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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **4559** | **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 | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification on Interaction between NSSAA and NSSRG | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNS\_Ph2 | | | | |  | ***Date:*** | | | 2022-08-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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 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:*** | | The stage 2 CRs having formal linkage below require change in the NAS protocol. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Implementation of the stage 2 CRs in the stage 3 TS.  The stage 2 CRs address the following scenario.   1. A UE has a pending NSSAI including S-NSSAI X. 2. During a registration procedure, the UE requests S-NSSAIs not sharing a common NSSRG value with S-NSSAI X. 3. The UE receives an allowed NSSAI including S-NSSAIs which the UE requested. 4. NSSAA is completed as a success for S-NSSAI X. 5. S-NSSAI X cannot be included in a new allowed NSSAI because it does not share a common NSSRG value with the existing allowed NSSAI. On the other hand, if the pending NSSAI keeps including S-NSSAI X, the UE will never be able to request S-NSSAI X.   The stage 2 CRs propose to send a new pending NSSAI not including S-NSSAI X. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | According to the current TS, a UE can request an S-NSSAI not sharing any common NSSRG value with S-NSSAIs in the pending NSSAI. And if a UE actually requests an S-NSSAI not sharing any common NSSRG value with S-NSSAIs in the pending NSSAI, the UE is allowed to use the S-NSSAI (i.e. the allowed NSSAI includes the S-NSSAI), and an NSSAA for an S-NSSAI in the pending NSSAI is completed as a success, the UE will have two incompatible (from the NSSRG pov) S-NSSAIs in the allowed NSSAI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.6.1, 4.6.2.1, 4.6.2.2, 4.6.2.4, 5.4.4.1, 5.4.4.2, 5.4.4.3, 8.2.19.1, 8.2.19.x (new), 9.11.3.37 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **x** |  | Other core specifications | | | | TS 23.501 CR 3684  TS 23.502 CR 3529 | | |
| ***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 \* \* \* \*

### 4.6.1 General

The 5GS supports network slicing as described in 3GPP TS 23.501 [8]. Within a PLMN or SNPN, a network slice is identified by an S-NSSAI, which is comprised of a slice/service type (SST) and a slice differentiator (SD). Inclusion of an SD in an S-NSSAI is optional. A set of one or more S-NSSAIs is called the NSSAI. The following NSSAIs are defined in 3GPP TS 23.501 [8]:

a) configured NSSAI;

b) requested NSSAI;

c) allowed NSSAI;

d) subscribed S-NSSAIs; and

e) pending NSSAI.

The following NSSAIs are defined in the present document:

a) rejected NSSAI for the current PLMN or SNPN;

b) rejected NSSAI for the current registration area;

c) rejected NSSAI for the failed or revoked NSSAA; and

d) rejected NSSAI for the maximum number of UEs reached.

In roaming scenarios, rejected NSSAI for the current PLMN or SNPN, or rejected NSSAI for the current registration area, or rejected NSSAI for the maximum number of UEs reached includes one or more S-NSSAI for the current PLMN and also contains a set of mapped S-NSSAI(s) if available. An S-NSSAI included in the rejected NSSAI for the failed or revoked NSSAA is an HPLMN S-NSSAI.

In case of a PLMN, a serving PLMN may configure a UE with the configured NSSAI per PLMN, and NSSRG information if the UE has indicated it support the subscription-based restrictions to simultaneous registration of network slices feature. In addition, the HPLMN may configure a UE with a single default configured NSSAI and consider the default configured NSSAI as valid in a PLMN for which the UE has neither a configured NSSAI nor an allowed NSSAI.

NOTE 1: The value(s) used in the default configured NSSAI are expected to be commonly decided by all roaming partners, e.g., values standardized by 3GPP or other bodies.

In case of an SNPN, the SNPN may configure a UE with a configured NSSAI applicable to the SNPN, and NSSRG information if the UE has indicated it support the subscription-based restrictions to simultaneous registration of network slices feature, if the UE is neither registering nor registered for onboarding services in SNPN. In addition, the credential holder may configure a single default configured NSSAI associated with the selected entry of the "list of subscriber data" or the PLMN subscription and consider the default configured NSSAI as valid in a SNPN for which the UE has neither a configured NSSAI nor an allowed NSSAI. If the UE is registering or registered for onboarding services in SNPN, the serving SNPN shall not provide a configured NSSAI to the UE.

The allowed NSSAI and the rejected NSSAI for the current registration area are managed per access type independently, i.e. 3GPP access or non-3GPP access, and is applicable for the registration area. If the UE does not have a valid registration area, the rejected NSSAI for the current registration area is applicable to the tracking area on which it was received. If the registration area contains TAIs belonging to different PLMNs, which are equivalent PLMNs, the allowed NSSAI and the rejected NSSAI for the current registration area are applicable to these PLMNs in this registration area.

The allowed NSSAI that is associated with a registration area containing TAIs belonging to different PLMNs, which are equivalent PLMNs, can be used to form the requested NSSAI for any of the equivalent PLMNs when the UE is outside of the registration area where the allowed NSSAI was received.

When the network slice-specific authentication and authorization procedure is to be initiated for one or more S-NSSAIs in the requested NSSAI or the network slice-specific authentication and authorization procedure is ongoing for one or more S-NSSAIs, these S-NSSAI(s) will be included in the pending NSSAI. When the network slice-specific authentication and authorization procedure is completed for an S-NSSAI that has been in the pending NSSAI, the S-NSSAI will be moved to the allowed NSSAI or rejected NSSAI or removed from the pending NSSAI. See further details in subclause 5.4.4. The pending NSSAI is managed regardless of access type i.e. the pending NSSAI is applicable to both 3GPP access and non-3GPP access for the current PLMN even if sent over only one of the accesses. If the registration area contains TAIs belonging to different PLMNs, which are equivalent PLMNs, the pending NSSAI is applicable to these PLMNs in this registration area.

The rejected NSSAI for the current PLMN or SNPN is applicable for the whole registered PLMN or SNPN. The AMF shall only send a rejected NSSAI for the current PLMN when the registration area consists of TAIs that only belong to the registered PLMN. If the UE receives a rejected NSSAI for the current PLMN, and the registration area also contains TAIs belonging to different PLMNs, the UE shall treat the received rejected NSSAI for the current PLMN as applicable to the whole registered PLMN.

The rejected NSSAI for the failed or revoked NSSAA includes one or more S-NSSAIs that have failed the network slice-specific authentication and authorization or for which the authorization have been revoked, and are applicable for the whole registered PLMN or SNPN.

The rejected NSSAI for the maximum number of UEs reached is applicable for the whole registered PLMN or SNPN, and the access type over which the rejected NSSAI was sent. The AMF shall send a rejected NSSAI including S-NSSAI(s) with the rejection cause "S-NSSAI not available due to maximum number of UEs reached", when one or more S-NSSAIs are indicated that the maximum number of UEs has been reached. If the timer T3526 associated with the S-NSSAI(s) was started upon reception of the rejected NSSAI for the maximum number of UEs reached, the UE may remove the S-NSSAI(s) from the rejected NSSAI including S-NSSAI(s) with the rejection cause "S-NSSAI not available due to maximum number of UEs reached", if the timer T3526 associated with the S-NSSAI(s) expires. If one or more S-NSSAIs are removed from the rejected NSSAI for the maximum number of UEs reached, the timer T3526 associated with the removed S-NSSAI(s) shall be stopped, if running. The UE shall not stop the timer T3526 if the UE selects an E-UTRA cell connected to EPC.

If the UE receives a rejected NSSAI for the maximum number of UEs reached, the registration area contains TAIs belonging to different PLMNs, which are equivalent PLMNs, the UE shall treat the received rejected NSSAI for the maximum number of UEs reached as applicable to these equivalent PLMNs when the UE is in this registration area.

NOTE 2: Based on local policies, the UE can remove an S-NSSAI from the rejected NSSAI for the failed or revoked NSSAA when the UE wants to register to the slice identified by this S-NSSAI.

NOTE 3: Based on network local policy, network slice-specific authentication and authorization procedure can be initiated by the AMF for an S-NSSAI in rejected NSSAI for the failed or revoked NSSAA when the S-NSSAI is requested by the UE based on its local policy.

NOTE 4: At least one S-NSSAI in the default configured NSSAI or at least one default S-NSSAI is recommended as not subject to network slice-specific authentication and authorization, in order to ensure that at least one PDU session can be established to access service, even when Network Slice-specific Authentication and Authorization fails.

NOTE 5: At least one S-NSSAI in the default configured NSSAI or in the subscribed S-NSSAIs marked as default S-NSSAI is recommended as not subject to network slice admission control, in order to ensure that at least one PDU session can be established to access service.

NOTE 6: The rejected NSSAI can be provided by the network via either Rejected NSSAI IE or the Extended rejected NSSAI IE.

\* \* \* Next Change \* \* \* \*

#### 4.6.2.1 General

Upon registration to a PLMN or SNPN (except for the registration procedure for periodic registration update, the initial registration for onboarding services in SNPN, and the registration procedure for mobility registration update when registered for onboarding services in SNPN), the UE shall send to the AMF the requested NSSAI which includes one or more S-NSSAIs of the allowed NSSAI for the PLMN or SNPN or the configured NSSAI for the PLMN or SNPN and corresponds to the network slice(s) to which the UE intends to register with, if:

a) the UE has a configured NSSAI for the current PLMN or SNPN;

b) the UE has an allowed NSSAI for the current PLMN or SNPN; or

c) the UE has neither allowed NSSAI for the current PLMN or SNPN nor configured NSSAI for the current PLMN or SNPN and has a default configured NSSAI. In this case the UE indicates to the AMF that the requested NSSAI is created from the default configured NSSAI.

Other than S-NSSAIs contained in the NSSAIs described above, the requested NSSAI can be formed based on the S-NSSAI(s) available in the UE (see subclause 5.5.1.3.2 for further details). In roaming scenarios, the UE shall also provide the mapped S-NSSAI(s) for the requested NSSAI, if available. The AMF verifies if the requested NSSAI is permitted based on the subscribed S-NSSAIs in the UE subscription and optionally the mapped S-NSSAI(s) provided by the UE, and if so then the AMF shall provide the UE with the allowed NSSAI for the PLMN or SNPN, and shall also provide the UE with the mapped S-NSSAI(s) for the allowed NSSAI for the PLMN or SNPN if available. The AMF shall ensure that there are not two or more S-NSSAIs of the allowed NSSAI which are mapped to the same S-NSSAI of the HPLMN or SNPN. If

a) all the S-NSSAIs included in the requested NSSAI are rejected, or the requested NSSAI was not included by the UE;

b) there is no default S-NSSAI(s) or all subscribed S-NSSAIs marked as default are not allowed; and

c) the UE is neither registering nor registered for onboarding services in SNPN and the UE is neither registering nor registered for emergency services;

then the AMF may reject the registration request (see subclauses 5.5.1.2.5 and 5.5.1.3.5 for further details).

