4 General

4.1 Overview

The non-access stratum (NAS) described in the present document forms the highest stratum of the control plane between the UE and the AMF (reference point "N1" see 3GPP TS 23.501 [8]) for both 3GPP and non-3GPP access.

Main functions of the protocols that are part of the NAS are:

a) support of mobility of the user equipment (UE) including also common procedures such as authentication, identification, generic UE configuration update and security mode control procedures;

b) support of session management procedures to establish and maintain data connectivity between the UE and the data network; and

c) NAS transport procedure to provide a transport of SMS, LPP, SLPP, LCS, UPP-CMI container, UE policy container, SOR transparent container and UE parameters update information payload.

Principles for the handing of 5GS security contexts and for the activation of ciphering and integrity protection, when a NAS signalling connection is established, are provided in subclause 4.4.

For the support of the above functions, the following procedures are supplied within this specification:

a) elementary procedures for 5GS mobility management in clause 5; and

b) elementary procedures for 5GS session management in clause 6.

Signalling procedures for the control of NAS security are described as part of the 5GMM common procedures in subclause 5.4.

Complete NAS transactions consist of specific sequences of elementary procedures. Examples of such specific sequences can be found in 3GPP TS 23.502 [9].

The NAS for 5GS follows the protocol architecture model for layer 3 as described in 3GPP TS 24.007 [11].

4.2 Coordination between the protocols for 5GS mobility management and 5GS session management

A 5GS session management (5GSM) message is piggybacked in specific 5GS mobility management (5GMM) transport messages. To this purpose, the 5GSM messages can be transmitted in an information element in the 5GMM transport messages. In this case, the UE, the AMF and the SMF execute the 5GMM procedure and the 5GSM procedure in parallel. The success of the 5GMM procedure is not dependent on the success of the piggybacked 5GSM procedure.

The UE can only initiate the 5GSM procedure when there is a 5GMM context established at the UE.

During 5GMM procedures, the UE and the AMF shall suspend the transmission of 5GSM messages, except when:

a) the 5GMM procedure is piggybacking 5GSM messages; or

b) the UE is in 5GMM-CONNECTED mode and a service request procedure for re-establishing user-plane resources of PDU session(s) is initiated without including PDU session status IE or Allowed PDU session status IE. In this case, the UE and the AMF need not suspend the transmission of 5GSM messages related to other PDU session(s) than the one(s) for which the user- plane resources re-establishment is requested.

If the UE determines to locally release the N1 NAS signalling connection upon receiving an SOR transparent container during a registration procedure as specified in 3GPP TS 23.122 [5] Annex C.2, the UE shall suspend the transmission of 5GSM messages after sending the REGISTRATION COMPLETE message and until the N1 NAS signalling connection is released to obtain service on a higher priority PLMN, with the exception of the case when the UE has an emergency PDU session.

A 5GMM message piggybacking a 5GSM message for a PDU session shall be delivered via the access associated with the PDU session, if any, with the following exceptions:

a) the AMF shall send, via 3GPP access, a DL NAS TRANSPORT message piggybacking a downlink 5GSM message of a network-requested 5GSM procedure for a PDU session associated with non-3GPP access if the conditions specified in subclause 5.5.1.3.4 or subclause 5.6.1.4 are met;

b) the UE shall send an UL NAS TRANSPORT message piggybacking a response message to the 5GSM message described in a) via either:

   1) 3GPP access; or

   2) non-3GPP access if the UE is in 5GMM-CONNECTED mode over non-3GPP access; and

NOTE: The interaction between the 5GMM sublayer and the 5GSM sublayer to enable the UE to send the UL NAS TRANSPORT message containing the response message via 3GPP access is required. This is achieved via UE implementation.

c) the UE shall send, via the target access, an UL NAS TRANSPORT message piggybacking a 5GSM message associated with a request type set to "existing PDU session" or "existing emergency PDU session" for handover of an existing PDU session between 3GPP access and non-3GPP access.

A 5GMM message piggybacking a 5GSM message as a response message to a request message associated with an MA PDU session, shall be delivered via the same access that the initial message was received.

4.3 UE domain selection

4.3.1 UE's usage setting

The UE's usage setting defined in 3GPP TS 24.301 [15] applies to voice capable UEs in 5GS and indicates whether the UE has preference for voice services over data services or vice-versa, where:

a) voice services include IMS voice; and

b) data services include any kind of user data transfer without a voice media component.

The UE's usage setting can be set to:

a) "voice centric"; or

b) "data centric".

If the UE is capable of S1 mode, there is a single UE's usage setting at the UE which applies to both 5GS and EPS.

4.3.2 Domain selection for UE originating sessions / calls

The behaviour of the UE for domain selection is determined by:

a) the UE usage setting;

b) the availability of IMS voice; and

c) whether the UE operates in single-registration mode or dual-registration mode (see 3GPP TS 23.501 [8]).

In the present document the condition "the UE supports IMS voice over 3GPP access" evaluates to "true" if at least one of the following is fulfilled:

1) the UE supports IMS voice over NR connected to 5GCN;

2) the UE supports IMS voice over E-UTRA connected to 5GCN; or

3) the UE supports IMS voice in EPS.

In the present document the condition "the UE does not support IMS voice over 3GPP access" evaluates to "true" if the condition "the UE supports IMS voice over 3GPP access" evaluates to "false".

In the present document the condition "the UE supports IMS voice over non-3GPP access" evaluates to "true" if the UE supports IMS voice over non-3GPP access connected to 5GCN.

In the present document the condition "the UE does not support IMS voice over non-3GPP access" evaluates to "true" if the condition "the UE supports IMS voice over non-3GPP access" evaluates to "false".

In the present document, "IMS voice not available" is determined per access type independently, i.e. 3GPP access or non-3GPP access.

In the present document, "IMS voice not available" refers to one of the following conditions:

a) the UE does not support IMS voice;

b) the UE supports IMS voice, but the network indicates in the REGISTRATION ACCEPT message that IMS voice over PS sessions are not supported; or

c) the UE supports IMS voice, the network indicates in the REGISTRATION ACCEPT message that IMS voice over PS sessions are supported, but the upper layers:

   1) provide no indication that the UE is available for voice call in the IMS within a manufacturer determined period of time; or

   2) indicate that the UE is not available for voice calls in the IMS.

NOTE 1: If conditions a and b evaluate to false, the upper layers need time to attempt IMS registration. In the event an indication from the upper layers that the UE is available for voice calls in the IMS takes longer than the manufacturer determined period of time (e.g. due to delay when attempting IMS registration or due to delay in obtaining a QoS flow for SIP signalling), the NAS layer assumes the UE is not available for voice calls in the IMS.

