**SA WG2 Meeting #143E e-meeting *S2-2100389***

**Elbonia, February 24 – March 09, 2021**

|  |
| --- |
| *CR-Form-v11.2* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **2567** | **rev** | **-** | **Current version:** | **16.7.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Network Slice restriction based on NWDAF analytics |
|  |  |
| ***Source to WG:*** | Samsung, Spirent, KDDI |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | eNA\_Ph2 |  | ***Date:*** | 2021-02-18 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | TR 23.700-91 concluded for KI#4 that a Network Slice restriction leveraging NWDAF analytics could be used to avoid accepting UE registrations and/or PDU Session establishments in the restricted Network Slice(s) and/or Network Slice instance(s), as shown in clause 8.4:“For KI#4, it is proposed that the following aspects from Solution #2 are considered for the normative work for slice load distribution mechanism based on determination by NWDAF of slice service experience and slice load analytics:“(…); leveraging the analytics information, NSSF and AMF can take actions as instructed in the Network Slice Restrictions or Network Slice instance Restrictions for example not to accept any more UE registrations, or not to accept PDU sessions establishment, until this restriction is lifted.”In addition, the following was agreed as part of the conclusion for KI#9 (i.e. cl. 8.9 in TR 23.700-91):‘The following procedures are considered for the normative work:(…)- Assistance to slice load distribution" procedure that also uses Data Dispersion Analytics as defined in solution#30.’This change addresses the above portions of the conclusions for KIs #4, #9 by introducing the slice restriction concept based on NWDAF analytics to the UE registration to a slice and PDU session establishment operations. |
|  |  |
| ***Summary of change:*** | * Indicated support for Network Slice and Network Slice instance restriction in AMF and NSSF
* Modification of Network Slice registration detailed operation by introducing i) NWDAF analytics subscriptions, and ii) Network Slice (+instance) restriction options, all involving AMF and optionally NSSF.
* Modification of PDU Session establishment description to account for Network Slice instance restriction
 |
|  |  |
| ***Consequences if not approved:*** | Study conclusions for FS\_eNA\_Ph2 would not be respected, and new agreed functionality would be missing from specification. |
|  |  |
| ***Clauses affected:*** | 6.2.1, 6.2.14, 5.15.5.2.1, 5.15.5.2.2, 5.15.5.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 23.502 CR2586 |
| ***affected:*** |  | **X** |  Test specifications | TS 23.288 CR0202 |
| ***(show related CRs)*** |  | **X** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |   |

\* \* \* \* Start of Changes \* \* \* \*

### 6.2.1 AMF

The Access and Mobility Management function (AMF) includes the following functionality. Some or all of the AMF functionalities may be supported in a single instance of an AMF:

- Termination of RAN CP interface (N2).

- Termination of NAS (N1), NAS ciphering and integrity protection.

- Registration management.

- Connection management.

- Reachability management.

- Mobility Management.

- Lawful intercept (for AMF events and interface to LI System).

- Provide transport for SM messages between UE and SMF.

- Transparent proxy for routing SM messages.

- Access Authentication.

- Access Authorization.

- Provide transport for SMS messages between UE and SMSF.

- Security Anchor Functionality (SEAF) as specified in TS 33.501 [29].

- Location Services management for regulatory services.

- Provide transport for Location Services messages between UE and LMF as well as between RAN and LMF.

- EPS Bearer ID allocation for interworking with EPS.

- UE mobility event notification.

- Support for Control Plane CIoT 5GS Optimisation.

- Support for User Plane CIoT 5GS Optimisation.

- Support for restriction of use of Enhanced Coverage.

- Provisioning of external parameters (Expected UE Behaviour parameters or Network Configuration parameters).

- Support for Network Slice-Specific Authentication and Authorization.

NOTE 1: Regardless of the number of Network functions, there is only one NAS interface instance per access network between the UE and the CN, terminated at one of the Network functions that implements at least NAS security and Mobility Management.

In addition to the functionalities of the AMF described above, the AMF may include the following functionality to support non-3GPP access networks:

- Support of N2 interface with N3IWF/TNGF. Over this interface, some information (e.g. 3GPP Cell Identification) and procedures (e.g. Handover related) defined over 3GPP access may not apply, and non-3GPP access specific information may be applied that do not apply to 3GPP accesses.

- Support of NAS signalling with a UE over N3IWF/TNGF. Some procedures supported by NAS signalling over 3GPP access may be not applicable to untrusted non-3GPP (e.g. Paging) access.