The set of network slice(s) for a UE can be changed at any time while the UE is registered to a PLMN or SNPN, and the change may be initiated by the network or the UE. In this case, the allowed NSSAI and associated registration area may be changed during the registration procedure or the generic UE configuration update procedure. The configured NSSAI and the rejected NSSAI may be changed during the registration procedure or the generic UE configuration update procedure. The default configured NSSAI may be changed by sending a UE parameters update transparent container to the UE during the NAS transport procedure. The pending NSSAI may be changed during the registration procedure or the generic UE configuration update procedure. In addition, using the generic UE configuration update procedure, the network may trigger the registration procedure in order to update the allowed NSSAI.

The UE in NB-N1 mode does not include the requested NSSAI during the registration procedure if the 5GS registration type IE indicates "mobility registration updating", procedure is not initiated to change the slice(s) that the UE is currently registered to, and the UE is still in the current registration area. The UE does not include the requested NSSAI during the registration procedure if the 5GS registration type IE indicates "SNPN onboarding registration" or the UE is registered for onboarding services in SNPN.

The AMF does not include the allowed NSSAI during a registration procedure with the 5GS registration type IE indicating "mobility registration updating" except if the allowed NSSAI has changed for the UE. The UE considers the last received allowed NSSAI as valid until the UE receives a new allowed NSSAI. The AMF does not include the allowed NSSAI during a registration procedure with the 5GS registration type IE indicating "SNPN onboarding registration" or during a registration procedure when the UE is registered for onboarding services in SNPN.

\* \* \* Next Change \* \* \* \*

#### 4.6.2.2 NSSAI storage

If available, the configured NSSAI(s) shall be stored in a non-volatile memory in the ME as specified in annex C. For a configured NSSAI, if there is associated NSSRG information, the NSSRG information shall also be stored in a non-volatile memory in the ME as specified in annex C. For a configured NSSAI, if there is associated NSAG information, the NSAG information shall be stored in the ME. The support for NSSRG information and NSAG information by a UE or an AMF is optional.

The allowed NSSAI(s) should be stored in a non-volatile memory in the ME as specified in annex C.

Each of the configured NSSAI stored in the UE is a set composed of at most 16 S-NSSAIs. Each of the allowed NSSAI stored in the UE is a set composed of at most 8 S-NSSAIs and is associated with a PLMN identity or SNPN identity, an access type and, if the UE supports access to an SNPN using credentials from a credentials holder, the selected entry of the "list of subscriber data" or the selected PLMN subscription. Each of the configured NSSAI except the default configured NSSAI, and the rejected NSSAI is associated with a PLMN identity or SNPN identity and, if the UE supports access to an SNPN using credentials from a credentials holder, the selected entry of the "list of subscriber data" or the selected PLMN subscription. Each of the pending NSSAI stored in the UE is a set composed of at most 16 S-NSSAIs and is associated with a PLMN identity or SNPN identity and, if the UE supports access to an SNPN using credentials from a credentials holder, the selected entry of the "list of subscriber data" or the selected PLMN subscription. The S-NSSAI(s) in the rejected NSSAI for the current registration area are further associated with one or more tracking areas where the rejected S-NSSAI(s) is not available. The S-NSSAI(s) in the rejected NSSAI for the current PLMN or SNPN shall be considered rejected for the current PLMN or SNPN regardless of the access type. The S-NSSAI(s) in the rejected NSSAI for the failed or revoked NSSAA shall be considered rejected for the current PLMN or SNPN regardless of the access type. The S-NSSAI(s) in the rejected NSSAI for the maximum number of UEs reached are further associated with the access type over which the rejected NSSAI was received. There shall be no duplicated PLMN identities or SNPN identities associated with each of the list of configured NSSAI(s), pending NSSAI(s), rejected NSSAI(s) for the current PLMN or SNPN, rejected NSSAI(s) for the current registration area, rejected NSSAI(s) for the failed or revoked NSSAA, and rejected NSSAI for the maximum number of UEs reached.

The UE stores NSSAIs as follows:

a) The configured NSSAI shall be stored until a new configured NSSAI is received for a given PLMN or SNPN. The network may provide to the UE the mapped S-NSSAI(s) for the new configured NSSAI which shall also be stored in the UE. When the UE is provisioned with a new configured NSSAI for a PLMN or SNPN, the UE shall:

1) replace any stored configured NSSAI for this PLMN or SNPN with the new configured NSSAI for this PLMN or SNPN;

2) delete any stored mapped S-NSSAI(s) for the configured NSSAI and, if available, store the mapped S-NSSAI(s) for the new configured NSSAI;

3) delete any stored allowed NSSAI for this PLMN or SNPN and, if available, the stored mapped S-NSSAI(s) for the allowed NSSAI, if the UE received the new configured NSSAI for this PLMN or SNPN and the Configuration update indication IE with the Registration requested bit set to "registration requested", in the same CONFIGURATION UPDATE COMMAND message but without any new allowed NSSAI for this PLMN or SNPN included;

4) delete any stored rejected NSSAI, and stop the timer T3526 associated with the deleted rejected S-NSSAI for the maximum number of UEs reached if running;

4A) remove from the stored mapped S-NSSAI(s) for the rejected NSSAI for the current PLMN or SNPN and the stored mapped S-NSSAI(s) for the rejected NSSAI for the current registration area and the stored rejected NSSAI for the maximum number of UEs reached, the S-NSSAI(s), if any, included in the mapped S-NSSAI(s) for the new configured NSSAI for the current PLMN or SNPN (if the UE is roaming), and stop the timer T3526 associated with the deleted rejected S-NSSAI for the maximum number of UEs reached if running; and

5) delete any S-NSSAI(s) stored in the pending NSSAI that are not included in the new configured NSSAI for the current PLMN or SNPN or any mapped S-NSSAI(s), if any, stored in the pending NSSAI that are not included in the mapped S-NSSAI(s) for the configured NSSAI (if the UE is roaming);

If the UE receives an S-NSSAI associated with a PLMN ID from the network during the PDN connection establishment procedure in EPS as specified in 3GPP TS 24.301 [15] or via ePDG as specified in 3GPP TS 24.302 [16], the UE may store the received S-NSSAI in the configured NSSAI for the PLMN identified by the PLMN ID associated with the S-NSSAI, if not already included in the configured NSSAI;

The UE may continue storing a received configured NSSAI for a PLMN and associated mapped S-NSSAI(s), if available, when the UE registers in another PLMN.

NOTE 1: The maximum number of configured NSSAIs and associated mapped S-NSSAIs for PLMNs other than the HPLMN that need to be stored in the UE, and how to handle the stored entries, are up to UE implementation.

ab) The NSAG information shall be stored until:

1) a new NSAG information is received for the registered PLMN over 3GPP access; or

2) a new configured NSSAI without any associated NSAG information is received for the registered PLMN over 3GPP access.

When a new NSAG information for the registered PLMN over 3GPP access is received, the UE shall replace any stored NSAG information for the registered PLMN and its equivalent PLMN(s) with the new NSAG information for the registered PLMN.

When a new configured NSSAI without any associated NSAG information is received for the registered PLMN over 3GPP access, the UE shall delete any stored NSAG information for the registered PLMN and its equivalent PLMN(s).

NOTE 2: Whether the UE stores the NSAG information also when the UE is switched off or when the UE is deregistered from the registered PLMN over 3GPP access is implementation specific.

b) The allowed NSSAI shall be stored until:

1) a new allowed NSSAI for the same access type (i.e. 3GPP access or non-3GPP access) is received for a given PLMN or SNPN;

2) the CONFIGURATION UPDATE COMMAND message with the Registration requested bit of the Configuration update indication IE set to "registration requested" is received and contains no other parameters (see subclauses 5.4.4.2 and 5.4.4.3); or

3) the REGISTRATION ACCEPT message is received with the "NSSAA to be performed" indicator of the 5GS registration result IE set to "Network slice-specific authentication and authorization is to be performed", and the REGISTRATION ACCEPT message contains a pending NSSAI and no new allowed NSSAI as described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4.

The network may provide to the UE the mapped S-NSSAI(s) for the new allowed NSSAI (see subclauses 5.5.1.2 and 5.5.1.3) which shall also be stored in the UE. When a new allowed NSSAI for a PLMN or SNPN is received, the UE shall:

1) replace any stored allowed NSSAI for this PLMN or SNPN and its equivalent PLMN(s) for the same access type with the new allowed NSSAI for this PLMN or SNPN;

2) delete any stored mapped S-NSSAI(s) for the allowed NSSAI for this PLMN or SNPN and its equivalent PLMN(s) for the same access type and, if available, store the mapped S-NSSAI(s) for the new allowed NSSAI;

3) remove from the stored rejected NSSAI for the current PLMN or SNPN, the rejected NSSAI for the current registration area and rejected NSSAI for the maximum number of UEs reached, the S-NSSAI(s), if any, included in the new allowed NSSAI for the current PLMN or SNPN, unless the S-NSSAI in the rejected NSSAI is associated with one or more S-NSSAI(s) in the stored mapped rejected NSSAI and these mapped S-NSSAI(s) are not included in the mapped S-NSSAI(s) for the new allowed NSSAI, and stop the timer T3526 associated with the deleted rejected S-NSSAI for the maximum number of UEs reached if running;

4) remove from the stored rejected NSSAI for the failed or revoked NSSAA, the S-NSSAI(s), if any, included in the new allowed NSSAI for the current PLMN or SNPN (if the UE is not roaming) or the mapped S-NSSAI(s) for the new allowed NSSAI for the current PLMN or SNPN (if the UE is roaming);

5) remove from the stored mapped S-NSSAI(s) for the rejected NSSAI for the current PLMN or SNPN, the stored mapped S-NSSAI(s) for the rejected NSSAI for the current registration area and rejected NSSAI for the maximum number of UEs reached, the S-NSSAI(s), if any, included in the mapped S-NSSAI(s) for the new allowed NSSAI for the current PLMN or SNPN (if the UE is roaming), and stop the timer T3526 associated with the deleted rejected S-NSSAI for the maximum number of UEs reached if running; and

6) remove from the stored pending NSSAI for this PLMN or SNPN and its equivalent PLMN(s), one or more S-NSSAIs, if any, included in the new allowed NSSAI for the current PLMN or SNPN and its equivalent PLMN(s) (if the UE is not roaming) or the mapped S-NSSAI(s) for the new allowed NSSAI for the current PLMN or SNPN and its equivalent PLMN(s) (if the UE is roaming).