Other conditions may exist but these are implementation specific.

In the present document, "IMS voice available" applies when "IMS voice not available" does not apply.

When IMS voice is not available over 3GPP access, if the UE's usage setting is "voice centric", the UE operates in single-registration mode, and the UE:

a) does not have a persistent PDU session, and:

   1) if the UE is only registered over 3GPP access, or if the UE is registered over both 3GPP access and non-3GPP access and IMS voice is not available over non-3GPP access, the UE shall disable the N1 mode capability for 3GPP access and proceed as specified in subclause 4.9.2 with modifications described below; or

   2) if the UE is registered over both 3GPP access and non-3GPP access and IMS voice is available over non-3GPP access, the UE may disable the N1 mode capability for 3GPP access and proceed as specified in subclause 4.9.2 with modifications described below; or

b) has a persistent PDU session, then the UE waits until the radio bearer associated with the persistent PDU session has been released. When the radio bearer associated with the persistent PDU session has been released, then:

   1) if the UE is only registered over 3GPP access, or if the UE is registered over both 3GPP access and non-3GPP access and IMS voice is not available over non-3GPP access,the UE shall disable the N1 mode capability for 3GPP access and proceed as specified in subclause 4.9.2 with modifications described below; or

   2) If the UE is registered over both 3GPP access and non-3GPP access and IMS voice is available over non-3GPP access, the UE may disable the N1 mode capability for 3GPP access and proceed as specified in subclause 4.9.2 with modifications described below.

The following modifications are applied to the procedure in subclause 4.9.2 for disabling the N1 mode capability for 3GPP access, if the UE's usage setting is "voice centric" and the UE operates in single-registration mode:

a) in item a) of subclause 4.9.2, the UE shall attempt to select an E-UTRA cell connected to EPC. If such a cell is found, the UE shall then perform voice domain selection procedures as defined in 3GPP TS 24.301 [15]; and

b) in item b) of subclause 4.9.2, if an E-UTRA cell connected to EPC cannot be found, the UE shall attempt to select another supported radio access technology which supports voice services.

When IMS voice is not available over non-3GPP access, if the UE's usage setting is "voice centric" and the UE operates in single-registration mode, then:

a) if the UE is only registered over non-3GPP access, the UE shall disable the N1 mode capability for non-3GPP access (see subclause 4.9.3); or

b) if the UE is registered over both 3GPP access and non-3GPP access and IMS voice is not available also over 3GPP access, the UE may disable the N1 mode capability for non-3GPP access (see subclause 4.9.3).

NOTE 2: The UE can register over 3GPP access in another mode, e.g., S1 mode, for voice service, and in this case the UE can keep the N1 mode capability for non-3GPP access enabled.

4.3.3 Change of UE's usage setting

If the UE operates in single-registration mode, whenever the UE's usage setting changes, the UE shall execute procedures according to table 4.3.3.1:

Table 4.3.3.1: Change of UE's usage setting for a UE in single-registration mode

UE's usage setting change	Procedure to execute
From "data centric" to "voice centric" and "IMS voice not available" over 3GPP access only	Disable the N1 mode capability for 3GPP access (see subclause 4.9.2), if the UE is only registered over 3GPP access (NOTE)
From "data centric" to "voice centric", and "IMS voice not available" over both 3GPP access and non-3GPP access	Disable the N1 mode capability for 3GPP access (see subclause 4.9.2) and non-3GPP access (see subclause 4.9.3), if the UE is registered over both 3GPP access and non-3GPP access Disable the N1 mode capability for 3GPP access (see subclause 4.9.2), if the UE is only registered over 3GPP access. Disable the N1 mode capability for non-3GPP access (see subclause 4.9.3), if the UE is only registered over non-3GPP access. (NOTE)
From "voice centric" to "data centric" and the N1 mode capability for 3GPP access is disabled at the UE due to "IMS voice not available"	Re-enable the N1 mode capability for 3GPP access (see subclause 4.9.2)
From "data centric" to "voice centric" and "IMS voice not available" over non-3GPP access only	Disable the N1 mode capability for non-3GPP access (see subclause 4.9.3), if the UE is only registered over non-3GPP access
From "voice centric" to "data centric", and the N1 mode capability for non-3GPP access is disabled at the UE due to "IMS voice not available"	Re-enable the N1 mode capability for non-3GPP access (see subclause 4.9.3)
NOTE: If the UE is registered over 3GPP access and has a persistent PDU session, then the UE waits until the radio bearer associated with the persistent PDU session has been released.	

4.3.4 Change or determination of IMS voice availability

If the UE operates in single-registration mode, whenever the IMS voice availability is determined or changes, the UE shall execute procedures according to table 4.3.4.1:

Table 4.3.4.1: Change of IMS voice availability for a UE in single-registration mode

Change of IMS voice available condition	Procedure to execute
"IMS voice not available" over 3GPP access only and the UE's usage setting is "voice centric"	Disable the N1 mode capability for 3GPP access, if the UE is only registered over 3GPP access (see subclause 4.9.2). (NOTE 2)
"IMS voice not available" over non-3GPP access only and the UE's usage setting is "voice centric"	Disable the N1 mode capability for non-3GPP access (see subclause 4.9.3), if the UE is only registered over non-3GPP access. (NOTE 2)
"IMS voice not available" over both 3GPP access and non-3GPP access, and the UE's usage setting is "voice centric"	Disable the N1 mode capability for 3GPP access (see subclause 4.9.2) and non-3GPP access (see subclause 4.9.3), if the UE is registered over both 3GPP access and non-3GPP access. Disable the N1 mode capability for 3GPP access (see subclause 4.9.2), if the UE is only registered over 3GPP access Disable the N1 mode capability for non-3GPP access (see subclause 4.9.3), if the UE is only registered over non-3GPP access. (NOTE 1, NOTE 2)
NOTE 1: If the UE is registered over 3GPP access and has a persistent PDU session, then the UE waits until the radio bearer associated with the persistent PDU session has been released. NOTE 2: If the UE determines "IMS voice not available" upon receipt of a 5GS session management reject message including a back-off timer value, and the re-attempt indicator indicates that the UE is not allowed to re-attempt the procedure in S1 mode then, upon inter-system change from N1 mode to S1 mode, the UE proceeds as specified in 3GPP TS 24.301 [15], subclause 4.3.2.4, Change or determination of IMS registration status.	

