**3GPP TSG-SA2 Meeting #154AH  *S2-22XXXX***

**January 16 – 20, 2023 (*revision of S2-22xxxx*)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** |  | **rev** |  | **Current version:** | **18.0.0** |  |
|  |
| *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:***  |

|  |
| --- |
| KI#4: Support for Centralized NSACF in a PLMN with multi-service areas |

 |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | eNS\_Ph3 |  | ***Date:*** | 2022-12-22 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | To enable support of a single centralized NSACF in a PLMN with multi service areas. |
|  |  |
| ***Summary of change:*** | Enable deployment in a PLMN with multiservice area with a single centralized NSACF. The centralized NSACF supports all services currently supported by a non-centralized NSACF architecture with the additional attribute of the service area identity where the AMF/SMF is located being passed on to the centralized NSACF. The AMF and SMF provides the service area identity to the centralized NSACF.  |
| ***--*** |  |
| ***Consequences if not approved:*** | No Support for eNS-PH3 for KI#4. |
|  |  |
| ***Clauses affected:*** | 5.15.11.0, 5.15.11.1, 5.15.11.2, 5.15.11.5, 6.2.28, 6.3.22. |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...23.502 CR |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR’s revision history:*** |  |

\* \* \* \* 1st change \* \* \* \*

#### 5.15.11.0 General

The Network Slice Admission Control Function (NSACF) monitors and controls the number of registered UEs per network slice and/or the number of PDU Sessions per network slice for the network slices that are subject to Network Slice Admission Control (NSAC). The NSACF is configured with the maximum number of UEs and/or the maximum number of PDU Sessions allowed to be served per S-NSSAI subject to NSAC. The NSACF is also configured with information indicating applicable access type(s) for the S-NSSAI (i.e. 3GPP Access Type, Non-3GPP Access Type, or both).

The NSACF also provides event-based Network Slice status notifications and reports to the consumer NFs (e.g. AF).

The NSACF may be responsible for one or more S-NSSAIs. For one S-NSSAI there may be one or multiple NSACFs deployed in a network (a PLMN or a SNPN) as follows:

- If the network is configured with a single service area, there is a single NSACF configured with the maximum number of UEs per network slice and/or the maximum number of PDU Sessions per network slice, which are valid in the network.

- If the network is configured with multiple service areas, an NSACF may be deployed on a service area basis, which can be one NSACF instance or one NSACF Set. There are multiple NSACF architecture options:

- -Option 1: non-Centralized Single tier NSACF architecture. In this architecture, independent NSACFs are deployed in every service area. There is no interaction between the NSACFs deployed in different service area. Each NSACF is configured with the maximum number of UEs per network slice and/or the maximum number of PDU Sessions which are valid in the service area (see clause 5.15.11.1 for more details).

- Option 2: Centralized architecture. In this architecture, a single centralized NSACF is deployed in the network to handle admissions in all service areas. The centralized NSACF is configured with the total number of UEs per network slice and the maximum number of PDU Sessions for the entire PLMN. NSAC Requests from AMF or SMF to the single centralized NSCAF in this case includes the service area of the NF consumer if available.

NOTE 1: It is possible to configure in the centralized architecture the maximum number of registered UEs and/or the number of PDU sessions per service area if required by the operator. In this case, NSAC admission can be performed on a per service area.

- Option 3: Hierarchical NSACF architecture is deployed in the network. There are two roles of NSACF and interaction between them may be required (see clause 5.15.11.1a for more details):

- Primary NSACF, controls and distributes of the maximum number of UEs and/or the maximum number of PDU Sessions for other NSACF(s) deployed in different service Area. The Primary NSACF handles overall NSAC for an S-NSSAI at the global level (i.e. it is ultimately responsible for the NSAC for an S-NSSAI).

‐ NSACF is responsible for one or multiple Service Area. And one Service area is only associated with one NSACF instance or one NSACF Set.

NOTE 2: When multiple NSACFs are deployed, how the maximum number of UEs per network slice and the maximum number of PDU Sessions per network slice is distributed (by OAM for Option 1 and by the primary NSAF for Option 3) among multiple NSACFs, is implementation specific.

NOTE 3: When multiple NSACFs are deployed based on option 1, the UE moves to new service area with a different NSACF, and if the number of UE or PDU Sessions in the target NSACF has reached the maximum number, whether the session continuity can be guaranteed is left to implementation.

Subject to operator policy and national/regional regulations, the AMF may exempt UEs and the SMF may exempt PDU sessions from NSAC when the UE and/or PDU Session is used for Emergency service or for Critical and Priority services (e.g. MCX, MPS).