If the UE receives the CONFIGURATION UPDATE COMMAND message with the Registration requested bit of the Configuration update indication IE set to "registration requested" and contains no other parameters (see subclauses 5.4.4.2 and 5.4.4.3), the UE shall delete any stored allowed NSSAI for this PLMN or SNPN, and delete any stored mapped S-NSSAI(s) for the allowed NSSAI, if available;

NOTE 3: Whether the UE stores the allowed NSSAI and the mapped S-NSSAI(s) for the allowed NSSAI also when the UE is switched off is implementation specific.

c) When the UE receives the S-NSSAI(s) included in the rejected NSSAI in the REGISTRATION ACCEPT message, the REGISTRATION REJECT message, the DEREGISTRATION REQUEST message or in the CONFIGURATION UPDATE COMMAND message, the UE shall:

1) store the S-NSSAI(s) into the rejected NSSAI and the mapped S-NSSAI(s) for the rejected NSSAI based on the associated rejection cause(s);

2) if the UE receives the S-NSSAI(s) included in the Rejected NSSAI IE, or if the UE receives the S-NSSAI(s) included in the Extended rejected NSSAI IE in non-roaming case, remove from the stored allowed NSSAI for the current PLMN or SNPN and its equivalent PLMN(s), the S-NSSAI(s), if any, included in the:

i) rejected NSSAI for the current PLMN or SNPN, for each and every access type;

ii) rejected NSSAI for the current registration area, associated with the same access type; or

iii) rejected NSSAI for the maximum number of UEs reached, associated with the same access type;

3) if the UE receives the S-NSSAI(s) included in the Extended rejected NSSAI IE in roaming case, remove from the stored allowed NSSAI for the current PLMN or SNPN and its equivalent PLMN(s), the S-NSSAI(s), if any, included in the:

i) rejected NSSAI for the current PLMN or SNPN, for each and every access type;

ii) rejected NSSAI for the current registration area, associated with the same access type; or

iii) rejected NSSAI for the maximum number of UEs reached, associated with the same access type;

if the mapped S-NSSAI(s) for the S-NSSAI in the stored allowed NSSAI for the current PLMN or SNPN are stored in the UE, and the all of the mapped S-NSSAI are included in the Extended rejected NSSAI IE;

4) remove from the stored allowed NSSAI for the current PLMN or SNPN and its equivalent PLMN(s) (if the UE is not roaming) or the stored mapped S-NSSAI(s) for the allowed NSSAI (if available and if the UE is roaming), the S-NSSAI(s), if any, included in the:

i) rejected NSSAI for the failed or revoked NSSAA, for each and every access type;

ii) mapped S-NSSAI(s) for the rejected NSSAI for the current PLMN or SNPN, for each and every access type;

iii) mapped S-NSSAI(s) for the rejected NSSAI for the current registration area, associated with the same access type; or

iv) mapped S-NSSAI(s) for the rejected NSSAI for the maximum number of UEs reached, associated with the same access type;

5) if the UE receives the S-NSSAI(s) included in the Rejected NSSAI IE, or if the UE receives the S-NSSAI(s) included in the Extended rejected NSSAI IE in non-roaming case, remove from the stored pending NSSAI for the current PLMN or SNPN and its equivalent PLMN(s), the S-NSSAI(s), if any, included in the:

i) rejected NSSAI for the current PLMN or SNPN, for each and every access type;

ii) rejected NSSAI for the current registration area, associated with the same access type; or

iii) rejected NSSAI for the maximum number of UEs reached, associated with the same access type;

6) if the UE receives the S-NSSAI(s) included in the Extended rejected NSSAI IE in roaming case, remove from the stored pending NSSAI for the current PLMN or SNPN and its equivalent PLMN(s), the S-NSSAI(s), if any, included in the:

i) rejected NSSAI for the current PLMN or SNPN, for each and every access type;

ii) rejected NSSAI for the current registration area, associated with the same access type; or

iii) rejected NSSAI for the maximum number of UEs reached, associated with the same access type,

if the mapped S-NSSAI(s) for the S-NSSAI in the stored pending NSSAI are stored in the UE, and all of the mapped S-NSSAI(s) are included in the Extended rejected NSSAI IE; and

7) remove from the stored pending NSSAI for the current PLMN and its equivalent PLMN(s) or SNPN (if the UE is not roaming) or the stored mapped S-NSSAI(s) for the pending NSSAI (if available and if the UE is roaming), the S-NSSAI(s) included in the:

i) rejected NSSAI for the failed or revoked NSSAA, for each and every access type;

ii) mapped S-NSSAI(s) for the rejected NSSAI for the current PLMN or SNPN, for each and every access type;

iii) mapped S-NSSAI(s) for the rejected NSSAI for the current registration area, associated with the same access type; or

iv) mapped S-NSSAI(s) for the rejected NSSAI for the maximum number of UEs reached, associated with the same access type;

8) If the UE receives the CONFIGURATION UPDATE COMMAND message with the Registration requested bit of the Configuration update indication IE set to "registration requested" and contains no other parameters (see subclauses 5.4.4.2 and 5.4.4.3), the UE shall delete any stored rejected NSSAI.

When the UE:

1) enters state 5GMM-DEREGISTERED following an unsuccessful registration for 5GMM causes other than #62 "No network slices available" for the current PLMN or SNPN;

2) successfully registers with a new PLMN or SNPN;

3) enters state 5GMM-DEREGISTERED following an unsuccessful registration with a new PLMN; or

4) performs inter-system change from N1 mode to S1 mode and the UE successfully completes tracking area update procedure;

and the UE is not registered with the current PLMN or SNPN over another access, the rejected NSSAI for the current PLMN or SNPN and the rejected NSSAI for the failed or revoked NSSAA shall be deleted.

When the UE receive ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message provided with S-NSSAI and the PLMN ID in the protocol configuration options IE or extended protocol configuration options IE (see subclause 6.2.2 of 3GPP TS 24.301 [15]), the UE shall remove the S-NSSAI from the rejected NSSAI for the current PLMN. When the UE receive ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message provided with S-NSSAI and the PLMN ID in the protocol configuration options IE or extended protocol configuration options IE (see subclause 6.2.2 of 3GPP TS 24.301 [15]), the UE may remove the S-NSSAI from the rejected NSSAI for the maximum number of UEs reached for each and every access type, if any, and stop the timer T3526 associated with the S-NSSAI if running.

When the UE:

1) deregisters over an access type;

2) successfully registers in a new registration area over an access type;

3) enters state 5GMM-DEREGISTERED or 5GMM-REGISTERED following an unsuccessful registration in a new registration area over an access type; or

4) performs inter-system change from N1 mode to S1 mode and the UE successfully completes tracking area update procedure;

the rejected NSSAI for the current registration area corresponding to the access type shall be deleted;

d) When the UE receives the pending NSSAI in the REGISTRATION ACCEPT message or the CONFIGURATION UPDATE COMMAND message, the UE shall replace any stored pending NSSAI for this PLMN or SNPN with the new pending NSSAI received in the REGISTRATION ACCEPT message or the CONFIGURATION UPDATE COMMAND message for this PLMN or SNPN. If the UE does not receive the pending NSSAI in the REGISTRATION ACCEPT message and the "NSSAA to be performed" indicator is not set to "Network slice-specific authentication and authorization is to be performed" in the 5GS registration result IE of the REGISTRATION ACCEPT message, the UE shall delete the stored pending NSSAI, if any, for this PLMN or SNPN and its equivalent PLMN(s).

If the registration area contains TAIs belonging to different PLMNs, which are equivalent PLMNs, then for each of the equivalent PLMNs, the UE shall replace any stored pending NSSAI with the pending NSSAI received in the registered PLMN.

When the UE:

1) deregisters with the current PLMN or SNPN using explicit signalling or enters state 5GMM-DEREGISTERED for the current PLMN or SNPN;

2) successfully registers with a new PLMN or SNPN not in the list of equivalent PLMNs;

3) enters state 5GMM-DEREGISTERED following an unsuccessful registration with a new PLMN or SNPN; or

4) successfully initiates an attach or tracking area update procedure in S1 mode and the UE is operating in single-registration mode;

and the UE is not registered with the current PLMN or SNPN over another access, the pending NSSAI for the current PLMN or SNPN and its equivalent PLMN(s) shall be deleted;

e) When the UE receives the Network slicing indication IE with the Network slicing subscription change indication set to "Network slicing subscription changed" in the REGISTRATION ACCEPT message or in the CONFIGURATION UPDATE COMMAND message, the UE shall delete the network slicing information for each of the PLMNs or SNPNs that the UE has slicing information stored for (excluding the current PLMN or SNPN). The UE shall delete any stored rejected NSSAI and stop the timer T3526 associated with the deleted rejected S-NSSAI for the maximum number of UEs reached if running. The UE shall not delete the default configured NSSAI. Additionally, the UE shall update the network slicing information for the current PLMN or SNPN (if received) as specified above in bullets a), b), c) and d); and

f) When the UE receives the new default configured NSSAI included in the default configured NSSAI update data in the Payload container IE of DL NAS TRANSPORT message, the UE shall replace any stored default configured NSSAI with the new default configured NSSAI. In case of SNPN, the UE shall replace the stored default configured NSSAI associated with the selected entry of the "list of subscriber data" or the PLMN subscription with the new default configured NSSAI.

\* \* \* Next Change \* \* \* \*

#### 4.6.2.4 Network slice-specific authentication and authorization

The UE and network may support network slice-specific authentication and authorization.

A serving PLMN or SNPN shall perform network slice-specific authentication and authorization for the S-NSSAI(s) of the HPLMN or SNPN which are subject to it based on subscription information. The UE shall indicate whether it supports network slice-specific authentication and authorization in the 5GMM Capability IE in the REGISTRATION REQUEST message as specified in subclauses 5.5.1.2.2 and 5.5.1.3.2.