- Support of authentication of UEs connected over N3IWF/TNGF.

- Management of mobility, authentication, and separate security context state(s) of a UE connected via a non-3GPP access or connected via a 3GPP access and a non-3GPP access simultaneously.

- Support as described in clause 5.3.2.3 a co-ordinated RM management context valid over a 3GPP access and a Non 3GPP access.

- Support as described in clause 5.3.3.4 dedicated CM management contexts for the UE for connectivity over non-3GPP access.

NOTE 2: Not all of the functionalities are required to be supported in an instance of a Network Slice.

In addition to the functionalities of the AMF described above, the AMF may include policy related functionalities as described in clause 6.2.8 in TS 23.503 [45].

The AMF uses the N14 interface for AMF re-allocation and AMF to AMF information transfer. This interface may be be either intra-PLMN or inter-PLMN (e.g. in the case of inter-PLMN mobility).

In addition to the functionality of the AMF described above, the AMF may include the following functionality to support monitoring in roaming scenarios:

- Normalization of reports according to roaming agreements between VPLMN and HPLMN (e.g. change the location granularity in a report from cell level to a level that is appropriate for the HPLMN); and

- Generation of charging/accounting information for Monitoring Event Reports that are sent to the HPLMN.

In addition to the functionality of the AMF described above, the AMF may provide support for Network Slice restriction and Network Slice instance restriction based on NWDAF analytics.

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

### 6.2.14 NSSF

The Network Slice Selection Function (NSSF) supports the following functionality:

- Selecting the set of Network Slice instances serving the UE;

- Determining the Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs;

- Determining the Configured NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs;

- Determining the AMF Set to be used to serve the UE, or, based on configuration, a list of candidate AMF(s), possibly by querying the NRF;

The NSSF may provide support for Network Slice restriction and Network Slice instance restriction based on NWDAF analytics.

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

##### 5.15.5.2.1 Registration to a set of Network Slices

When a UE registers over an Access Type with a PLMN, if the UE has either or both of:

- a Configured NSSAI for this PLMN;

- an Allowed NSSAI for this PLMN and Access Type;

the UE shall provide to the network, in AS layer under the conditions described in clause 5.15.9 and in NAS layer, a Requested NSSAI containing the S-NSSAI(s) corresponding to the Network Slice(s) to which the UE wishes to register, unless they are stored in the UE in the Pending NSSAI.

The Requested NSSAI shall be one of:

- the Default Configured NSSAI, i.e. if the UE has no Configured NSSAI nor an Allowed NSSAI for the serving PLMN;

- the Configured-NSSAI, or a subset thereof as described below, e.g. if the UE has no Allowed NSSAI for the Access Type for the serving PLMN;

- the Allowed-NSSAI for the Access Type over which the Requested NSSAI is sent, or a subset thereof; or

- the Allowed-NSSAI for the Access Type over which the Requested NSSAI is sent, or a subset thereof, plus one or more S-NSSAIs from the Configured-NSSAI not yet in the Allowed NSSAI for the Access Type as described below.

NOTE 1: If the UE wishes to register only a subset of the S-NSSAIs from the Configured NSSAI or the Allowed NSSAI, to be able to register with some Network Slices e.g. to establish PDU Sessions for some application(s), and the UE uses the URSP rules (which includes the NSSP) or the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45], then the UE uses applicable the URSP rules or the UE Local Configuration to ensure that the S-NSSAIs included in the Requested NSSAI are not in conflict with the URSP rules or with the UE Local Configuration.

The subset of S-NSSAIs in the Configured-NSSAI provided in the Requested NSSAI consists of one or more S-NSSAI(s) in the Configured NSSAI applicable to this PLMN, if one is present, and for which no corresponding S-NSSAI is already present in the Allowed NSSAI for the access type for this PLMN. The UE shall not include in the Requested NSSAI any S-NSSAI that is currently rejected by the network (i.e. rejected in the current registration area or rejected in the PLMN). For the registration to a PLMN for which neither a Configured NSSAI applicable to this PLMN or an Allowed NSSAI are present, the S-NSSAIs provided in the Requested NSSAI correspond to the S-NSSAI(s) in the Default Configured NSSAI unless the UE has HPLMN S-NSSAI for established PDU Session(s) in which case the HPLMN S-NSSAI(s) shall be provided in the mapping of Requested NSSAI in the NAS Registration Request message, with no corresponding VPLMN S-NSSAI in the Requested NSSAI.

When a UE registers over an Access Type with a PLMN, the UE shall also indicate in the Registration Request message when the Requested NSSAI is based on the Default Configured NSSAI.