4.4 NAS security

4.4.1 General

This clause describes the principles for the handling of 5G NAS security contexts in the UE and in the AMF, the procedures used for the security protection of NAS messages between the UE and the AMF, and the procedures used for the protection of NAS IEs between the UE and the UDM. Security protection involves integrity protection and ciphering of the 5GMM messages. 5GSM messages are security protected indirectly by being piggybacked by the security protected 5GMM messages (i.e. UL NAS TRANSPORT message and the DL NAS TRANSPORT message).

The signalling procedures for the control of NAS security are part of the 5GMM protocol and are described in detail in clause 5.

NOTE: The use of ciphering in a network is an operator option. In this subclause, for the ease of description, it is assumed that ciphering is used, unless explicitly indicated otherwise. Operation of a network without ciphering is achieved by configuring the AMF so that it always selects the "null ciphering algorithm", 5G-EA0.

4.4.2 Handling of 5G NAS security contexts

4.4.2.1 General

4.4.2.1.1 Establishment of 5G NAS security context

The security parameters for authentication, integrity protection and ciphering are tied together in a 5G NAS security context and identified by a key set identifier (ngKSI). The relationship between the security parameters is defined in 3GPP TS 33.501 [24].

Before security can be activated, the AMF and the UE need to establish a 5G NAS security context. Usually, the 5G NAS security context is created as the result of a primary authentication and key agreement procedure between the AMF and the UE. A new 5G NAS security context may also be created during an N1 mode to N1 mode handover. Alternatively, during inter-system change from S1 mode to N1 mode, the AMF not supporting interworking without

N26 and the UE operating in single-registration mode may derive a mapped 5G NAS security context from an EPS security context that has been established while the UE was in S1 mode.

The 5G NAS security context is taken into use by the UE and the AMF, when the AMF initiates a security mode control procedure, during an N1 mode to N1 mode handover, or during the inter-system change procedure from S1 mode to N1 mode. The 5G NAS security context which has been taken into use by the network most recently is called current 5G NAS security context. This current 5G NAS security context can be of type native or mapped, i.e. originating from a native 5G NAS security context or mapped 5G NAS security context.

The key set identifier ngKSI is assigned by the AMF either during the primary authentication and key agreement procedure or, for the mapped 5G NAS security context, during the inter-system change. The ngKSI consists of a value and a type of security context parameter indicating whether a 5G NAS security context is a native 5G NAS security context or a mapped 5G NAS security context. When the 5G NAS security context is a native 5G NAS security context, the ngKSI has the value of KSI_{AMF}, and when the current 5G NAS security context is of type mapped, the ngKSI has the value of KSI_{ASME}.

The 5G NAS security context which is indicated by an ngKSI can be taken into use to establish the secure exchange of NAS messages when a new N1 NAS signalling connection is established without executing a new primary authentication and key agreement procedure (see subclause 5.4.1) or when the AMF initiates a security mode control procedure. For this purpose, the initial NAS messages (i.e. REGISTRATION REQUEST, DEREGISTRATION REQUEST, SERVICE REQUEST and CONTROL PLANE SERVICE REQUEST) and the SECURITY MODE COMMAND message contain an ngKSI in the ngKSI IE indicating the current 5G NAS security context used to integrity protect the NAS message.

In the present document, when the UE is required to delete an ngKSI, the UE shall set the ngKSI to the value "no key is available" and consider also the associated keys K_{AMF} or K'_{AMF}, 5G NAS ciphering key and 5G NAS integrity key invalid (i.e. the 5G NAS security context associated with the ngKSI as no longer valid). In the initial registration procedure, when the key $K_{AUSF,}$ is invalid, the UE shall delete the ngKSI.

NOTE: In some specifications the term ciphering key sequence number might be used instead of the term key set identifier (KSI).

As described in subclause 4.8 in order to interwork with E-UTRAN connected to EPC, the UE supporting both S1 mode and N1 mode can operate in either single-registration mode or dual-registration mode. A UE operating in dual-registration mode shall independently maintain and use both EPS security context (see 3GPP TS 24.301 [15]) and 5G NAS security context. When the UE operating in dual-registration mode performs an EPS attach procedure, it shall take into use an EPS security context and follow the handling of this security context as specified in 3GPP TS 24.301 [15]. However, when the UE operating in dual-registration mode performs an initial registration procedure, it shall take into use a 5G NAS security context and follow the handling of this security context as described in the present specification.

The UE and the AMF need to be able to maintain two 5G NAS security contexts simultaneously, i.e. a current 5G NAS security context and a non-current 5G NAS security context, since:

a) after a 5G re-authentication, the UE and the AMF can have both a current 5G NAS security context and a non-current 5G NAS security context which has not yet been taken into use (i.e. a partial native 5G NAS security context); and

b) after an inter-system change from S1 mode to N1 mode, the UE and the AMF can have both a mapped 5G NAS security context, which is the current 5G NAS security context, and a non-current native 5G NAS security context that was created during a previous access in N1 mode.

The number of 5G NAS security contexts that need to be maintained simultaneously by the UE and the AMF is limited by the following requirements:

a) after a successful 5G (re-)authentication, which creates a new partial native 5G NAS security context, the AMF and the UE shall delete the non-current 5G NAS security context, if any;

b) when a partial native 5G NAS security context is taken into use through a security mode control procedure, the AMF shall delete the previously current 5G NAS security context. If the UE does not support multiple records of NAS security context storage for multiple registration (see 3GPP TS 31.102 [22]), the UE shall delete the previously current 5G NAS security context. If the UE supports multiple records of NAS security context storage for multiple registration, the UE shall:

1) replace the previously current 5G NAS security context stored in the first 5G security context of that access (see 3GPP TS 31.102 [22]) with the new 5G security context (taken into use through a security mode control procedure), when the UE activates the new 5G security context for the same PLMN and access;

1a) replace the previously current 5G NAS security context stored in the first 5G security context of that access (see 3GPP TS 31.102 [22]) with the new 5G security context (taken into use through a security mode control procedure), when the UE activates the new 5G security context for a different PLMN over that access but the previously current 5G NAS security context is not associated with the 5G-GUTI of the other access; or