The upper layer stores an association between each S-NSSAI and its corresponding credentials for the network slice-specific authentication and authorization.

NOTE 1: The credentials for network slice-specific authentication and authorization and how to provision them in the upper layer are out of the scope of 3GPP.

The network slice-specific authentication and authorization procedure shall not be performed unless the primary authentication and key agreement procedure as specified in the subclause 5.4.1 has successfully been completed.

The AMF informs the UE about S-NSSAI(s) for which network slice-specific authentication and authorization (except for re-NSSAA) will be performed or is ongoing in the pending NSSAI. If the subscription information does not include NSSRG information, the AMF informs the UE about S-NSSAI(s) for which NSSAA procedure is completed as:

a) success in the allowed NSSAI; or

b) failure in the rejected NSSAI for the failed or revoked NSSAA.

For the case where the subscription information includes NSSRG information, see subclause 5.4.4.

The AMF stores and handles allowed NSSAI, pending NSSAI, rejected NSSAI, and 5GS registration result in the REGISTRATION ACCEPT message according to subclauses 5.5.1.2.4 and 5.5.1.3.4.

NOTE 2: The AMF maintains the NSSAA procedure status for each S-NSSAI, as specified in 3GPP TS 29.518 [20B] and the NSSAA procedure status for each S-NSSAI is not impacted by NSAC as specified in subclauses 4.6.2.5 and 4.6.3.1.

NOTE 3: Upon completion of NSSAA procedures, it can happen that the total number of S-NSSAIs which need to be included in the allowed NSSAI exceeds eight. In this case, it is up to the AMF implementation on how to pick up the S-NSSAIs included in the allowed NSSAI.

NOTE 4: It can happen that one or more S-NSSAIs included in the received allowed NSSAI, are not the S-NSSAIs that the UE intends to register to. In this case, it is up to the UE implementation on how to use these S-NSSAIs.

To perform network slice-specific authentication and authorization for an S-NSSAI, the AMF invokes an EAP-based network slice-specific authentication and authorization procedure for the S-NSSAI, see subclause 5.4.7 and 3GPP TS 23.502 [9] using the EAP framework as described in 3GPP TS 33.501 [24].

The AMF updates the allowed NSSAI, the rejected NSSAI, and pending NSSAI using the generic UE configuration update procedure as specified in the subclause 5.4.4 after the network slice-specific authentication and authorization procedure is completed.

The AMF shall send the pending NSSAI containing all S-NSSAIs for which the network slice-specific authentication and authorization procedure (except for re-NSSAA) will be performed or is ongoing in the REGISTRATION ACCEPT message. The AMF shall also include in the REGISTRATION ACCEPT message the allowed NSSAI containing one or more S-NSSAIs from the requested NSSAI which are allowed by the AMF and for which network slice-specific authentication and authorization is not required, if any. The network slice-specific authentication and authorization procedure or the network slice-specific authorization revocation procedure can be invoked by the network for a UE supporting NSSAA at any time. After the network performs the network slice-specific re-authentication and re-authorization procedure or network slice-specific authorization revocation procedure:

a) if network slice-specific authentication and authorization fails or network slice-specific authorization is revoked for some but not all S-NSSAIs in the allowed NSSAI, the AMF updates the allowed NSSAI and the rejected NSSAI accordingly using the generic UE configuration update procedure as specified in the subclause 5.4.4 and inform the SMF to release all PDU sessions associated with the S-NSSAI for which network slice-specific re-authentication and re-authorization fails or network slice-specific authorization is revoked;

b) if network slice-specific authentication and authorization fails or network slice-specific authorization is revoked for all S-NSSAIs in the allowed NSSAI but there are one or more default S-NSSAIs which are not subject to network slice-specific authentication and authorization or for which the network slice-specific authentication and authorization has been successfully performed, the AMF updates the allowed NSSAI containing these default S-NSSAIs and the rejected NSSAI accordingly using the generic UE configuration update procedure as specified in the subclause 5.4.4. The AMF shall also inform the SMF to release all PDU sessions associated with the S-NSSAI for which network slice-specific re-authentication and re-authorization fails or network slice-specific authorization is revoked; or

c) if network slice-specific authentication and authorization fails or network slice-specific authorization is revoked for all S-NSSAIs in the allowed NSSAI and all default S-NSSAIs are subject to network slice-specific authentication and authorization, then AMF performs the network-initiated de-registration procedure and includes the rejected NSSAI in the DEREGISTRATION REQUEST message as specified in the subclause 5.5.2.3 except when the UE has an emergency PDU session established or the UE is establishing an emergency PDU session. In this case the AMF shall send the CONFIGURATION UPDATE COMMAND message containing rejected NSSAI and inform the SMF to release all PDU sessions associated with the S-NSSAI for which network slice-specific re-authentication and re-authorization fails or network slice-specific authorization is revoked. After the emergency PDU session is released, the AMF performs the network-initiated de-registration procedure as specified in the subclause 5.5.2.3.

The UE does not include in the requested NSSAI any of the S-NSSAIs from the pending NSSAI that the UE stores, regardless of the access type. When the UE storing a pending NSSAI intends to register to one or more additional S-NSSAIs not included in the pending NSSAI, the UE initiates the registration procedure with a requested NSSAI containing these S-NSSAIs as described in subclause 5.5.1.3.2. In this case, the requested NSSAI shall also include one or more S-NSSAIs from the allowed NSSAI, if the UE still wants to use the S-NSSAI(s) from the allowed NSSAI.

During the registration procedure, when the AMF receives a requested NSSAI from a UE over an access type, for which there is a pending NSSAI including one or more S-NSSAIs that were previously requested over the same access type, the AMF considers S-NSSAIs included in the requested NSSAI and S-NSSAIs in the pending NSSAI that were previously requested over the same access type as requested S-NSSAIs by the UE. The AMF handles the requested S-NSSAIs as described in subclause 5.5.1.3.4.

When performing the network slice-specific re-authentication and re-authorization procedure if the S-NSSAI is included in the allowed NSSAI for both 3GPP and non-3GPP accesses, and the UE is registered to both 3GPP and non-3GPP accesses in the same PLMN, then the AMF selects an access type to perform network slice-specific authentication and authorization based upon operator policy.

If network slice-specific authorization is revoked for an S-NSSAI that is in the current allowed NSSAI for an access type, the AMF shall:

a) provide a new allowed NSSAI, excluding the S-NSSAI for which the network slice-specific authorization is revoked; and

b) provide a new rejected NSSAI for the failed or revoked NSSAA, including the S-NSSAI for which the network slice-specific authorization is revoked, with the rejection cause "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization",

to the UE using the generic UE configuration update procedure as specified in the subclause 5.4.4 and inform the SMF to release all PDU sessions associated with the S-NSSAI for which the network slice-specific authorization is revoked for this access type.

If the UE requests the establishment of a new PDU session or the modification of a PDU session for an S-NSSAI for which the AMF is performing network slice-specific re-authentication and re-authorization procedure, the AMF may determine to not forward the 5GSM message to the SMF as described in subclause 5.4.5.2.4.

NOTE 5: If the AMF receives the HTTP code set to "4xx" or "5xx" as specified in 3GPP TS 29.500 [20AA] or the AMF detects that the NSSAAF failure as specified in 3GPP TS 29.526 [21A] during the NSSAA procedure for an S-NSSAI, then the AMF considers the NSSAA procedure has failed for this S-NSSAI.

\* \* \* Next Change \* \* \* \*

#### 5.4.4.1 General

The purpose of this procedure is to:

a) allow the AMF to update the UE configuration for access and mobility management-related parameters decided and provided by the AMF by providing new parameter information within the command;

b) request the UE to perform a registration procedure for mobility and periodic registration update towards the network to update access and mobility management-related parameters decided and provided by the AMF (see subclause 5.5.1.3);

c) deliver the UAV authorization information to the UE, as described in 3GPP TS 23.256 [6AB]; or

d) update the PEIPS assistance information in the UE (see subclause 5.3.25).

This procedure is initiated by the network and can only be used when the UE has an established 5GMM context, and the UE is in 5GMM-CONNECTED mode. When the UE is in 5GMM-IDLE mode, the AMF may use the paging or notification procedure to initiate the generic UE configuration update procedure. The AMF can request a confirmation response in order to ensure that the parameter has been updated by the UE.

This procedure shall be initiated by the network to assign a new 5G-GUTI to the UE after:

a) a successful service request procedure invoked as a response to a paging request from the network and before the:

1) release of the N1 NAS signalling connection; or

2) suspension of the N1 NAS signalling connection due to user plane CIoT 5GS optimization i.e. before the UE and the AMF enter 5GMM-IDLE mode with suspend indication; or

b) the AMF receives an indication from the lower layers that it has received the NGAP UE context resume request message as specified in 3GPP TS 38.413 [31] for a UE in 5GMM-IDLE mode with suspend indication and this resumption is a response to a paging request from the network, and before the:

1) release of the N1 NAS signalling connection; or

2) suspension of the N1 NAS signalling connection due to user plane CIoT 5GS optimization i.e. before the UE and the AMF enter 5GMM-IDLE mode with suspend indication.

If the service request procedure was triggered due to 5GSM downlink signalling pending, the procedure for assigning a new 5G-GUTI can be initiated by the network after the transport of the 5GSM downlink signalling.

The following parameters are supported by the generic UE configuration update procedure without the need to request the UE to perform the registration procedure for mobility and periodic registration update:

a) 5G-GUTI;

b) TAI list;

c) Service area list;

d) Network identity and time zone information (Full name for network, short name for network, local time zone, universal time and local time zone, network daylight saving time);

e) LADN information;

f) Rejected NSSAI;

g) void;

h) Operator-defined access category definitions;

i) SMS indication;

j) "CAG information list";

k) UE radio capability ID;

l) 5GS registration result;

m) Truncated 5G-S-TMSI configuration;

n) T3447 value;

o) "list of PLMN(s) to be used in disaster condition";

p) disaster roaming wait range;

q) disaster return wait range;

r) PEIPS assistance information;

s) Priority indicator; and

t) pending NSSAI.

The following parameters can be sent to the UE with or without a request to perform the registration procedure for mobility and periodic registration update:

a) Allowed NSSAI;

b) Configured NSSAI;

c) Network slicing subscription change indication; or

d) NSSRG information.