The UE shall include the Requested NSSAI in the RRC Connection Establishment and in the establishment of the connection to the N3IWF/TNGF (as applicable) and in the NAS Registration procedure messages subject to conditions set out in clause 5.15.9. However, the UE shall not indicate any NSSAI in RRC Connection Establishment or Initial NAS message unless it has either a Configured NSSAI for the corresponding PLMN, an Allowed NSSAI for the corresponding PLMN and Access Type, or the Default Configured NSSAI. If the UE has HPLMN S-NSSAI(s) for established PDU Session(s), the HPLMN S-NSSAI(s) shall be provided in the mapping of Requested NSSAI in the NAS Registration Request message, independent of whether the UE has the corresponding VPLMN S-NSSAI. The (R)AN shall route the NAS signalling between this UE and an AMF selected using the Requested NSSAI obtained during RRC Connection Establishment or connection to N3IWF/TNGF respectively. If the (R)AN is unable to select an AMF based on the Requested NSSAI, it routes the NAS signalling to an AMF from a set of default AMFs. In the NAS signalling, if available, the UE provides the mapping of each S-NSSAI of the Requested NSSAI to a corresponding HPLMN S-NSSAI.

When a UE registers with a PLMN, if for this PLMN the UE has not included a Requested NSSAI nor a GUAMI while establishing the connection to the (R)AN, the (R)AN shall route all NAS signalling from/to this UE to/from a default AMF. When receiving from the UE a Requested NSSAI and a 5G-S-TMSI or a GUAMI in RRC Connection Establishment or in the establishment of connection to N3IWF/TNGF, if the 5G-AN can reach an AMF corresponding to the 5G-S-TMSI or GUAMI, then 5G-AN forwards the request to this AMF. Otherwise, the 5G-AN selects a suitable AMF based on the Requested NSSAI provided by the UE and forwards the request to the selected AMF. If the 5G-AN is not able to select an AMF based on the Requested NSSAI, then the request is sent to a default AMF.

When the AMF selected by the AN during Registration Procedure receives the UE Registration request, or after an AMF selection by MME (i.e. during EPS to 5GS handover) the AMF receives S-NSSAI(s) from SMF+PGW-C in 5GC:

- As part of the Registration procedure described in TS 23.502 [3], clause 4.2.2.2.2, or as part of the EPS to 5GS handover using N26 interface procedure described in clause 4.11.1.2.2 in TS 23.502 [3], the AMF may query the UDM to retrieve UE subscription information including the Subscribed S-NSSAIs.

- The AMF verifies whether the S-NSSAI(s) in the Requested NSSAI or the S-NSSAI(s) received from SMF+PGW-C are permitted based on the Subscribed S-NSSAIs (to identify the Subscribed S-NSSAIs the AMF may use the mapping to HPLMN S-NSSAIs provided by the UE, in the NAS message, for each S-NSSAI of the Requested NSSAI).

- When the UE context in the AMF does not yet include an Allowed NSSAI for the corresponding Access Type, the AMF queries the NSSF (see (B) below for subsequent handling), except in the case when, based on configuration in this AMF, the AMF is allowed to determine whether it can serve the UE (see (A) below for subsequent handling). The IP address or FQDN of the NSSF is locally configured in the AMF.

NOTE 2: The configuration in the AMF depends on operator's policy.

- When the UE context in the AMF already includes an Allowed NSSAI for the corresponding Access Type, based on the configuration for this AMF, the AMF may be allowed to determine whether it can serve the UE (see (A) below for subsequent handling).

- AMF or NSSF may have previously subscribed to slice load level and/or Observed Service Experience and/or Dispersion Analytics related network data analytics for a Network Slice from NWDAF. If AMF subscribes to analytics, AMF may determine that it cannot serve the UE based on received analytics (see (A) below). If AMF subscribes to Network Slice restriction notification service from NSSF, it may determine that it cannot serve the UE after the restriction notification is received (see (A) below). If AMF does not subscribe to Network Slice restriction notification service from NSSF, NSSF may take the analytics information into account when AMF queries NSSF (see (B) below).NOTE 3: The configuration in the AMF depends on the operator's policy.

**(A)** Depending on fulfilling the configuration as described above, the AMF may be allowed to determine whether it can serve the UE, and the following is performed:

- For the mobility from EPS to 5GS, the AMF first derives the serving PLMN value(s) of S-NSSAI(s) based on the HPLMN S-NSSAI(s) in the mapping of Requested NSSAI (in CM-IDLE state) or the HPLMN S-NSSAI(s) received from SMF+PGW-C (in CM-CONNECTED state). After that the AMF regards the derived value(s) as the Requested NSSAI.