2) store the previously current 5G NAS security context in the second 5G security context of that access (see 3GPP TS 31.102 [22]) and store the new 5G security context (taken into use through a security mode control procedure) in the first 5G security context, when the UE activates the new 5G security context for a different PLMN over that access but the previously current 5G NAS security context is associated with the 5G-GUTI of the other access;

c) when the AMF and the UE create a 5G NAS security context using "null integrity protection algorithm" and "null ciphering algorithm" during an initial registration procedure for emergency services, or a registration procedure for mobility and periodic registration update for a UE that has an emergency PDU session (see subclause 5.4.2.2), the AMF and the UE shall delete the previous current 5G NAS security context. The UE shall not update the USIM and non-volatile ME memory with the current 5G NAS security context and shall delete the current 5G NAS security context when the UE is deregistered from emergency services (e.g. before registering for normal service);

d) when a new mapped 5G NAS security context or 5G NAS security context created using "null integrity protection algorithm" and "null ciphering algorithm" is taken into use during the inter-system change from S1 mode to N1 mode, the AMF and the UE shall not delete the previously current native 5G NAS security context, if any. Instead, the previously current native 5G NAS security context shall become a non-current native 5G NAS security context, and the AMF and the UE shall delete any partial native 5G NAS security context;

If no previously current native 5G NAS security context exists, the AMF and the UE shall not delete the partial native 5G NAS security context, if any;

e) when the AMF and the UE derive a new mapped 5G NAS security context during inter-system change from S1 mode to N1 mode, the AMF and the UE shall delete any existing current mapped 5G NAS security context;

f) when a non-current full native 5G NAS security context is taken into use by a security mode control procedure, then the AMF and the UE shall delete the previously current mapped 5G NAS security context;

g) when the UE or the AMF moves from 5GMM-REGISTERED to 5GMM-DEREGISTERED state, if the current 5G NAS security context is a mapped 5G NAS security context and a non-current full native 5G NAS security context exists, then the non-current 5G NAS security context shall become the current 5G NAS security context. Furthermore, the UE and the AMF shall delete any mapped 5G NAS security context or partial native 5G NAS security context.

h) when the UE operating in single-registration mode in a network supporting N26 interface performs an inter-system change from N1 mode to S1 mode:

1) if the UE has a mapped 5G NAS security context and the inter-system change is performed in:

i) 5GMM-IDLE mode, the UE shall delete the mapped 5G NAS security context after the successful completion of the tracking area update procedure or attach procedure (see 3GPP TS 24.301 [15]); or

ii) 5GMM-CONNECTED mode, the UE shall delete the mapped 5G NAS security context after the completion of the inter-system change.

After deletion of the mapped 5G NAS security context, if the UE has a non-current full native 5G NAS security context, then the non-current full native 5G NAS security context shall become the current full native 5G NAS security context; and

i) when the UE operating in single-registration mode in a network supporting N26 interface performs an inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, if the UE has a non-current full native 5G NAS security context, then the UE shall make the non-current full native 5G NAS security context as the current native 5G NAS security context. The UE shall delete the mapped 5G NAS security context, if any.

4.4.2.1.2 UE leaving state 5GMM-DEREGISTERED

If the UE is capable of registration over a single access only, the UE shall mark the 5G NAS security context on the USIM or in the non-volatile memory as invalid when the UE initiates an initial registration procedure as described in subclause 5.5.1.2 or when the UE leaves state 5GMM-DEREGISTERED for any other state except 5GMM-NULL.

If the UE is capable of registration over both 3GPP access and non-3GPP access and was last registered on the same PLMN over both 3GPP access and the non-3GPP access, the UE in the state 5GMM-DEREGISTERED over both 3GPP access and non-3GPP access shall mark the 5G NAS security contexts in record 1 of the 3GPP access and the non-3GPP access on the USIM or in the non-volatile memory as invalid when the UE initiates an initial registration procedure over either 3GPP access or non-3GPP access as described in subclause 5.5.1.2 or when the UE leaves state 5GMM-DEREGISTERED for any other state except 5GMM-NULL over either 3GPP access or non-3GPP access.

4.4.2.1.3 UE entering state 5GMM-DEREGISTERED

If the UE is capable of registration over a single access only, the UE shall store the current native 5G NAS security context on the USIM or in the non-volatile memory and mark it as valid only when the UE enters state 5GMM-DEREGISTERED from any other state except 5GMM-NULL or when the UE aborts the initial registration procedure without having left 5GMM-DEREGISTERED.

If the UE is capable of registration over both 3GPP access and non-3GPP access and is registered on the same PLMN over both 3GPP access and the non-3GPP access, the UE shall store the current native 5G NAS security contexts of the 3GPP access and the non-3GPP access as specified in annex C and mark them as valid only when the UE enters state 5GMM-DEREGISTERED from any other state except 5GMM-NULL over both the 3GPP access and non-3GPP access or only when the UE aborts the initial registration procedure without having left 5GMM-DEREGISTERED over both the 3GPP access and non-3GPP access.

4.4.2.2 Establishment of a mapped 5G NAS security context during inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode

In order for the UE operating in single-registration mode in a network supporting N26 interface to derive a mapped 5G NAS security context for an inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, the AMF shall construct a mapped 5G NAS security context from the EPS security context received from the source MME as indicated in 3GPP TS 33.501 [24]. The AMF shall select the 5G NAS security algorithms and derive the 5G NAS keys (i.e. K_{NASenc} and K_{NASint}). The AMF shall define an ngKSI for the newly derived K'_{AMF} key such that the value field is taken from the eKSI of the K_{ASME} key and the type field is set to indicate a mapped security context and associate this ngKSI with the newly created mapped 5G NAS security context. The AMF shall then include the message authentication code, selected NAS algorithms, NCC and generated ngKSI in the S1 mode to N1 mode NAS transparent container IE (see subclause 9.11.2.9).

When the UE operating in single-registration mode in a network supporting N26 interface receives the command to perform inter-system change to N1 mode in 5GMM-CONNECTED mode, the UE shall derive a mapped $K'_{AMF,}$ as indicated in 3GPP TS 33.501 [24], using the K_{ASME} from the EPS security context. Furthermore, the UE shall also derive the 5G NAS keys from the mapped K'_{AMF} using the selected NAS algorithm identifiers included in the S1 mode to N1 mode NAS transparent container IE and associate this mapped 5G NAS security context with the ngKSI value received. The UE shall then verify the received NAS MAC. In case the received NAS MAC is not verified successfully (see subclause 4.4.3.3) the UE shall discard the content of the received S1 mode to N1 mode NAS transparent container IE and inform the lower layers that the received S1 mode to N1 mode NAS transparent container is invalid.

When the UE operating in single-registration mode in a network supporting N26 interface has a PDN connection for emergency bearer services and has no current EPS security context, the AMF shall set 5G-IA0 and 5G-EA0 as the selected 5G NAS security algorithms in the S1 mode to N1 mode NAS transparent container IE. The AMF shall create a locally generated K'_{AMF}. The AMF shall set the ngKSI value of the associated security context to "000" and the type of security context flag to "mapped security context" in the S1 mode to N1 mode NAS transparent container IE.