The following parameters are sent to the UE with a request to perform the registration procedure for mobility and periodic registration update:

a) MICO indication;

b) UE radio capability ID deletion indication; and

c) Additional configuration indication.

The following parameters can be included in the Service-level-AA container IE to be sent to the UE without a request to perform the registration procedure for mobility and periodic registration update:

a) Service-level device ID;

b) Service-level-AA payload type;

c) Service-level-AA payload; or

d) Service-level-AA response.

The following parameters are sent over 3GPP access only:

a) LADN information;

b) MICO indication;

c) TAI list;

d) Service area list;

e) "CAG information list";

f) UE radio capability ID;

g) UE radio capability ID deletion indication;

h) Truncated 5G-S-TMSI configuration;

i) Additional configuration indication;

j) T3447 value; and

k) Service-level-AA container.

The following parameters are managed and sent per access type i.e., independently over 3GPP access or non-3GPP access:

a) Allowed NSSAI;

b) Rejected NSSAI (when the NSSAI is rejected for the current registration area) or is rejected for the maximum number of UEs reached); and

c) If the UE is not registered to the same PLMN or SNPN over 3GPP and non-3GPP access:

- 5G-GUTI;

- Network identity and time zone information;

- Rejected NSSAI (when the NSSAI is rejected for the current PLMN or SNPN or rejected for the failed or revoked NSSAA);

- Configured NSSAI;

- NSSRG information;- SMS indication;

- 5GS registration result; and

- PEIPS assistance information.

If the UE is registered to the same PLMN or SNPN over 3GPP and non-3GPP access, the following parameters are managed commonly and sent over 3GPP access or non-3GPP access:

a) 5G-GUTI;

b) Network identity and time zone information;

c) Rejected NSSAI (when the NSSAI is rejected for the current PLMN or SNPN or rejected for the failed or revoked NSSAA);

d) Configured NSSAI;

e) SMS indication; and

f) 5GS registration result;

g) "list of PLMN(s) to be used in disaster condition";

h) disaster roaming wait range;

i) disaster return wait range;

j) PEIPS assistance information;

k) NSSRG information; and

l) pending NSSAI.



Figure 5.4.4.1.1: Generic UE configuration update procedure

\* \* \* Next Change \* \* \* \*

#### 5.4.4.2 Generic UE configuration update procedure initiated by the network

The AMF shall initiate the generic UE configuration update procedure by sending the CONFIGURATION UPDATE COMMAND message to the UE.

The AMF shall in the CONFIGURATION UPDATE COMMAND message either:

a) include one or more of the following parameters: 5G-GUTI, TAI list, allowed NSSAI that may include the mapped S-NSSAI(s), LADN information, service area list, MICO indication, NITZ information, configured NSSAI that may include the mapped S-NSSAI(s), rejected S-NSSAI(s) in the Rejected NSSAI IE or in the Extended rejected NSSAI IE, network slicing subscription change indication, operator-defined access category definitions, SMS indication, service gap time value, "CAG information list", UE radio capability ID, 5GS registration result, UE radio capability ID deletion indication, truncated 5G-S-TMSI configuration, T3447 value, "list of PLMN(s) to be used in disaster condition", disaster roaming wait range, disaster return wait range, PEIPS assistance information or the priority indicator;

b) include the Configuration update indication IE with the Registration requested bit set to "registration requested"; or

c) include a combination of both a) and b).

If the UE is registering or registered for onboarding services in SNPN, the serving SNPN shall not provide the configured NSSAI, the allowed NSSAI or the rejected NSSAI to the UE.

If the UE supports extended rejected NSSAI, the rejected S-NSSAI(s) shall be included in the Extended rejected NSSAI IE. Otherwise the rejected S-NSSAI(s) shall be included in the Rejected NSSAI IE.

If an acknowledgement from the UE is requested, the AMF shall indicate "acknowledgement requested" in the Acknowledgement bit of the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message and shall start timer T3555. Acknowledgement shall be requested for all parameters except when only NITZ is included.

To initiate parameter re-negotiation between the UE and network, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message.

NOTE 1: Generic UE configuration update procedure can be initiated by the AMF for updating the emergency number list, the extended emergency number list or both by indicating "registration requested" in the Registration requested bit of the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message to the UE.

If a new allowed NSSAI information or AMF re-configuration of supported S-NSSAIs requires an AMF relocation, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and include the Allowed NSSAI IE in the CONFIGURATION UPDATE COMMAND message.

If the AMF includes a new allowed NSSAI in the CONFIGURATION UPDATE COMMAND message and the subscription information includes the NSSRG information, then the S-NSSAIs of the allowed NSSAI shall be associated with at least one common NSSRG value.

If the AMF includes a new configured NSSAI in the CONFIGURATION UPDATE COMMAND message and the new configured NSSAI requires an AMF relocation as specified in 3GPP TS 23.501 [8], the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE in the message.

If the AMF includes a new configured NSSAI in the CONFIGURATION UPDATE COMMAND message, the subscription information includes the NSSRG information, and the UE has set the NSSRG bit in the 5GMM capability IE of the REGISTRATION REQUEST message to:

a) "NSSRG supported", then the AMF shall include the NSSRG information in the CONFIGURATION UPDATE COMMAND message; or

b) "NSSRG not supported", then the configured NSSAI shall include one or more S-NSSAIs each of which is associated with all the NSSRG value(s) of the default S-NSSAI(s), or the configured NSSAI shall include, based on the indication received from the UDM as specified in 3GPP TS 23.501 [8], all subscribed S-NSSAIs even if these S-NSSAIs do not share any common NSSRG value.

If the CONFIGURATION UPDATE COMMAND message is initiated only due to changes to the allowed NSSAI and these changes require the UE to initiate a registration procedure, but the AMF is unable to determine an allowed NSSAI for the UE as specified in 3GPP TS 23.501 [8], then the CONFIGURATION UPDATE COMMAND message shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE, and shall not contain any other parameters.

If:

- the AMF needs to enforce a change in the restriction on the use of enhanced coverage or use of CE mode B as described in subclause 5.3.18; or

- the AMF decides to inform a UE in 5GMM-CONNECTED mode and registered for disaster roaming services, that a disaster condition is no longer applicable;

NOTE 1A: The case of the AMF triggering a generic UE configuration update procedure to inform a UE registered for disaster roaming services that a disaster condition is no longer applicable, is only applicable for a UE already in 5GMM-CONNECTED mode.

the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and "release of N1 NAS signalling connection not required" in the Signalling connection maintain request bit of the Additional configuration indication IE in the CONFIGURATION UPDATE COMMAND message.

If a network slice-specific authentication and authorization procedure for an S-NSSAI is completed as a:

a) success and:

1) the subscription information:

i) does not include the NSSRG information; or

ii) includes the NSSRG information and this S-NSSAI shares at least an NSSRG value common to all the S-NSSAI(s) of the allowed NSSAI:

then the AMF shall include this S-NSSAI in the allowed NSSAI over the same access of the requested S-NSSAI; or

2) the subscription information includes the NSSRG information and this S-NSSAI does not share any NSSRG value common to all the S-NSSAI(s) of the allowed NSSAI, then the AMF shall include a pending NSSAI not including this S-NSSAI and including other S-NSSAI(s) which has (have) been included in the pending NSSAI, if any.

NOTE 1B: If there is no other S-NSSAI which has been included in the pending NSSAI, the pending NSSAI does not include any S-NSSAI.

b) failure, the AMF shall include this S-NSSAI in the rejected NSSAI for the failed or revoked NSSAA with the rejection cause "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization" over either 3GPP access or non-3GPP access.

If authorization is revoked for an S-NSSAI that is in the current allowed NSSAI for an access type, the AMF shall:

a) provide a new allowed NSSAI to the UE, excluding the S-NSSAI for which authorization is revoked; and

b) provide a new rejected NSSAI for the failed or revoked NSSAA, including the S-NSSAI in the rejected NSSAI for which the authorization is revoked, with the rejection cause "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization".

The allowed NSSAI and the rejected NSSAI shall be included in the CONFIGURATION UPDATE COMMAND message to reflect the result of the procedures subject to network slice-specific authentication and authorization.

NOTE 2: If there are multiple S-NSSAIs subject to network slice-specific authentication and authorization, it is implementation specific if the AMF informs the UE about the outcome of the procedures in one or more CONFIGURATION UPDATE COMMAND messages.

If the AMF includes the Network slicing indication IE in the CONFIGURATION UPDATE COMMAND message with the Network slicing subscription change indication set to "Network slicing subscription changed", and changes to the allowed NSSAI require the UE to initiate a registration procedure, but the AMF is unable to determine an allowed NSSAI for the UE as specified in 3GPP TS 23.501 [8], then the CONFIGURATION UPDATE COMMAND message shall additionally indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and shall not include an allowed NSSAI.

If EAC mode is activated for an S-NSSAI, the AMF shall perform NSAC for the S-NSSAI subject to NSAC before such S-NSSAI is included in the allowed NSSAI in the CONFIGURATION UPDATE COMMAND message. If EAC mode is deactivated for an S-NSSAI, the AMF shall perform NSAC for the S-NSSAI subject to NSAC after such S-NSSAI is included in the allowed NSSAI in the CONFIGURATION UPDATE COMMAND message.

If the UE supports extended rejected NSSAI and the AMF determines that maximum number of UEs reached for one or more S-NSSAI(s) in the allowed NSSAI as specified in subclause 4.6.2.5, the AMF shall include the rejected NSSAI containing one or more S-NSSAIs with the rejection cause "S-NSSAI not available due to maximum number of UEs reached" in the Extended rejected NSSAI IE in the CONFIGURATION UPDATE COMMAND message. In addition, the AMF may include a back-off timer value for each S-NSSAI with the rejection cause "S-NSSAI not available due to maximum number of UEs reached" included in the Extended rejected NSSAI IE of the CONFIGURATION UPDATE COMMAND message. To avoid that large numbers of UEs simultaneously initiate deferred requests, the network should select the value for the backoff timer for each S-NSSAI for the informed UEs so that timeouts are not synchronised.

If the UE does not indicate support for extended rejected NSSAI and the maximum number of UEs has been reached, the AMF should include the rejected NSSAI containing one or more S-NSSAIs with the rejection cause "S-NSSAI not available in the current registration area" in the Rejected NSSAI IE and should not include these S-NSSAIs in the allowed NSSAI in the CONFIGURATION UPDATE COMMAND message. In addition, the AMF may based on the network policies start a local implementation specific timer for the UE per rejected S-NSSAI and upon expiration of the local implementation specific timer, the AMF may remove the rejected S-NSSAI from the rejected NSSAI and update to the UE by initiating the generic UE configuration update procedure.