- For the inter PLMN within 5GC mobility, the new AMF derives the serving PLMN value(s) of S-NSSAI(s) based on the HPLMN S-NSSAI(s) in the mapping of Requested NSSAI. After that the AMF regards the derived value(s) as the Requested NSSAI.

- AMF checks whether it can serve all the S-NSSAI(s) from the Requested NSSAI present in the Subscribed S-NSSAIs (potentially using configuration for mapping S-NSSAI values between HPLMN and Serving PLMN), or all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs in the case that no Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI are permitted, i.e. do not match any of the Subscribed S-NSSAIs or not available at the current UE's Tracking Area (see clause 5.15.3).

- If AMF has subscribed to slice load level and/or Observed Service Experience and/or Dispersion Analytics related network data analytics for a Network Slice from NWDAF, or if AMF had received a Network Slice restriction from NSSF, it may use that information to determine whether the AMF can serve the UE on the S-NSSAI(s) in the Requested NSSAI.

- If the AMF can serve the S-NSSAIs in the Requested NSSAI, the AMF remains the serving AMF for the UE. The Allowed NSSAI is then composed of the list of S-NSSAI(s) in the Requested NSSAI permitted based on the Subscribed S-NSSAIs and/or the list of S-NSSAI(s) for the Serving PLMN which are mapped to the HPLMN S-NSSAI(s) provided in the mapping of Requested NSSAI permitted based on the Subscribed S-NSSAIs, or, if neither Requested NSSAI nor the mapping of Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI are permitted, all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs and taking also into account the availability of the Network Slice instances as described in clause 5.15.8 that are able to serve the S-NSSAI(s) in the Allowed NSSAI in the current UE's Tracking Areas in addition to any Network Slice instance restriction for the S-NSSAI(s) in the Allowed NSSAI provided by the NSSF. It also determines the mapping if the S-NSSAI(s) included in the Allowed NSSAI needs to be mapped to Subscribed S-NSSAI(s) values. If no Requested NSSAI is provided, or the mapping of the S-NSSAIs in Requested NSSAI to HPLMN S-NSSAIs is incorrect, or the Requested NSSAI includes an S-NSSAI that is not valid in the Serving PLMN, or the UE indicated that the Requested NSSAI is based on the Default Configured NSSAI, the AMF, based on the Subscribed S-NSSAI(s) and operator's configuration, may also determine the Configured NSSAI for the Serving PLMN and, if applicable, the associated mapping of the Configured NSSAI to HPLMN S-NSSAIs, so these can be configured in the UE. Then Step (C) is executed.

- Else, the AMF queries the NSSF (see (B) below).

**(B)** When required as described above, the AMF needs to query the NSSF, and the following is performed:

- The AMF queries the NSSF, with Requested NSSAI (excluding S-NSSAIs subject to NSSA which are in "Pending" state and are not yet in the Allowed NSSAI, if any), Default Configured NSSAI Indication, mapping of Requested NSSAI to HPLMN S-NSSAIs, the Subscribed S-NSSAIs (with an indication if marked as default S-NSSAI), any Allowed NSSAI it might have for the other Access Type (including its mapping to HPLMN S-NSSAIs), PLMN ID of the SUPI and UE's current Tracking Area.

- Based on this information, local configuration, and other locally available information including RAN capabilities in the current Tracking Area for the UE or load level information for a Network Slice instance provided by the NWDAF, the NSSF does the following:

- It verifies which S-NSSAI(s) in the Requested NSSAI are permitted based on comparing the Subscribed S-NSSAIs with the S-NSSAIs in the mapping of Requested NSSAI to HPLMN S-NSSAIs. It considers the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs in the case that no Requested NSSAI was provided or no S-NSSAI from the Requested NSSAI are permitted i.e. are not present in the Subscribed S-NSSAIs or not available e.g. at the current UE's Tracking Area.

- If AMF has not subscribed to Network Slice instance restriction service from NSSF and NSSF has subscribed to slice load level and/or Observed Service Experience and/or Dispersion Analytics related network data analytics for a Network Slice from NWDAF, NSSF may use the analytics information for the determination of the (Network Slice instance(s) and the) list of S-NSSAI(s) in the Allowed NSSAI(s) to serve the UE.