When the UE operating in single-registration mode in a network supporting N26 interface receives the command to perform inter-system change to N1 mode in 5GMM-CONNECTED mode (see 3GPP TS 38.331 [30]) and has a PDN connection for emergency bearer services, if 5G-IA0 and 5G-EA0 as the selected 5G NAS security algorithms are included in the S1 mode to N1 mode NAS transparent container IE, the UE shall create a locally generated K'_{AMF}. Furthermore, the UE shall set the ngKSI value of the associated security context to the KSI value received.

After the new mapped 5G NAS security context is taken into use for the 3GPP access following a successful inter system change from S1 mode to N1 mode in 5GMM-CONNECTED mode and the UE is registered with the same PLMN over the 3GPP access and non-3GPP access:

a) if a native 5G NAS security context is used on the non-3GPP access and:

   1) the UE is in 5GMM-IDLE mode over non-3GPP access, then the AMF and the UE shall activate and take into use the new mapped 5G NAS security context on the 3GPP access for the non-3GPP access as described in 3GPP TS 33.501 [24] after the AMF sends or the UE receives the REGISTRATION ACCEPT message respectively. The UE and AMF shall keep the native 5G NAS security context which was used on the non-3GPP access and make it a non-current native 5G NAS security context. The non-current native 5G NAS security context may be re-activated later using the security mode control procedure; or

   2) the UE is in 5GMM-CONNECTED mode over non-3GPP access, in order to activate the native 5G NAS security context over the 3GPP access that is active on the non-3GPP access the AMF shall send the SECURITY MODE COMMAND message over the 3GPP access as described in 3GPP TS 33.501 [24]. The SECURITY MODE COMMAND message shall include the same ngKSI to identify the native 5G NAS security context that is used on the non-3GPP access; or

b) if a mapped 5G NAS security context is used on the non-3GPP access and:

   1) the UE is in 5GMM-IDLE mode over non-3GPP access, the AMF and the UE shall activate and take into use the new mapped 5G NAS security context active on the 3GPP access for the non-3GPP access as described in 3GPP TS 33.501 [24] after the AMF sends or the UE receives the REGISTRATION ACCEPT message respectively; or

   2) the UE is in 5GMM-CONNECTED mode over non-3GPP access, in order to activate the same mapped 5G NAS security context over one access that is used on the other access the AMF shall send the SECURITY MODE COMMAND message over one-access as described in 3GPP TS 33.501 [24]. The SECURITY MODE COMMAND message shall include the same ngKSI to identify the mapped 5G NAS security context that is used over the other access.

If the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode is not completed successfully, the AMF and the UE operating in single-registration mode in a network supporting N26 interface shall delete the new mapped 5G NAS security context.

4.4.2.3 Establishment of a 5G NAS security context during N1 mode to N1 mode handover

During an N1 mode to N1 mode handover, the target AMF may derive a new 5G NAS security context for which the target AMF creates a new 5G NAS security context as indicated in 3GPP TS 33.501 [24].

When a new 5G NAS security context is derived using the same K_{AMF}, the target AMF includes the 8 least significant bits of the downlink NAS COUNT in the Intra N1 mode NAS transparent container IE, and indicates that a new K_{AMF} shall not be derived (see subclause 9.11.2.6). The AMF shall increment the downlink NAS COUNT by one after creating the Intra N1 mode NAS transparent container IE.

When a new 5G NAS security context is created from a new K_{AMF}, the target AMF includes the 8 least significant bits of the downlink NAS COUNT in the Intra N1 mode NAS transparent container IE and indicates that a new K_{AMF} shall be derived (see subclause 9.11.2.6). The AMF shall then set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero. The AMF shall increment the downlink NAS COUNT by one after creating the Intra N1 mode NAS transparent container IE.

The target AMF also includes the ngKSI with the same value as the ngKSI currently being used with the UE, the message authentication code, and the selected NAS algorithms in the Intra N1 mode NAS transparent container IE.

When the UE receives a command to perform handover to NG-RAN including an Intra N1 mode NAS transparent container IE (see subclause 9.11.2.6), the UE derives a new 5G NAS security context as described in 3GPP TS 33.501 [24]. When the Intra N1 mode NAS transparent container IE indicates that a new K_{AMF} needs to be derived, the UE shall set both the downlink NAS COUNT and uplink NAS COUNT to zero after creating the new 5G NAS security context.

If the received Intra N1 mode NAS transparent container IE does not have a valid NAS COUNT (see subclause 4.4.3.2) or the received NAS MAC is not verified successfully (see subclause 4.4.3.3) the UE shall discard the content of the

received Intra N1 mode NAS transparent container IE, continue to use the current 5G NAS security context, and inform the lower layers that the received Intra N1 mode NAS transparent container is invalid.

NOTE 1: During N1 mode to N1 mode handover, the Intra N1 mode NAS transparent container IE (see subclause 9.11.2.6) is equivalent to sending a SECURITY MODE COMMAND message to the UE in order to derive and use a new 5G NAS security context, optionally created with a new K_{AMF}. The UE maintains the Selected EPS NAS security algorithms until the UE receives a new Selected EPS NAS security algorithms.

After the new 5G NAS security context is taken into use for 3GPP access following a successful N1 mode to N1 mode handover and the UE is registered with the same PLMN over the 3GPP access and non-3GPP access:

a) the UE is in 5GMM-IDLE mode over non-3GPP access, the AMF and the UE shall activate and take into use the new 5G NAS security context over the non-3GPP access as described in 3GPP TS 33.501 [24] after the AMF sends or the UE receives the REGISTRATION ACCEPT message respectively. If the new 5G NAS security context is created from a new K_{AMF}, the AMF and the UE shall set the downlink NAS COUNT and uplink NAS COUNT to zero also for the non-3GPP access, otherwise the downlink NAS COUNT and uplink NAS COUNT for the non-3GPP access are not changed; or

b) the UE is in 5GMM-CONNECTED mode over non-3GPP access, in order to activate the new 5G NAS security context over the non-3GPP access that has been activated for the 3GPP access the AMF shall send the SECURITY MODE COMMAND message over the non-3GPP access as described in 3GPP TS 33.501 [24]. The SECURITY MODE COMMAND message shall include the same ngKSI to identify the new 5G NAS security context that was activated over the 3GPP access and shall include the horizontal derivation parameter indicating "K_{AMF} derivation is not required". Otherwise, if the new 5G NAS security context is created from a new K_{AMF}, the AMF and the UE shall set the downlink NAS COUNT and uplink NAS COUNT to zero for the non-3GPP access.