NOTE 3: Based on network policies, the AMF can include the S-NSSAI(s) for which the maximum number of UEs has been reached in the rejected NSSAI with rejection causes other than "S-NSSAI not available in the current registration area".

If the UE has set the NSAG bit to "NSAG supported" in the 5GMM capability IE of the REGISTRATION REQUEST message, the AMF may include the NSAG information IE in the CONFIGURATION UPDATE COMMAND message.

If the AMF needs to update the LADN information, the AMF shall include the LADN information in the LADN information IE of the CONFIGURATION UPDATE COMMAND message.

If the AMF needs to update the "CAG information list", the AMF shall include the CAG information list IE or the Extended CAG information list IE in the CONFIGURATION UPDATE COMMAND message.

NOTE 4: If the UE supports extended CAG information list, the CAG information list can be included either in the CAG information list IE or Extended CAG information list IE.

If the UE does not support extended CAG information list, the CAG information list shall not be included in the Extended CAG information list IE.

If the AMF needs to update the "CAG information list", the UE has an emergency PDU session, and the AMF can determine that the UE is in

a) a CAG cell and none of the CAG-ID(s) supported by the CAG cell is included in the "allowed CAG list" for the current PLMN in the updated "CAG information list"; or

b) a non-CAG cell and the entry for the current PLMN in the updated "CAG information list" includes an "indication that the UE is only allowed to access 5GS via CAG cells";

the AMF may indicate to the SMF to perform a local release of:

a) all non-emergency single access PDU sessions associated with 3GPP access;

b) all MA PDU sessions without a PDN connection established as a user-plane resource and without user plane resources established on non-3GPP access; and

c) the 3GPP access user plane resources of all those MA PDU sessions with user plane resources established on both accesses.

The AMF shall not indicate to the SMF to release the emergency PDU session. If the AMF indicated to the SMF to perform a local release of:

a) all single access non-emergency PDU sessions associated with 3GPP access;

b) all MA PDU sessions without a PDN connection established as a user-plane resource and without user plane resources established on non-3GPP access; and

c) the 3GPP access user plane resources of all those MA PDU sessions with user plane resources established on both accesses;

the network shall behave as if the UE is registered for emergency services over 3GPP access and shall set the 5GS registration result IE value to "Registered for emergency services" in the CONFIGURATION UPDATE COMMAND message.

If the AMF is initiating the generic UE configuration update procedure to indicate to a UE which is registered for disaster roaming services, and which has an ongoing emergency PDU session, that the UE is registered for emergency services as described in subclause 4.24, the AMF shall set the 5GS registration result IE value to "Registered for emergency services" in the CONFIGURATION UPDATE COMMAND message.

If the AMF:

- updated the "CAG information list" to remove one or more CAG-ID(s) in the Allowed CAG list for the serving PLMN or an equivalent PLMN; or

- updated the "CAG information list" to set the "indication that the UE is only allowed to access 5GS via CAG cells" for the serving PLMN or an equivalent PLMN which was not set before,

then upon completion of the configuration update procedure and if the UE does not have an emergency PDU session, the AMF shall initiate the release of the N1 NAS signalling connection according to subclause 5.3.1.3.

If the AMF needs to update the truncated 5G-S-TMSI configuration for a UE in NB-N1 mode using control plane CIoT 5GS optimization, the AMF shall include the Truncated 5G-S-TMSI configuration IE in the CONFIGURATION UPDATE COMMAND message.

If the AMF includes a UE radio capability ID deletion indication IE in the CONFIGURATION UPDATE COMMAND message, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE.

If the AMF needs to redirect the UE to EPC as described in subclause 4.8.4A.2, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and "release of N1 NAS signalling connection not required" in the Signalling connection maintain request bit of the Additional configuration indication IE in the CONFIGURATION UPDATE COMMAND message.

If the UE is not in NB-N1 mode and the UE supports RACS, the AMF may include either a UE radio capability ID IE or a UE radio capability ID deletion indication IE in the CONFIGURATION UPDATE COMMAND message.

During an established 5GMM context, the network may send none, one, or more CONFIGURATION UPDATE COMMAND messages to the UE. If more than one CONFIGURATION UPDATE COMMAND message is sent, the messages need not have the same content.

Upon receipt of the result of the UUAA-MM procedure from the UAS-NF, the AMF shall include:

a) the service-level-AA response with the SLAR field set to:

1) "Service level authentication and authorization was successful" if the AMF detects the UUAA-MM procedure has succeeded; or

2) "Service level authentication and authorization was not successful or service level authorization is revoked" if the AMF detects the UUAA-MM procedure has failed;

b) if the CAA-Level UAV ID is provided by the UAS-NF, the service-level device ID with the value set to the CAA-Level UAV ID; and;

c) if the UUAA authorization payload is received from the UAS-NF:

1) the service-level-AA payload type, with the values set to "UUAA payload"; and

2) the service-level-AA payload, with the value set to the UUAA payload;

in the Service-level-AA container IE of the CONFIGURATION UPDATE COMMAND message.

NOTE 5: UAS security information can be included in the UUAA payload by the USS as specified in 3GPP TS 33.256 [24B].

NOTE 6: If the AMF receives the HTTP code set to "4xx" or "5xx" as specified in 3GPP TS 29.500 [20AA] or the AMF detects that the UUAA-MM failure as specified in 3GPP TS 29.256 [21B], then the AMF considers the UUAA-MM procedure has failed.

If the AMF needs to deliver to the UE the UUAA revocation notification received from the UAS-NF, the AMF shall include the service-level-AA response with SLAR set to "Service level authentication and authorization was not successful or service level authorization is revoked" in the Service-level-AA container IE of the CONFIGURATION UPDATE COMMAND message.

If the UE supports MINT, the AMF may include the List of PLMNs to be used in disaster condition IE in the CONFIGURATION UPDATE COMMAND message.

If the UE supports MINT, the AMF may include the Disaster roaming wait range IE in the CONFIGURATION UPDATE COMMAND message.

If the UE supports MINT, the AMF may include the Disaster return wait range IE in the CONFIGURATION UPDATE COMMAND message.

NOTE 7: The AMF can determine the content of the "list of PLMN(s) to be used in disaster condition", the value of the disaster roaming wait range and the value of the disaster return wait range based on the network local configuration.

If the UE supports and the network supports and accepts the use of the PEIPS assistance information, and the AMF needs to update the PEIPS assistance information, the AMF may include the PEIPS assistance information in the Updated PEIPS assistance information IE of the CONFIGURATION UPDATE COMMAND message.

If the AMF needs to inform the UE that the use of access identity 1 is valid or is no longer valid, the AMF informs the UE by setting the MPS indicator bit of the Priority indicator IE to "Access identity 1 valid" or "Access identity 1 not valid" respectively, in the CONFIGURATION UPDATE COMMAND message. Based on operator policy, the AMF sets the MPS indicator bit in the CONFIGURATION UPDATE COMMAND message based on the MPS priority information in the user's subscription context obtained from the UDM.

\* \* \* Next Change \* \* \* \*

#### 5.4.4.3 Generic UE configuration update accepted by the UE

Upon receiving the CONFIGURATION UPDATE COMMAND message, the UE shall stop timer T3346 if running and use the contents to update appropriate information stored within the UE.

If "acknowledgement requested" is indicated in the Acknowledgement bit of the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message, the UE shall send a CONFIGURATION UPDATE COMPLETE message.

If the UE receives a new 5G-GUTI in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new 5G-GUTI as valid, the old 5G-GUTI as invalid, stop timer T3519 if running, and delete any stored SUCI; otherwise, the UE shall consider the old 5G-GUTI as valid. The UE shall provide the 5G-GUTI to the lower layer of 3GPP access if the CONFIGURATION UPDATE COMMAND message is sent over the non-3GPP access, and the UE is in 5GMM-REGISTERED in both 3GPP access and non-3GPP access in the same PLMN.

If the UE receives a new TAI list in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new TAI list as valid and the old TAI list as invalid; otherwise, the UE shall consider the old TAI list as valid. If the registration area contains TAIs belonging to different PLMNs, which are equivalent PLMNs, and

a) the UE already has stored allowed NSSAI for the current registration area, the UE shall store the allowed NSSAI for the current registration area in each of the allowed NSSAIs which are associated with each of the PLMNs in the registration area; and

b) the UE already has stored rejected NSSAI for the current registration area, the UE shall store the rejected NSSAI for the current registration area in each of the rejected NSSAIs which are associated with each of the PLMNs in the registration area.

If the UE receives a new truncated 5G-S-TMSI configuration in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new truncated 5G-S-TMSI configuration as valid and the old truncated 5G-S-TMSI configuration as invalid; otherwise, the UE shall consider the old truncated 5G-S-TMSI configuration as valid.

If the UE receives a new service area list in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new service area list as valid and the old service area list as invalid; otherwise, the UE shall consider the old service area list, if any, as valid.

If the UE receives new NITZ information in the CONFIGURATION UPDATE COMMAND message, the UE considers the new NITZ information as valid and the old NITZ information as invalid; otherwise, the UE shall consider the old NITZ information as valid.

If the UE receives a LADN information IE in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the old LADN information as invalid and the new LADN information as valid, if any; otherwise, the UE shall consider the old LADN information as valid.

If the UE receives a new allowed NSSAI for the associated access type in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new allowed NSSAI as valid for the associated access type, store the allowed NSSAI for the associated access type as specified in subclause 4.6.2.2 and consider the old allowed NSSAI for the associated access type as invalid; otherwise, the UE shall consider the old allowed NSSAI as valid for the associated access type.

If the UE receives a new configured NSSAI in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new configured NSSAI for the registered PLMN or SNPN as valid and the old configured NSSAI for the registered PLMN or SNPN as invalid; otherwise, the UE shall consider the old configured NSSAI for the registered PLMN or SNPN as valid The UE shall store the new configured NSSAI as specified in subclause 4.6.2.2. In addition, if the CONFIGURATION UPDATE COMMAND message contains an NSSRG information IE, the UE shall store the contents of the NSSRG information IE as specified in subclause 4.6.2.2.

If the UE receives the Network slicing indication IE in the CONFIGURATION UPDATE COMMAND message with the Network slicing subscription change indication set to "Network slicing subscription changed", the UE shall delete the network slicing information for each and every PLMN except for the current PLMN as specified in subclause 4.6.2.2.