When the AMF receives a Registration Request for an Emergency Registration, or with a Registration Request with an Establishment Cause indicating a priority service (e.g. MCX, MPS) or when the AMF determines that there is a priority subscription (e.g., MPS, MCX) in the UDM, the AMF may accept the registration request without applying NSAC, i.e. the AMF triggers the NSAC procedure, but the response from the NSACF is ignored at the AMF.

When the SMF receives a PDU Session Establishment Request for an emergency PDU Session or a PDU Session Establishment Request with a priority header, the SMF may accept the PDU Session Establishment Request without applying NSAC, i.e. the SMF triggers the NSAC procedure, but the response from the NSACF is ignored at the SMF.

Alternatively, when NSAC is exempted for the UE and/or PDU Session, the AMF and the SMF skip the corresponding NSAC procedure, i.e. this UE (respectively PDU Session) is not counted towards the maximum number of UEs (respectively PDU Sessions).

The support of NSAC for the S-NSSAI used for onboarding as described in clause 5.30.2.10 is optional and subject to Onboarding Network operator policies. However, NSAC for S-NSSAI used for onboarding is not applicable to UEs that registered in ON-SNPN with Registration Type "SNPN Onboarding".

\* \* \* \* Next change \* \* \* \*

#### 5.15.11.1 Network Slice Admission Control for maximum number of UEs

The NSACF keeps track of the current number of UEs registered for a network slice so that it can ensure it does not exceed the maximum number of UEs allowed to register with the network slice. The NSACF also maintains a list of UE IDs registered with a network slice that is subject to NSAC. When an event related to a UE causes the current number of UEs registered with a network slice to increase, the NSACF first checks whether the UE Identity is already in the list of UEs registered with that network slice. If not, the NSACF checks whether the maximum number of UEs per network slice for that network slice has already been reached and if it has, the NSACF applies admission control policies. For deployments with a centralized NSACF architecture, in addition to the above, the centralized NSACF also maintains the service area for the AMF the UE is registered with if available. In this case, the AMF provides the information to the centralized NSACF.

The AMF triggers a request to NSACF for NSAC for maximum number of UEs when the UE's registration status for a network slice subject to NSAC is changing, i.e. during the UE Registration procedure in clause 4.2.2.2.2 of TS 23.502 [3], UE Deregistration procedure in clause 4.2.2.3 of TS 23.502 [3], Network Slice-Specific Authentication and Authorisation procedure in clause 4.2.9.2 of TS 23.502 [3], AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure in clause 4.2.9.3 of TS 23.502 [3], AAA Server triggered Slice-Specific Authorization Revocation in clause 4.2.9.4 of TS 23.502 [3] and UE Configuration Update procedure in clause 4.2.4.2 of TS 23.502 [3].

NOTE 1: Early Admission Control (EAC) mode is applicable for Number of UEs per network slice admission control. The use of EAC in relation to the number of registered UEs is described in clauses 4.2.11.2 and 4.2.11.3 of TS 23.502 [3].

Since the UE may register or deregister for an S-NSSAI via 3GPP access and/or non-3GPP access as described in clause 5.15.5.2.1. The Allowed NSSAI for the access type may change while the UE is registering to a network. The AMF provides the Access Type to the NSACF when triggering a request to increase or decrease the current number of UEs registered with a S-NSSAI. The NSACF may take the Access Type into account for increasing and decreasing the number of UEs per network slice by storing the UE ID with the associated one or more Access Type(s), i.e. the NSACF is able to add or remove a registration for the UE ID for each Access Type and trigger the increase or decrease of the current number of UEs registered with a S-NSSAI based on a policy that takes the access type into account. If the Access Type provided by the AMF is not configured for NSAC in the NSACF, the NSACF always accepts the request from the AMF without increasing or decreasing the number of UEs. If the Access Type provided by the AMF is configured for NSAC in the NSACF and the maximum number is reached, the NSACF sends a reject response to the AMF including the access type.

NOTE 2: For example, if the NSACF is configured to apply NSAC for 3GPP Access Type only, the NSACF counts registration via 3GPP access type only. If the NSACF is configured to apply NSAC for both Access Types, and the UE newly registers via 3GPP access while the UE is already registered via non-3GPP access (or vice versa), the NSACF updates the UE ID entry with both 3GPP Access Type and non-3GPP Access Type and the NSACF may count the UE once or twice based on its policy.

\* \* \* \* Next change \* \* \* \*

#### 5.15.11.2 Network Slice Admission Control for maximum number of PDU sessions

The NSACF keeps track of the current number of PDU Sessions per network slice so that it can ensure it does not exceed the maximum number of PDU session allowed to be served by the network slice. When an event related to a UE causes the current number of PDU sessions established within the network slice is to increase, the NSACF checks whether the maximum number of PDU sessions per network slice for that network slice has already been reached and if it has, the NSACF applies admission control policies.