- It selects the Network Slice instance(s) to serve the UE. When multiple Network Slice instances in the UE's Tracking Area are able to serve a given S-NSSAI, based on operator's configuration, the NSSF may select one of them to serve the UE, or the NSSF may defer the selection of the Network Slice instance until a NF/service within the Network Slice instance needs to be selected.

- It determines the target AMF Set to be used to serve the UE, or, based on configuration, the list of candidate AMF(s), possibly after querying the NRF.

NOTE 4: If the target AMF(s) returned from the NSSF is the list of candidate AMF(s), the Registration Request message can only be redirected via the direct signalling between the initial AMF and the selected target AMF as described in clause 5.15.5.2.3.

- It determines the Allowed NSSAI(s) for the applicable Access Type, composed of the list of S-NSSAI(s) in the Requested NSSAI permitted based on the Subscribed S-NSSAIs and/or the list of S-NSSAI(s) for the Serving PLMN which are mapped to the HPLMN S-NSSAIs provided in the mapping of Requested NSSAI permitted based on the Subscribed S-NSSAIs, or, if neither Requested NSSAI nor the mapping of Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI are permitted, all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs, and taking also into account the availability of the Network Slice instances as described in clause 5.15.8 that are able to serve the S-NSSAI(s) in the Allowed NSSAI in the current UE's Tracking Areas.

- It also determines the mapping of each S-NSSAI of the Allowed NSSAI(s) to the Subscribed S-NSSAIs if necessary.

- Based on operator configuration, the NSSF may determine the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s).

- Additional processing to determine the Allowed NSSAI(s) in roaming scenarios and the mapping to the Subscribed S-NSSAIs, as described in clause 5.15.6.

- If no Requested NSSAI is provided or the Requested NSSAI includes an S-NSSAI that is not valid in the Serving PLMN, or the mapping of the S-NSSAIs in Requested NSSAI to HPLMN S-NSSAIs is incorrect, or the Default Configured NSSAI Indication is received from AMF, the NSSF based on the Subscribed S-NSSAI(s) and operator configuration may also determine the Configured NSSAI for the Serving PLMN and, if applicable, the associated mapping of the Configured NSSAI to HPLMN S-NSSAIs, so these can be configured in the UE.

- The NSSF returns to the current AMF the Allowed NSSAI for the applicable Access Type, the mapping of each S-NSSAI of the Allowed NSSAI to the Subscribed S-NSSAIs if determined and the target AMF Set, or, based on configuration, the list of candidate AMF(s). The NSSF may return the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s), and the NRF to be used to determine the list of candidate AMF(s) from the AMF Set. The NSSF may return NSI ID(s) to be associated to the Network Slice instance(s) corresponding to certain S-NSSAIs. NSSF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1. The NSSF may return the Configured NSSAI for the Serving PLMN and the associated mapping of the Configured NSSAI to HPLMN S-NSSAIs.

 - Depending on the available information and based on configuration, the AMF may query the appropriate NRF (e.g. locally pre-configured or provided by the NSSF) with the target AMF Set. The NRF returns a list of candidate AMFs.

- If AMF Re-allocation is necessary, the current AMF reroutes the Registration Request or forwards the UE context to a target serving AMF as described in clause 5.15.5.2.3.

- Step (C) is executed.

**(C)** The serving AMF shall determine a Registration Area such that all S-NSSAIs of the Allowed NSSAI for this Registration Area are available in all Tracking Areas of the Registration Area (and also considering other aspects as described in clause 5.3.2.3) and then return to the UE this Allowed NSSAI and the mapping of the Allowed NSSAI to the Subscribed S-NSSAIs if provided. The AMF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1.

NOTE 5: As there is a single distinct Registration Area for Non-3GPP access in a PLMN, the S-NSSAIs in the Allowed NSSAI for this Registration Area (i.e. for Non-3GPP access) are available homogeneously in the PLMN.

When either no Requested NSSAI was included, or the mapping of the S-NSSAIs in Requested NSSAI to HPLMN S-NSSAIs is incorrect, or a Requested NSSAI is not considered valid in the PLMN and as such at least one S-NSSAI in the Requested NSSAI was rejected as not usable by the UE in the PLMN, or the UE indicated that the Requested NSSAI is based on the Default Configured NSSAI, the AMF may update the UE slice configuration information for the PLMN as described in clause 5.15.4.2.