If the UE receives Operator-defined access category definitions IE in the CONFIGURATION UPDATE COMMAND message and the Operator-defined access category definitions IE contains one or more operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN and shall store the received operator-defined access category definitions for the RPLMN. If the UE receives the Operator-defined access category definitions IE in the CONFIGURATION UPDATE COMMAND message and the Operator-defined access category definitions IE contains no operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN. If the CONFIGURATION UPDATE COMMAND message does not contain the Operator-defined access category definitions IE, the UE shall not delete the operator-defined access category definitions stored for the RPLMN.

If the UE receives the SMS indication IE in the CONFIGURATION UPDATE COMMAND message with the SMS availability indication set to:

a) "SMS over NAS not available", the UE shall consider that SMS over NAS transport is not allowed by the network; and

b) "SMS over NAS available", the UE may request the use of SMS over NAS transport by performing a registration procedure for mobility and periodic registration update as specified in subclause 5.5.1.3, after the completion of the generic UE configuration update procedure.

If the UE receives the CAG information list IE in the CONFIGURATION UPDATE COMMAND message, the UE shall:

a) replace the "CAG information list" stored in the UE with the received CAG information list IE when received in the HPLMN or EHPLMN;

NOTE 1: When the UE receives the CAG information list IE in the HPLMN derived from the IMSI, the EHPLMN list is present and is not empty and the HPLMN is not present in the EHPLMN list, the UE behaves as if it receives the CAG information list IE in a VPLMN.

b) replace the serving VPLMN's entry of the "CAG information list" stored in the UE with the serving VPLMN's entry of the received CAG information list IE when the UE receives the CAG information list IE in a serving PLMN other than the HPLMN or EHPLMN; or

NOTE 2: When the UE receives the CAG information list IE in a serving PLMN other than the HPLMN or EHPLMN, entries of a PLMN other than the serving VPLMN, if any, in the received CAG information list IE are ignored.

c) remove the serving VPLMN's entry of the "CAG information list" stored in the UE when the UE receives the CAG information list IE in a serving PLMN other than the HPLMN or EHPLMN and the CAG information list IE does not contain the serving VPLMN's entry.

The UE shall store the "CAG information list" received in the CAG information list IE as specified in annex C.

If the received "CAG information list" includes an entry containing the identity of the current PLMN and the UE had set the CAG bit to "CAG supported" in the 5GMM capability IE of the REGISTRATION REQUEST message, the UE shall operate as follows.

a) If the UE receives the CONFIGURATION UPDATE COMMAND message via a CAG cell, the entry for the current PLMN in the received "CAG information list" does not include any of the CAG-ID(s) supported by the current CAG cell, and:

1) the entry for the current PLMN in the received "CAG information list" does not include an "indication that the UE is only allowed to access 5GS via CAG cells", then the UE shall enter the state 5GMM-REGISTERED.LIMITED-SERVICE and shall search for a suitable cell according to 3GPP TS 38.304 [28] or 3GPP TS 36.304 [25C] with the updated "CAG information list"; or

2) the entry for the current PLMN in the received "CAG information list" includes an "indication that the UE is only allowed to access 5GS via CAG cells" and:

i) if the entry for the current PLMN in the received "CAG information list" includes one or more CAG-IDs, the UE shall enter the state 5GMM-REGISTERED.LIMITED-SERVICE and shall search for a suitable cell according to 3GPP TS 38.304 [28] with the updated "CAG information list"; or

ii) if the entry for the current PLMN in the received "CAG information list" does not include any CAG-ID and:

A) the UE does not have an emergency PDU session, then the UE shall enter the state 5GMM-REGISTERED.PLMN-SEARCH and shall apply the PLMN selection process defined in 3GPP TS 23.122 [5] with the updated "CAG information list"; or

B) the UE has an emergency PDU session, then the UE shall perform a local release of all PDU sessions associated with 3GPP access except for the emergency PDU session and enter the state 5GMM-REGISTERED.LIMITED-SERVICE; or

b) If the UE receives the CONFIGURATION UPDATE COMMAND message via a non-CAG cell and the entry for the current PLMN in the received "CAG information list" includes an "indication that the UE is only allowed to access 5GS via CAG cells" and:

1) if the "allowed CAG list" for the current PLMN in the received "CAG information list" includes one or more CAG-IDs, the UE shall enter the state 5GMM-REGISTERED.LIMITED-SERVICE and shall search for a suitable cell according to 3GPP TS 38.304 [28] with the updated "CAG information list"; or

2) if the entry for the current PLMN in the received "CAG information list" does not include any CAG-ID and:

i) the UE does not have an emergency PDU session, then the UE shall enter the state 5GMM-REGISTERED.PLMN-SEARCH and shall apply the PLMN selection process defined in 3GPP TS 23.122 [5] with the updated "CAG information list"; or

ii) the UE has an emergency PDU session, then the UE shall perform a local release of all PDU sessions associated with 3GPP access except for the emergency PDU session and enter the state 5GMM-REGISTERED.LIMITED-SERVICE.

If the received "CAG information list" does not include an entry containing the identity of the current PLMN and the UE receives the CONFIGURATION UPDATE COMMAND message via a CAG cell, the UE shall enter the state 5GMM-REGISTERED.LIMITED-SERVICE and shall search for a suitable cell according to 3GPP TS 38.304 [28] or 3GPP TS 36.304 [25C] with the updated "CAG information list".

If the CONFIGURATION UPDATE COMMAND message indicates "registration requested" in the Registration requested bit of the Configuration update indication IE and:

a) contains no other parameters or contains at least one of the following parameters: a new allowed NSSAI, a new configured NSSAI or the Network slicing subscription change indication, and:

1) an emergency PDU session exists, the UE shall, after the completion of the generic UE configuration update procedure and the release of the emergency PDU session, release the existing N1 NAS signalling connection. If any Tsor-cm timer(s) were running and have stopped, the UE shall attempt to obtain service on a higher priority PLMN (see 3GPP TS 23.122 [5]). Otherwise the UE start a registration procedure for mobility and periodic registration update as specified in subclause 5.5.1.3; or

2) no emergency PDU Session exists, the UE shall, after the completion of the generic UE configuration update procedure and the release of the existing N1 NAS signalling connection. If any Tsor-cm timer(s) were running and have stopped, the UE shall attempt to obtain service on a higher priority PLMN (see 3GPP TS 23.122 [5]). Otherwise the UE start a registration procedure for mobility and periodic registration update as specified in subclause 5.5.1.3;

b) a MICO indication is included without a new allowed NSSAI; a new configured NSSAI or the Network slicing subscription change indication, the UE shall, after the completion of the generic UE configuration update procedure, start a registration procedure for mobility and registration update as specified in subclause 5.5.1.3 to re-negotiate MICO mode with the network;

c) an Additional configuration indication IE is included, and:

1) "release of N1 NAS signalling connection not required" is indicated in the Signalling connection maintain request bit of the Additional configuration indication IE; and

2) a new allowed NSSAI, a new configured NSSAI and the Network slicing subscription change indication is not included in the CONFIGURATION UPDATE COMMAND message,

the UE shall, after the completion of the generic UE configuration update procedure, start a registration procedure for mobility and registration update as specified in subclause 5.5.1.3; or

d) a UE radio capability ID deletion indication IE set to "Network-assigned UE radio capability IDs deletion requested" is included, and:

1) the UE is not in NB-N1 mode;

2) a new allowed NSSAI, a new configured NSSAI or a Network slicing subscription change indication is not included; and

3) the UE has set the RACS bit to "RACS supported" in the 5GMM capability IE of the REGISTRATION REQUEST message,

the UE shall, after the completion of the generic UE configuration update procedure, start a registration procedure for mobility and registration update as specified in subclause 5.5.1.3.

The UE receiving the rejected NSSAI in the CONFIGURATION UPDATE COMMAND message takes the following actions based on the rejection cause in the rejected S-NSSAI(s):

"S-NSSAI not available in the current PLMN or SNPN"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current PLMN or SNPN as specified in subclause 4.6.2.2 and shall not attempt to use this S-NSSAI(s) in the current PLMN or SNPN until switching off the UE, the UICC containing the USIM is removed, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN is updated, or the rejected S-NSSAI(s) are removed or deleted as described in subclause 4.6.2.2.

"S-NSSAI not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current registration area as specified in subclause 4.6.2.2 and shall not attempt to use this S-NSSAI(s) in the current registration area until switching off the UE, the UE moving out of the current registration area, the UICC containing the USIM is removed, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN is updated, or the rejected S-NSSAI(s) are removed or deleted as described in subclause 4.6.2.2.

"S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the failed or revoked NSSAA as specified in subclause 4.6.2.2 and shall not attempt to use this S-NSSAI in the current PLMN or SNPN over any access until switching off the UE, the UICC containing the USIM is removed, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN is updated, or the rejected S-NSSAI(s) are removed or deleted as described in subclause 4.6.1 and 4.6.2.2.

"S-NSSAI not available due to maximum number of UEs reached"

Unless the back-off timer value received along with the S-NSSAI is zero, the UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the maximum number of UEs reached as specified in subclause 4.6.2.2 and shall not attempt to use this S-NSSAI in the current PLMN or SNPN over the current access until switching off the UE, the UICC containing the USIM is removed, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN is updated, or the rejected S-NSSAI(s) are removed as described in subclause 4.6.2.2.

NOTE 3: If the back-off timer value received along with the S-NSSAI in the rejected NSSAI for the maximum number of UEs reached is zero as specified in subclause 10.5.7.4a of TS 24.008, the UE does not consider the S-NSSAI as the rejected S-NSSAI.

If there is one or more S-NSSAIs in the rejected NSSAI with the rejection cause "S-NSSAI not available due to maximum number of UEs reached", then for each S-NSSAI, the UE shall behave as follows:

a) stop the timer T3526 associated with the S-NSSAI, if running;

b) start the timer T3526 with:

1) the back-off timer value received along with the S-NSSAI, if back-off timer value is received along with the S-NSSAI that is neither zero nor deactivated; or

2) an implementation specific back-off timer value, if no back-off timer value is received along with the S-NSSAI; and

c) remove the S-NSSAI from the rejected NSSAI for the maximum number of UEs reached when the timer T3526 associated with the S-NSSAI expires.