NOTE 2: Explicit indication "K_{AMF} derivation is not required" for the non-3GPP access is to align security contexts within the UE without a subsequent derivation of a new K_{AMF} in the non-3GPP access.

4.4.2.4 Establishment of an EPS security context during inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode

In order for the UE operating in single-registration mode in a network supporting N26 interface to derive a mapped EPS security context for an inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode, the AMF shall prepare a mapped EPS security context for the target MME as indicated in 3GPP TS 33.501 [24].

The AMF shall derive a K'_{ASME} using the K_{AMF} key and the downlink NAS COUNT of the current 5G NAS security context, include the corresponding NAS sequence number in the N1 mode to S1 mode NAS transparent container IE (see subclause 9.11.2.7) and then increments its stored downlink NAS COUNT value by one.

NOTE: The creation of the N1 mode to S1 mode NAS transparent container and the increment of the stored downlink NAS COUNT value by one are performed in prior to transferring the mapped EPS security context to the MME.

The AMF shall select the NAS algorithms identifiers to be used in the target MME after the inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode, for encryption and integrity protection. The uplink and downlink NAS COUNT associated with the newly derived K'_{ASME} key are set to the uplink and downlink NAS COUNT value of the current 5G NAS security context, respectively. The eKSI for the newly derived K'_{ASME} key shall be defined such as the value field is taken from the ngKSI and the type field is set to indicate a mapped security context.

When the UE operating in single-registration mode in a network supporting N26 interface receives a command to perform inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode, the UE shall derive the mapped EPS security context, i.e. derive K'_{ASME} from K_{AMF} using a downlink NAS COUNT based on the NAS sequence number received in the N1 mode to S1 mode NAS transparent container IE (see subclause 9.11.2.7) as described in 3GPP TS 33.501 [24]. The UE shall set the uplink and downlink NAS COUNT values associated with the newly derived K'_{ASME} key to the uplink and downlink NAS COUNT values of the current 5G NAS security context respectively. The eKSI for the newly derived K'_{ASME} key is defined such that the value field is taken from the ngKSI and the type field is set to indicate a mapped security context. The UE shall also derive the NAS keys as specified in 3GPP TS 33.401 [23A] using the EPS NAS security algorithms identifiers that are stored in the UE's 5G NAS security context.

If the received N1 mode to S1 mode NAS transparent container IE does not have a valid NAS COUNT (see subclause 4.4.3.2) the UE shall discard the content of the received N1 mode to S1 mode NAS transparent container IE and inform the lower layers that the received N1 mode to S1 mode NAS transparent container is invalid.

If the inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode is not completed successfully, the AMF and the UE shall delete the new mapped EPS security context.

4.4.2.5 Establishment of secure exchange of NAS messages

Secure exchange of NAS messages via a NAS signalling connection is usually established by the AMF during the registration procedure by initiating a security mode control procedure. After successful completion of the security mode control procedure, all NAS messages exchanged between the UE and the AMF are sent integrity protected using the current 5G security algorithms, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered using the current 5G security algorithms.

During inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, secure exchange of NAS messages is established between the AMF and the UE by:

a) the transmission of NAS security related parameters encapsulated in the AS signalling from the AMF to the UE triggering the inter-system change in 5GMM-CONNECTED mode (see 3GPP TS 33.501 [24]). The UE uses these parameters to generate the mapped 5G NAS security context (see subclause 8.6.2 of 3GPP TS 33.501 [24]); and

b) after the inter-system change in 5GMM-CONNECTED mode, the transmission of a REGISTRATION REQUEST message from the UE to the AMF. The UE shall send this message integrity protected using the mapped 5G NAS security context and further protect this message as specified in subclause 4.4.6 and subclause 5.5.1.3.2. After the AMF receives the REGISTRATION REQUEST message:

   1) if the AMF decides to take the native 5G NAS security context into use, the security mode control procedure is performed. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected using the native 5G NAS security context, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered using the native 5G NAS security context; or

   2) if the AMF decides to take the mapped 5G NAS security context into use, from this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected using the mapped 5G NAS security context, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered using the mapped 5G NAS security context.

During inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, if the UE is operating in single-registration mode and:

a) if the UE has a valid native 5G NAS security context, the UE shall transmit a REGISTRATION REQUEST message integrity protected with the native 5G NAS security context. The UE shall include the ngKSI indicating the native 5G NAS security context value in the REGISTRATION REQUEST message.

   After receiving the REGISTRATION REQUEST message including the ngKSI indicating a native 5G NAS security context value, the AMF shall check whether the ngKSI included in the REGISTRATION REQUEST message belongs to a 5G NAS security context available in the AMF, and shall verify the MAC of the REGISTRATION REQUEST message. If the verification is successful, the AMF deletes the EPS security context received from the source MME if any, and the AMF re-establishes the secure exchange of NAS messages by either:

   1) replying with a REGISTRATION ACCEPT message that is integrity protected and ciphered using the native 5G NAS security context. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered; or

   2) initiating a security mode control procedure. This can be used by the AMF to take a non-current 5G NAS security context into use or to modify the current 5G NAS security context by selecting new NAS security algorithms.

b) if the UE has no valid native 5G NAS security context, the UE shall send the REGISTRATION REQUEST message without integrity protection and encryption.

After receiving the REGISTRATION REQUEST message without integrity protection and encryption:

1) if N26 interface is supported:

   i) if an EPS security context received from the source MME does not include the NAS security algorithms set to EIA0 and EEA0, the AMF shall either create a fresh mapped 5G NAS security context (see subclause 8.6.2 of 3GPP TS 33.501 [24]) or trigger a primary authentication and key agreement procedure to create a fresh native 5G NAS security context; or

   ii) if an EPS security context received from the source MME includes the NAS security algorithms set to EIA0 and EEA0, the AMF shall trigger a primary authentication and key agreement procedure to create a fresh native 5G NAS security context; or

2) if N26 interface is not supported, the AMF shall trigger a primary authentication and key agreement procedure.

The newly created 5G NAS security context is taken into use by initiating a security mode control procedure and this context becomes the current 5G NAS security context in both the UE and the AMF. This re-establishes the secure exchange of NAS messages.