If the Requested NSSAI does not include S-NSSAIs which map to S-NSSAIs of the HPLMN subject to Network Slice-Specific Authentication and Authorization and the AMF determines that no S-NSSAI can be provided in the Allowed NSSAI for the UE in the current UE's Tracking Area and if no default S-NSSAI(s) could be added as described in step (A), the AMF shall reject the UE Registration and shall include in the rejection message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

If the Requested NSSAI includes S-NSSAIs which map to S-NSSAIs of the HPLMN subject to Network Slice-Specific Authentication and Authorization, the AMF shall include in the Registration Accept message an Allowed NSSAI containing only those S-NSSAIs that are not to be subject to Network Slice-Specific Authentication and Authorization and, based on the UE Context in AMF, those S-NSSAIs for which Network Slice-Specific Authentication and Authorization for at least one of the corresponding HPLMN S-NSSAIs succeeded previously regardless the Access Type, if any.

The AMF shall also provide the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

The S-NSSAIs which map to S-NSSAIs of the HPLMN subject to Network Slice-Specific Authentication and Authorization is ongoing are in "pending" state in the AMF and shall be included in the Pending NSSAI. The Pending NSSAI may contain a mapping of the S-NSSAI(s) for the Serving PLMN to the HPLMN S-NSSAIs, if applicable. The UE shall not include in the Requested NSSAI any of the S-NSSAIs from the Pending NSSAI the UE stores, regardless of the Access Type.

If:

- all the S-NSSAI(s) in the Requested NSSAI are still to be subject to Network Slice-Specific Authentication and Authorization; or

- no Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI matches any of the Subscribed S-NSSAIs, and all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs are to be subject to Network Slice-Specific Authentication and Authorization;

the AMF shall provide an empty Allowed NSSAI to the UE in the Registration Accept message. Upon receiving an empty Allowed NSSAI, the UE is registered in the PLMN but shall wait for the completion of the Network Slice-Specific Authentication and Authorization without attempting to use any service provided by the PLMN on any access, except e.g. emergency services (see TS 24.501 [47]), until the UE receives an allowed NSSAI.

Then, the AMF shall initiate the Network Slice-Specific Authentication and Authorization procedure as described in clause 5.15.10 for each S-NSSAI that requires it, except, based on Network policies, for those S-NSSAIs for which Network Slice-Specific Authentication and Authorization have been already initiated on another Access Type for the same S-NSSAI(s). At the end of the Network Slice-Specific Authentication and Authorization steps, the AMF by means of the UE Configuration Update procedure shall provide a new Allowed NSSAI to the UE which also contains the S-NSSAIs subject to Network Slice-Specific Authentication and Authorization for which the authentication and authorization is successful. The AMF may perform AMF selection when NSSAA completes for the S-NSSAIs subject to S-NSSAI in "pending" status. If an AMF change is required, this shall be triggered by the AMF using the UE Configuration Update procedure indicating a UE re-registration is required. The S-NSSAIs which were not successfully authenticated and authorized are not included in the Allowed NSSAI and are included in the list of Rejected S-NSSAIs with a rejection cause value indicating Network Slice-Specific Authentication and Authorization failure.

Once completed the Network Slice-Specific Authentication and Authorization procedure, if the AMF determines that no S-NSSAI can be provided in the Allowed NSSAI for the UE, which is already authenticated and authorized successfully by a PLMN, and if no default S-NSSAI(s) could be added as described in step (A), the AMF shall execute the Network-initiated Deregistration procedure described in TS 23.502 [3], clause 4.2.2.3.3, and shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

If an S-NSSAI is rejected with a rejection cause value indicating Network Slice-Specific Authentication and Authorization failure or revocation, the UE can re-attempt to request the S-NSSAI based on policy, local in the UE.

##### 5.15.5.2.2 Modification of the Set of Network Slice(s) for a UE

The set of Network Slices for a UE can be changed at any time while the UE is registered with a network, and may be initiated by the network, or by the UE, under certain conditions as described below.

The network, based on local policies, subscription changes and/or UE mobility, and/or UE Dispersion data classification, operational reasons (e.g. a Network Slice instance is no longer available or load level information or service experience for a Network Slice or network slice instance provided by the NWDAF), may change the set of Network Slice(s) to which the UE is registered and provide the UE with a new Registration Area and/or Allowed NSSAI and the mapping of this Allowed NSSAI to HPLMN S-NSSAIs, for each Access Type over which the UE is registered. In addition, the network may provide the Configured NSSAI for the Serving PLMN, the associated mapping information, and the rejected S-NSSAIs. The network may perform such a change over each Access Type during a Registration procedure or trigger a notification towards the UE of the change of the Network Slices using a UE Configuration Update procedure as specified in TS 23.502 [3], clause 4.2.4. The new Allowed NSSAI(s) and the mapping to HPLMN S-NSSAIs are determined as described in clause 5.15.5.2.1 (an AMF Re-allocation may be needed). The AMF provides the UE with:

- an indication that the acknowledgement from UE is required;

- Configured NSSAI for the Serving PLMN (if required), rejected S-NSSAI(s) (if required) and TAI list, and

- the new Allowed NSSAI with the associated mapping of Allowed NSSAI for each Access Type (as applicable) unless the AMF cannot determine the new Allowed NSSAI (e.g. all S-NSSAIs in the old Allowed NSSAI have been removed from the Subscribed S-NSSAIs).

 Furthermore:

- If the changes to the Allowed NSSAI require the UE to perform immediately a Registration procedure because they affect the existing connectivity to Network Slices (e.g. the new S-NSSAIs require a separate AMF that cannot be determined by the current serving AMF, or the AMF cannot determine the Allowed NSSAI) or due to AMF local policies also when the changes does not affect the existing connectivity to Network Slices:

- The serving AMF indicates to the UE the need for the UE to perform a Registration procedure without including the GUAMI or 5G-S-TMSI in the access stratum signalling after entering CM-IDLE state. The AMF shall release the NAS signalling connection to the UE to allow to enter CM-IDLE after receiving the acknowledgement from UE.

- When the UE receives indications to perform a Registration procedure without including the GUAMI or 5G-S-TMSI in the access stratum signalling after entering CM-IDLE state, then:

- The UE deletes any stored (old) Allowed NSSAI and associated mapping as well as any (old) rejected S-NSSAI.

- The UE shall initiate a Registration procedure with the registration type Mobility Registration Update after the UE enters CM-IDLE state as specified in as described in TS 23.502 [3] step 4 of clause 4.2.4.2. The UE shall include a Requested NSSAI (as described in clause 5.15.5.2.1) with the associated mapping of Requested NSSAI in the Registration Request message. Also, the UE shall include, subject to the conditions set out in clause 5.15.9, a Requested NSSAI in access stratum signalling but no GUAMI.

If there are established PDU Session(s) associated with emergency services, then the serving AMF indicates to the UE the need for the UE to perform a Registration procedure but does not release the NAS signalling connection to the UE. The UE performs the Registration procedure only after the release of the PDU Session(s) used for the emergency services.

In addition to sending the new Allowed NSSAI to the UE, when a Network Slice used for a one or multiple PDU Sessions is no longer available for a UE, the following applies:

- If the Network Slice becomes no longer available under the same AMF (e.g. due to UE subscription change), the AMF indicates to the SMF(s) which PDU Session ID(s) corresponding to the relevant S-NSSAI shall be released. SMF releases the PDU Session according to clause 4.3.4.2 in TS 23.502 [3].

- If the Network Slice becomes no longer available upon a change of AMF (e.g. due to Registration Area change), the new AMF indicates to the old AMF that the PDU Session(s) corresponding to the relevant S-NSSAI shall be released. The old AMF informs the corresponding SMF(s) to release the indicated PDU Session(s). The SMF(s) release the PDU Session(s) as described in clause 4.3.4 of TS 23.502 [3]. Then the new AMF modifies the PDU Session Status correspondingly. The PDU Session(s) context is locally released in the UE after receiving the PDU Session Status in the Registration Accept message.

The UE uses either the URSP rules (which includes the NSSP) or the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45] to determine whether ongoing traffic can be routed over existing PDU Sessions belonging to other Network Slices or establish new PDU Session(s) associated with same/other Network Slice.

In order to change the set of S-NSSAIs the UE is registered to over an Access Type, the UE shall initiate a Registration procedure over this Access Type as specified in clause 5.15.5.2.1.

If, for an established PDU Session:

- none of the values of the S-NSSAIs of the HPLMN in the mapping of the Requested NSSAI to S-NSSAIs of the HPLMN included in the Registration Request matches the S-NSSAI of the HPLMN associated with the PDU Session; or

- none of the values of the S-NSSAIs in the Requested NSSAI matches the value of the S-NSSAI of HPLMN associated with the PDU Session and the mapping of the Requested NSSAI to S-NSSAIs of the HPLMN is not included in the Registration Request,

the network shall release this PDU Session as follows.