If the UE receives the NSAG information IE in the CONFIGURATION UPDATE COMMAND message, the UE shall store the NSAG information as specified in subclause 4.6.2.2.

If the UE receives a T3447 value IE in the CONFIGURATION UPDATE COMMAND message and has indicated "service gap control supported" in the REGISTRATION REQUEST, then the UE shall replace the stored T3447 value with the received value in the T3447 value IE, and if neither zero nor deactivated use the received T3447 value with the timer T3447 next time it is started. If the received T3447 value is zero or deactivated, then the UE shall stop the timer T3447 if running.

If the UE is not in NB-N1 mode, the UE has set the RACS bit to "RACS supported" in the 5GMM capability IE of the REGISTRATION REQUEST message and the CONFIGURATION UPDATE COMMAND message includes:

a) a UE radio capability ID deletion indication IE set to "Network-assigned UE radio capability IDs deletion requested", the UE shall delete any network-assigned UE radio capability IDs associated with the RPLMN or RSNPN and, if the UE supports access to an SNPN using credentials from a credentials holder, the selected entry of the "list of subscriber data" or the selected PLMN subscription stored at the UE; or

b) a UE radio capability ID IE, the UE shall store the UE radio capability ID as specified in annex C.

If the UE is not currently registered for emergency services and the 5GS registration result IE value in the CONFIGURATION UPDATE COMMAND message is set to "Registered for emergency services", the UE shall consider itself registered for emergency services and shall locally release all non-emergency PDU sessions, if any.

If the UE receives the service-level-AA container IE of the CONFIGURATION UPDATE COMMAND message, the UE passes it to the upper layer.

If the CONFIGURATION UPDATE COMMAND message includes the service-level-AA response in the Service-level-AA container IE with the SLAR field set to "Service level authentication and authorization was not successful or service level authorization is revoked", the UE shall forward the service-level-AA response to the upper layers, so the UUAA authorization data is deleted as specified in 3GPP TS 33.256 [24B].

If the UE receives the List of PLMNs to be used in disaster condition IE in the CONFIGURATION UPDATE COMMAND message and the UE supports MINT, the UE shall delete the "list of PLMN(s) to be used in disaster condition" stored in the ME together with the PLMN ID of the RPLMN, if any, and may store the "list of PLMN(s) to be used in disaster condition" included in the List of PLMNs to be used in disaster condition IE in the ME together with the PLMN ID of the RPLMN.

If the UE receives the Disaster roaming wait range IE in the CONFIGURATION UPDATE COMMAND message and the UE supports MINT, the UE shall delete the disaster roaming wait range stored in the ME, if any, and store the disaster roaming wait range included in the Disaster roaming wait range IE in the ME.

If the UE receives the Disaster return wait range IE in the CONFIGURATION UPDATE COMMAND message and the UE supports MINT, the UE shall delete the disaster roaming wait range stored in the ME, if any, and store the disaster roaming wait range included in the Disaster roaming wait range IE in the ME.

If the UE receives the Updated PEIPS assistance information IE in the CONFIGURATION UPDATE COMMAND message and the UE supports NR paging subgrouping, the UE shall use the PEIPS assistance information included in the Updated PEIPS assistance information IE.

If the UE receives a CONFIGURATION UPDATE COMMAND message with the MPS indicator bit set to "Access identity 1 valid", the UE shall act as a UE with access identity 1 configured for MPS as described in subclause 4.5.2, in all NG-RAN of the registered PLMN and its equivalent PLMNs or in the case of SNPN, as described in subclause 4.5.2A, in all NG-RAN of the registered SNPN. The MPS indicator bit in the Priority indicator IE provided in the CONFIGURATION UPDATE COMMAND message is valid until the UE receives a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid" or the UE receives a CONFIGURATION UPDATE COMMAND message with the MPS indicator bit of the Priority indicator IE set to "Access identity 1 not valid" or until the UE selects a non-equivalent PLMN (or in the case of SNPN, selects another SNPN). Access identity 1 is only applicable while the UE is in N1 mode.

If the UE receives a CONFIGURATION UPDATE COMMAND message with a new pending NSSAI, the UE shall replace the old pending NSSAI with the new pending NSSAI as specified in subclause 4.6.2.2.

\* \* \* Next Change \* \* \* \*

#### 8.2.19.1 Message definition

The CONFIGURATION UPDATE COMMAND message is sent by the AMF to the UE. See table 8.2.19.1.1.

Message type: CONFIGURATION UPDATE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.19.1.1: CONFIGURATION UPDATE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Configuration update command message identity | Message type  9.7 | M | V | 1 |
| D- | Configuration update indication | Configuration update indication  9.11.3.18 | O | TV | 1 |
| 77 | 5G-GUTI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 14 |
| 54 | TAI list | 5GS tracking area identity list  9.11.3.9 | O | TLV | 9-114 |
| 15 | Allowed NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 27 | Service area list | Service area list  9.11.3.49 | O | TLV | 6-114 |
| 43 | Full name for network | Network name  9.11.3.35 | O | TLV | 3-n |
| 45 | Short name for network | Network name  9.11.3.35 | O | TLV | 3-n |
| 46 | Local time zone | Time zone  9.11.3.52 | O | TV | 2 |
| 47 | Universal time and local time zone | Time zone and time  9.11.3.53 | O | TV | 8 |
| 49 | Network daylight saving time | Daylight saving time  9.11.3.19 | O | TLV | 3 |
| 79 | LADN information | LADN information  9.11.3.30 | O | TLV-E | 3-1715 |
| B- | MICO indication | MICO indication  9.11.3.31 | O | TV | 1 |
| 9- | Network slicing indication | Network slicing indication  9.11.3.36 | O | TV | 1 |
| 31 | Configured NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-146 |
| 11 | Rejected NSSAI | Rejected NSSAI  9.11.3.46 | O | TLV | 4-42 |
| 76 | Operator-defined access category definitions | Operator-defined access category definitions  9.11.3.38 | O | TLV-E | 3-8323 |
| F- | SMS indication | SMS indication  9.11.3.50A | O | TV | 1 |
| 6C | T3447 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 75 | CAG information list | CAG information list  9.11.3.18A | O | TLV-E | 3-n |
| 67 | UE radio capability ID | UE radio capability ID  9.11.3.68 | O | TLV | 3-n |
| A- | UE radio capability ID deletion indication | UE radio capability ID deletion indication  9.11.3.69 | O | TV | 1 |
| 44 | 5GS registration result | 5GS registration result  9.11.3.6 | O | TLV | 3 |
| 1B | Truncated 5G-S-TMSI configuration | Truncated 5G-S-TMSI configuration  9.11.3.70 | O | TLV | 3 |
| C- | Additional configuration indication | Additional configuration indication  9.11.3.74 | O | TV | 1 |
| 68 | Extended rejected NSSAI | Extended rejected NSSAI  9.11.3.75 | O | TLV | 5-90 |
| 72 | Service-level-AA container | Service-level-AA container  9.11.2.10 | O | TLV-E | 6-n |
| 70 | NSSRG information | NSSRG information  9.11.3.82 | O | TLV-E | 7-65538 |
| 14 | Disaster roaming wait range | Registration wait range  9.11.3.84 | O | TLV | 4 |
| 2C | Disaster return wait range | Registration wait range  9.11.3.84 | O | TLV | 4 |
| 13 | List of PLMNs to be used in disaster condition | List of PLMNs to be used in disaster condition  9.11.3.83 | O | TLV | 2-n |
| 71 | Extended CAG information list | Extended CAG information list  9.11.3.86 | O | TLV-E | 3-n |
| 1F | Updated PEIPS assistance information | PEIPS assistance information  9.11.3.80 | O | TLV | 3-n |
| 73 | NSAG information | NSAG information  9.11.3.87 | O | TLV-E | 10-n |
| E- | Priority indicator | Priority indicator  9.11.3.91 | O | TV | 1 |
| TBD | Pending NSSAI | NSSAI  9.11.3.37 | O | TLV | 2-146 |

\* \* \* Next Change \* \* \* \*

#### 8.2.19.x Pending NSSAI

This IE may be included to provide a new pending NSSAI to the UE.

\* \* \* Next Change \* \* \* \*

#### 9.11.3.37 NSSAI

The purpose of the NSSAI information element is to identify a collection of S-NSSAIs

The NSSAI information element is coded as shown in figure 9.11.3.37.1 and table 9.11.3.37.1.

The NSSAI is a type 4 information element with a minimum length of 2 octets and a maximum length of 146 octets.

NOTE: More than one S-NSSAIs in an NSSAI can have the same SST values, and optionally same SD values, which are associated with different mapped HPLMN SST values and optionally mapped HPLMN SD values.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NSSAI IEI | | | | | | | | octet 1 |
| Length of NSSAI contents | | | | | | | | octet 2 |
| S-NSSAI value 1 | | | | | | | | octet 3\*  octet m\* |
| S-NSSAI value 2 | | | | | | | | octet m+1\*  octet n\* |
| … | | | | | | | | octet n+1\*  octet u\* |
| S-NSSAI value n | | | | | | | | octet u+1\*  octet v\* |

Figure 9.11.3.37.1: NSSAI information element

Table 9.11.3.37.1: NSSAI information element

|  |
| --- |
| Value part of the NSSAI information element (octet 3 to v)  The value part of the NSSAI information element consists of one or more S-NSSAI values. Each S-NSSAI value consists of one S-NSSAI and optionally one mapped S-NSSAI.  The recipient of this information element shall store the complete list received (NOTE 1, NOTE 2, NOTE 3). If the NSSAI information element conveys an allowed NSSAI and more than 8 S-NSSAI values are included in this information element, the UE shall store the first 8 S-NSSAI values and ignore the remaining octets of the information element.  If the NSSAI information element conveys a configured NSSAI or pending NSSAI and more than 16 S-NSSAI values are included in this information element, the UE shall store the first 16 S-NSSAI values and ignore the remaining octets of the information element.  S-NSSAI value:  S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. |
| NOTE 1: The total number of S-NSSAI values in a requested NSSAI shall not exceed eight.  NOTE 2: The number of S-NSSAI values in an allowed NSSAI shall not exceed eight.  NOTE 3: The number of S-NSSAI values in a configured NSSAI or pending NSSAI shall not exceed sixteen.  NOTE 4: The total number of S-NSSAI values may be zero only if an NSSAI is conveyed via the Pending NSSAI IE in the CONFIGURATION UPDATE COMMAND message. |

\* \* \* End of Changes \* \* \* \*