDENTIFICATION RESPONSE message; and

b) when the network requests the IMEISV by using the security mode control procedure, in the SECURITY MODE COMPLETE message.

NOTE 3: In case b) above, the MAC address is provided even though AMF requests the IMEISV.

The W-AGF acting on behalf of the N5GC device shall use as a PEI the MAC address provided by the N5GC device and the MAC address usage restriction indication set to "no restrictions". Based on operator policy, the W-AGF acting on behalf of the N5GC device may encode the MAC address of the N5GC device using the EUI-64 format as specified in [48] and use as a PEI the derived EUI-64.

NOTE 4: The MAC address of an N5GC device is universally/globally unique.

The AMF can request the PEI at any time by using the identification procedure.

\* \* \* End of Change \* \* \* \*