The anchor SMF triggers a request to NSACF for maximum number of PDU sessions per network slice control during PDU session establishment/release procedures in clauses 4.3.2 and 4.3.4 of TS 23.502 [3].

The SMF provides the Access Type to the NSACF when triggering a request to increase or decrease the number of PDU Sessions. The NSACF takes Access Type into account for increasing and decreasing the current number of PDU Sessions depending on the applicability of the Access Type for the NSAC for maximum number of PDU Sessions for the S-NSSAI.

For deployments with a centralized NSACF the SMF, additionally, provides the service area information of the SMF to the centralized NSACF if available.NOTE 1: For MA PDU Session, the SMF provides the Access Type to NSACF when the user plane connection is about to be established or released in the corresponding access network. With this, the SMF provides one or two Access Types for the MA PDU Session in the same request message to the NSACF. The NSACF can reject a single or both Access Types depending on the applicability of the Access Type for the NSAC.

NOTE 2: I-SMF does not interact with NSCAF.

Access Type and the NSACF may count the UE once or twice based on its policy.

\* \* \* \* Next change \* \* \* \*

#### 5.15.11.5 Support of Network Slice Admission Control and Interworking with EPC

If EPS counting is required for a network slice, the NSAC for maximum number of UEs and/or for maximum number of PDU Sessions per network slice is performed at the time of PDN connection establishment in case of EPC interworking. To support the NSAC for maximum number of UEs and/or for maximum number of PDU Sessions per network slice in EPC, the SMF+PGW-C is configured with the information indicating which network slice is subject to NSAC. During PDN connection establishment in EPC, the SMF+PGW-C selects an S-NSSAI associated with the PDN connection as described in clause 5.15.7.1. If the selected S-NSSAI by the SMF+PGW-C is subject to the NSAC, the SMF+PGW-C triggers interaction with NSACF to check the availability of the network slice by invoking separate NSAC procedures for number of UE and number of PDU Session (as described in clause 4.11.5.9 of TS 23.502 [3]), before the SMF+PGW-C provides the selected S-NSSAI to the UE. If the network slice is available, the SMF+PGW-C continues to proceed with the PDN connection establishment procedure.

The NSACF performs the following for checking network slice availability prior to returning a response to the SMF+PGW-C:

- For NSAC for number of UEs, if the UE identity is already included in the list of UE IDs registered with a network slice, or the UE identity is not included in the list of UE IDs registered with a network slice and the current number of UE registration did not reach the maximum number, the NSACF responds to the SMF+PGW-C with the information that the network slice is available. The NSACF includes the UE identity in the list of UE IDs if not already on the list and increases the current number of UE registration. Otherwise, the NSACF returns a response indicating that the maximum number with the network slice has been reached.

- For NSAC for number of PDU Sessions, if the current number of PDU sessions is below the maximum number, the NSACF responds to the SMF+PGW-C with the information that the network slice is available. The NSACF increases the current number of PDU sessions. Otherwise, the NSACF returns the response indicating that the maximum number with the network slice has been reached.

If the maximum number of UEs and/or the maximum number of PDU sessions has already been reached, unless operator policy implements a different action, the SMF+PGW-C rejects the PDN connection.

NOTE 1: As an implementation option, if the APN is mapped to more than one S-NSSAI and the first selected S-NSSAI is not available (e.g. either current number of UE registration reached maximum or current number of PDU sessions reached maximum), then based on the operator policy the PGW-C+SMF can try another mapped S-NSSAI for the PDN connection establishment procedure.

If the establishment of a new PDN Connections is with a different SMF+PGW-C from the SMF+PGW-C used for already existing PDN connection associated with the same S-NSSAI, each SMF+PGW-C will send a request for update (e.g. increase or decrease) to the NSACF. The NSACF may maintain a registration entry per SMF+PGW-C for the same UE ID.

The SMF+PGW-C provides the Access Type to the NSACF when triggering a request to increase or decrease the number of UEs and/or the number of PDU Sessions for an S-NSSAI.

NOTE 2: The SMF+PGW-C determines the Access Type based on the RAT type parameter in the PMIP or GTP message received from the ePDG; or alternatively it can internally determine the Access Type based on the source node (e.g. SGW) sending the request for the PDN Connection establishment.