During an N1 mode to N1 mode handover, secure exchange of NAS messages is established between the AMF and the UE by:

- the transmission of NAS security related parameters encapsulated in the AS signalling from the target AMF to the UE triggering the N1 mode to N1 mode handover (see 3GPP TS 33.501 [24]). The UE uses these parameters to create a new 5G NAS security context.

The secure exchange of NAS messages shall be continued after N1 mode to N1 mode handover. It is terminated after inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode or when the NAS signalling connection is released.

When a UE in 5GMM-IDLE mode establishes a new NAS signalling connection and has a valid current 5G NAS security context, the UE shall transmit the initial NAS message integrity protected with the current 5G NAS security context and further protect this message as specified in subclause 4.4.6. The UE shall include the ngKSI indicating the current 5G NAS security context value in the initial NAS message. The AMF shall check whether the ngKSI included in the initial NAS message belongs to a 5G NAS security context available in the AMF, and shall verify the MAC of the NAS message. If the verification is successful, the AMF may re-establish the secure exchange of NAS messages:

a) by replying with a NAS message that is integrity protected and ciphered using the current 5G NAS security context. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered; or

b) by initiating a security mode control procedure. This can be used by the AMF to take a non-current 5G NAS security context into use or to modify the current 5G NAS security context by selecting new NAS security algorithms.

When a UE attempts multiple registrations in the same or different serving network, both the AMF and the UE shall follow the behavior specified in subclause 6.3.2 of 3GPP TS 33.501 [24]. The UE may support multiple records of NAS security context storage for multiple registration (see 3GPP TS 31.102 [22]). If the UE supports multiple records of NAS security context storage for multiple registration, the UE can select the appropriate one among the stored 5G security contexts to protect the initial NAS message (see 3GPP TS 33.501 [24]).

NOTE: For the case when the UE has two records of NAS security context stored and is attempting registration to the PLMN associated with the 5G-GUTI (or an equivalent PLMN) for that access, the UE uses the first NAS security context of that access to protect the initial NAS message. For the case when the UE has two records of NAS security context stored and is attempting registration to the PLMN associated with the second record (or an equivalent PLMN) of that access, the UE uses the second NAS security context of that access to protect the initial NAS message. For other cases when the UE has two records of NAS security context stored and is attempting registration to a PLMN which is not associated with any NAS security context record, the UE uses either record of the NAS security context of that access to protect the initial NAS message.

4.4.2.6 Change of security keys

When the AMF initiates a re-authentication to create a new 5G NAS security context, the messages exchanged during the authentication procedure are integrity protected and ciphered using the current 5G NAS security context, if any.

Both UE and AMF shall continue to use the current 5G NAS security context, until the AMF initiates a security mode control procedure. The SECURITY MODE COMMAND message sent by the AMF includes the ngKSI of the new 5G NAS security context to be used. The AMF shall send the SECURITY MODE COMMAND message integrity protected with the new 5G NAS security context, but unciphered. When the UE responds with a SECURITY MODE COMPLETE message, it shall send the message integrity protected and ciphered with the new 5G NAS security context.

The AMF can also modify the current 5G NAS security context or take the non-current native 5G NAS security context, if any, into use, by sending a SECURITY MODE COMMAND message including the ngKSI of the 5G NAS security context to be modified and including a new set of selected NAS security algorithms. In this case the AMF shall send the SECURITY MODE COMMAND message integrity protected with the modified 5G NAS security context, but unciphered. When the UE replies with a SECURITY MODE COMPLETE message, it shall send the message integrity protected and ciphered with the modified 5G NAS security context.

4.4.3 Handling of NAS COUNT and NAS sequence number

4.4.3.1 General

Each 5G NAS security context shall be associated with two separate counters NAS COUNT per access type in the same PLMN: one related to uplink NAS messages and one related to downlink NAS messages. If the 5G NAS security context is used for access via both 3GPP and non-3GPP access in the same PLMN, there are two NAS COUNT counter pairs associated with the 5G NAS security context. The NAS COUNT counters use 24-bit internal representation and are independently maintained by UE and AMF. The NAS COUNT shall be constructed as a NAS sequence number (8 least significant bits) concatenated with a NAS overflow counter (16 most significant bits).

When NAS COUNT is input to NAS ciphering or NAS integrity algorithms it shall be considered to be a 32-bit entity which shall be constructed by padding the 24-bit internal representation with 8 zeros in the most significant bits.

The value of the uplink NAS COUNT that is stored or read out of the USIM or non-volatile memory as described in annex C, is the value that shall be used in the next NAS message.

The value of the downlink NAS COUNT that is stored or read out of the USIM or non-volatile memory as described in annex C, is the largest downlink NAS COUNT used in a successfully integrity checked NAS message.

The value of the uplink NAS COUNT stored in the AMF is the largest uplink NAS COUNT used in a successfully integrity checked NAS message.

The value of the downlink NAS COUNT stored in the AMF is the value that shall be used in the next NAS message.

The NAS sequence number part of the NAS COUNT shall be exchanged between the UE and the AMF as part of the NAS signalling. After each new or retransmitted outbound SECURITY PROTECTED 5GS NAS MESSAGE message, the sender shall increase the NAS COUNT number by one, except for the initial NAS messages if the lower layers indicated the failure to establish the RRC connection (see 3GPP TS 38.331 [30]). Specifically, on the sender side, the NAS sequence number shall be increased by one, and if the result is zero (due to wrap around), the stored NAS overflow counter shall also be incremented by one (see subclause 4.4.3.5). If, through implementation-dependent means, the receiver determines that the NAS message is a replay of an earlier NAS message, then the receiver handles the received NAS message as described in subclause 4.4.3.2. Otherwise, in order to determine the estimated NAS COUNT value to be used for integrity verification of a received NAS message:

- The sequence number part of the estimated NAS COUNT value shall be equal to the sequence number in the received NAS message; and

- If the receiver can guarantee that this NAS message was not previously accepted, then the receiver may select the estimated NAS overflow counter so that the estimated NAS COUNT value is lower than the stored NAS COUNT value; otherwise, the receiver selects the estimated NAS overflow counter so that the estimated NAS COUNT value is higher than the stored NAS COUNT value.

During the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, when a mapped 5G NAS security context is derived and taken into use, the AMF shall set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero. The UE shall set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero.

During the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, the AMF shall increment the downlink NAS COUNT by one after it has created an S1 mode to N1 mode NAS transparent container (see subclause 9.11.2.9).

During the inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode, the AMF shall increment the downlink NAS COUNT by one after it has created an N1 mode to S1 mode NAS transparent container (see subclause 9.11.2.7).