- the AMF informs the corresponding SMF(s) to release the indicated PDU Session(s). The SMF(s) release the PDU Session(s) as described in clause 4.3.4 of TS 23.502 [3]. Then the AMF modifies the PDU Session Status correspondingly. The PDU Session(s) context is locally released in the UE after receiving the PDU Session Status from the AMF.

A change of the set of S-NSSAIs (whether UE or Network initiated) to which the UE is registered may, subject to operator policy, lead to AMF change, as described in clause 5.15.5.2.1.

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

#### 5.15.5.3 Establishing a PDU Session in a Network Slice

The PDU Session Establishment in a Network Slice instance to a DN allows data transmission in a Network Slice instance. A PDU Session is associated to an S-NSSAI and a DNN. A UE that is registered in a PLMN over an Access Type and has obtained a corresponding Allowed NSSAI, shall indicate in the PDU Session Establishment procedure the S-NSSAI according to the NSSP in the URSP rules or according to the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45], and, if available, the DNN the PDU Session is related to. The UE includes the appropriate S-NSSAI from this Allowed NSSAI and, if mapping of the Allowed NSSAI to HPLMN S-NSSAIs was provided, an S-NSSAI with the corresponding value from this mapping.

If the UE cannot determine any S-NSSAI after performing the association of the application to a PDU Session according to clause 6.1.2.2.1 of TS 23.503 [45], the UE shall not indicate any S-NSSAI in the PDU Session Establishment procedure.

The network (HPLMN) may provision the UE with Network Slice selection policy (NSSP) as part of the URSP rules, see TS 23.503 [45], clause 6.6.2. When the Subscription Information contains more than one S-NSSAI and the network wants to control/modify the UE usage of those S-NSSAIs, then the network provisions/updates the UE with NSSP as part of the URSP rules. When the Subscription Information contains only one S-NSSAI, the network needs not provision the UE with NSSP as part of the URSP rules. The NSSP rules associate an application with one or more HPLMN S-NSSAIs. A default rule which matches all applications to a HPLMN S-NSSAI may also be included.

The UE shall store and use the URSP rules, including the NSSP, as described in TS 23.503 [45]. When a UE application associated with a specific S-NSSAI requests data transmission:

- if the UE has one or more PDU Sessions established corresponding to the specific S-NSSAI, the UE routes the user data of this application in one of these PDU Sessions, unless other conditions in the UE prohibit the use of these PDU Sessions. If the application provides a DNN, then the UE considers also this DNN to determine which PDU Session to use. This is further described in TS 23.503 [45], clause 6.6.2.

- If the UE does not have a PDU Session established with this specific S-NSSAI, the UE requests a new PDU Session corresponding to this S-NSSAI and with the DNN that may be provided by the application. In order for the RAN to select a proper resource for supporting network slicing in the RAN, RAN needs to be aware of the Network Slices used by the UE. This is further described in TS 23.503 [45], clause 6.6.2.

If the AMF is not able to determine the appropriate NRF to query for the S-NSSAI provided by the UE, the AMF may query the NSSF with this specific S-NSSAI, location information, PLMN ID of the SUPI. The NSSF determines and returns the appropriate NRF to be used to select NFs/services within the selected Network Slice instance. The NSSF may also return an NSI ID to be used to select NFs within the selected Network Slice instance to use for this S-NSSAI.

The AMF or NSSF may select a Network Slice instance based on load level and/or Observe Service Experience and/or Dispersion analytics from NWDAF.

The IP address or FQDN of the NSSF is locally configured in the AMF.

SMF discovery and selection within the selected Network Slice instance is initiated by the AMF when a SM message to establish a PDU Session is received from the UE. The appropriate NRF is used to assist the discovery and selection tasks of the required network functions for the selected Network Slice instance.

The AMF queries the appropriate NRF to select an SMF in a Network Slice instance based on S-NSSAI, DNN, NSI-ID (if available) and other information e.g. UE subscription and local operator policies, when the UE triggers PDU Session Establishment. The selected SMF establishes a PDU Session based on S-NSSAI and DNN.

When the AMF belongs to multiple Network Slice instances, based on configuration, the AMF may use an NRF at the appropriate level for the SMF selection.

For further details on the SMF selection, refer to clause 4.3.2.2.3 in TS 23.502 [3].

When a PDU Session for a given S-NSSAI is established using a specific Network Slice instance, the CN provides to the (R)AN the S-NSSAI corresponding to this Network Slice instance to enable the RAN to perform access specific functions.

The UE shall not perform PDU Session handover from one Access Type to another if the S-NSSAI of the PDU Session is not included in the Allowed NSSAI of the target Access Type.

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