When the UE with ongoing PDN connection(s) moves from EPC to 5GC, the SMF+PGW-C triggers a request to decrease the number of the UE registration in NSACF and the AMF triggers a request to increase the number of the UE registration in NSACF when the UE is registered in the new AMF. If there are more than one PDN connections associated with the S-NSSAI, the NSACF may receive multiple requests for the same S-NSSAI from different SMF+PGW-Cs. When the UE with ongoing PDU session(s) moves from 5GC to EPC, the SMF+PGW-C triggers a request to increase the number of the UE registration in NSACF and the old AMF triggers a request to decrease the number of the UE registration in NSACF when the UE is deregistered in old AMF. If there are more than one PDU sessions associated with the S-NSSAI, the NSACF may receive multiple requests for the same S-NSSAI from different SMF+PGW-Cs. The NSACF maintains a list of UE IDs based on the requests from SMF+PGW-C(s) and AMF, and adjusts the current number of registrations accordingly.

When EPS counting is performed for a network slice, and the UE with ongoing PDN connection(s) moves from EPC to 5GC, session continuity is guaranteed from NSAC standpoint, as the admission was granted at the time of PDN connection establishment, i.e. the number of PDU session is not counted again in 5GC. Similarly, when the UE with ongoing PDU session(s) moves from 5GC to EPC, session continuity is guaranteed from NSAC standpoint as the admission of the PDN Connection(s) to the network slice was already granted at the time of PDU Session establishment in 5GC.

If the PDN connection associated with S-NSSAI is released in EPC, the SMF+PGW-C triggers a request (i.e. decrease) to NSACF for maximum number of UEs and/or maximum number of PDU sessions per network slice control. The NSACF decreases the current number of registrations and removes the UE identity from the list of UE IDs if the PDN connection(s) associated with the S-NSSAI are all released in EPC.

NOTE 3: NSAC in EPC is not performed for the attachment without PDN connectivity.

If EPS counting is not required for a network slice, the NSAC for maximum number of UEs and/or for maximum number of PDU Sessions per network slice is performed when the UE moves from EPC to 5GC, i.e. when the UE performs mobility Registration procedure from EPC to 5GC (NSAC for maximum number of UEs per network slice) and/or when the PDN connections are handed over from EPC to 5GC (NSAC for maximum number of PDU Sessions per network slice). The SMF+PGW-C is configured with the information indicating the network slice is subject to NSAC only in 5GS. The PDN connection interworking procedure is performed as described in clause 5.15.7.1. Mobility from EPC to 5GC does not guarantee all active PDU Session(s) can be transferred to the 5GC in certain circumstances when either the current number of UE registration or the current number of PDU sessions would exceed the maximum number when the UE moves from EPC to 5GC.

NOTE 4: Given that session continuity is not guaranteed when EPS counting is not required, it is recommended for services which require the session continuity to support EPS counting.

NOTE 5: When multiple NSACFs are deployed and if the number of UE in target NSACF has reached the maximum number, whether session continuity can be guaranteed is left to implementation

NOTE 6: When a centralized architecture is deployed, UE are always guaranteed admission at inter-system mobility.

\* \* \* \* Next change \* \* \* \*

### 6.2.28 NSACF

The Network Slice Admission Control Function (NSACF) support the following functionality:

- Support of monitoring and controlling the number of registered UEs per network slice.

- Support of monitoring and controlling the number of established PDU Sessions per network slice.

- Support of event based Network Slice status notification and reports to a consumer NF.

The details of the NSACF functionality are defined in clause 5.15.11.

The NSACF can be deployed in a PLMN including no or multiple service areas, with a centralized architecture, or a hierarchal architecture, as depicted in clause 5.15.11.0

\* \* \* \* Next change \* \* \* \*

### 6.3.22 NSACF discovery and selection

The NF consumers shall utilise the NRF to discover NSACF instance(s) unless NSACF information is available by other means, e.g. locally configured in NF consumers.

If the NSACF NF consumer is the AMF, the NSACF selection function in the AMF selects an NSACF instance based on the available NSACF instances, which are obtained from the NRF or locally configured in the AMF.

The following factors may be considered by the NF consumer for NSACF selection:

- S-NSSAI(s).

- NSACF Serving Area information. The NSACF service area is related to the location of the NF consumer.

- Centralized NSACF

NOTE: Each Serving Area is unique and unambiguously identified.

- NSACF service capabilities:

- Support monitoring and controlling the number of registered UEs per network slice for the network slice that is subject to NSAC.

- Support monitoring and controlling the number of established PDU Sessions per network slice for the network slice that is subject to NSAC.

In the case of delegated discovery and selection in SCP, the NSACF NF consumer shall send all available factors to the SCP.

\* \* \* \* End of changes \* \* \* \*