During N1 mode to N1 mode handover:

a) if the new 5G NAS security context is created with the same K_{AMF}, the AMF shall signal the 8 least significant bits of the current downlink NAS COUNT value in an Intra N1 mode NAS transparent container (see subclause 9.11.2.6). The AMF shall then increment the downlink NAS COUNT by one; or

b) if the new 5G NAS security context is created with a new K_{AMF}, the AMF shall signal the 8 least significant bits of the current downlink NAS COUNT value in an Intra N1 mode NAS transparent container (see subclause 9.11.2.6) and shall then set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero. The AMF shall then increment the downlink NAS COUNT by one. The UE shall also set both the uplink and downlink NAS COUNT counters to zero.

NOTE: During the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, the S1 mode to N1 mode NAS transparent container (see subclause 9.11.2.9) is treated as an implicit SECURITY MODE COMMAND message for the UE and the AMF, and therefore the AMF regards the sending of the S1 mode to N1 mode NAS transparent container as the sending of an initial SECURITY MODE COMMAND message in order to derive and take into use a mapped 5G NAS security context for the purpose of the NAS COUNT handling.

4.4.3.2 Replay protection

Replay protection shall be supported for received NAS messages both in the AMF and the UE. However, since the realization of replay protection does not affect the interoperability between nodes, no specific mechanism is required for implementation.

Replay protection assures that one and the same NAS message is not accepted twice by the receiver. Specifically, for a given 5G NAS security context, a given NAS COUNT value shall be accepted at most one time and only if message integrity verifies correctly.

Replay protection is not applicable when 5G-IA0 is used.

4.4.3.3 Integrity protection and verification

The sender shall use its locally stored NAS COUNT as input to the integrity protection algorithm.

The receiver shall use the NAS sequence number included in the received message and an estimate for the NAS overflow counter as defined in subclause 4.4.3.1 to form the NAS COUNT input to the integrity verification algorithm.

The algorithm to calculate the integrity protection information is specified in 3GPP TS 33.501 [24], and in case of the:

a) SECURITY PROTECTED 5GS NAS MESSAGE message, the integrity protection shall include octet 7 to n, i.e. the Sequence number IE and the NAS message IE.

b) Intra N1 mode NAS transparent container IE and S1 mode to N1 mode NAS transparent container IE, the integrity protection shall include all octets of the value part of the IE starting from octet 7.

NOTE: To ensure backward compatibility, the UE uses all octets starting from octet 7 in the received NAS transparent container for the purpose of integrity check of the NAS transparent container irrespective of the release/version it supports. After a successful integrity check, the UE can ignore the octets which are not specified in the release/version which the UE supports.

In addition to the data that is to be integrity protected, the BEARER ID, DIRECTION bit, NAS COUNT and 5G NAS integrity key are input to the integrity protection algorithm. These parameters are described in 3GPP TS 33.501 [24].

After successful integrity protection validation, the receiver shall update its corresponding locally stored NAS COUNT with the value of the estimated NAS COUNT for this NAS message.

Integrity verification is not applicable when 5G-IA0 is used.

4.4.3.4 Ciphering and deciphering

The sender shall use its locally stored NAS COUNT as input to the ciphering algorithm.

The receiver shall use the NAS sequence number included in the received message and an estimate for the NAS overflow counter as defined in subclause 4.4.3.1 to form the NAS COUNT input to the deciphering algorithm.

The input parameters to the NAS ciphering algorithm are the BEARER ID, DIRECTION bit, NAS COUNT, NAS encryption key and the length of the key stream to be generated by the encryption algorithm.

When applying initial NAS message protection to the REGISTRATION REQUEST, DEREGISTRATION REQUEST or SERVICE REQUEST message as described in subclause 4.4.6, the length of the key stream is set to the length of the entire plain NAS message that is included in the NAS message container IE, i.e. the value part of the NAS message container IE, that is to be ciphered.

When applying initial NAS message protection to the CONTROL PLANE SERVICE REQUEST message as described in subclause 4.4.6, the length of the key stream is set to the length of:

a) the value part of the CIoT small data container IE that is to be ciphered; or

b) the value part of the NAS message container IE that is to be ciphered.

4.4.3.5 NAS COUNT wrap around

If, when increasing the NAS COUNT as specified above, the AMF detects that either its downlink NAS COUNT or the UE's uplink NAS COUNT is "close" to wrap around, (close to 2^{24}), the AMF shall take the following actions:

- If there is no non-current native 5G NAS security context with sufficiently low NAS COUNT values, the AMF shall initiate a new primary authentication and key agreement procedure with the UE, leading to a new established 5G NAS security context and the NAS COUNT being reset to 0 in both the UE and the AMF when the new 5G NAS security context is activated;

- Otherwise, the AMF can activate a non-current native 5G NAS security context with sufficiently low NAS COUNT values or initiate a new primary authentication and key agreement procedure as specified above.

If for some reason a new K_{AMF} has not been established using primary authentication and key agreement procedure before the NAS COUNT wraps around, the node (AMF or UE) in need of sending a NAS message shall instead release the NAS signalling connection. Prior to sending the next uplink NAS message, the UE shall delete the ngKSI indicating the current 5G NAS security context.

When the 5G-IA0 is used as the NAS integrity algorithm, the UE and the AMF shall allow NAS COUNT wrap around. If NAS COUNT wrap around occurs, the following requirements apply:

a) the UE and the AMF shall continue to use the current 5G NAS security context;

b) the AMF shall not initiate the primary authentication and key agreement procedure;

c) the AMF shall not release the NAS signalling connection; and

d) the UE shall not perform a local release of the NAS signalling connection.

4.4.4 Integrity protection of NAS signalling messages

4.4.4.1 General

For the UE, integrity protected signalling is mandatory for the 5GMM NAS messages once a valid 5G NAS security context exists and has been taken into use. For the network, integrity protected signalling is mandatory for the 5GMM NAS messages once a secure exchange of 5GS NAS messages has been established for the NAS signalling connection. Integrity protection of all NAS signalling messages is the responsibility of the NAS. It is the network which activates integrity protection.

The use of "null integrity protection algorithm" 5G-IA0 (see subclause 9.11.3.34) in the current 5G NAS security context is only allowed:

a) for an unauthenticated UE for which establishment of emergency services is allowed;

b) for a W-AGF acting on behalf of an FN-RG;

c) for a W-AGF acting on behalf of an N5GC device; and

d) for a 5G-RG acting on behalf of an AUN3 device.

For setting the security header type in outbound NAS messages, the UE and the AMF shall apply the same rules irrespective of whether the "null integrity protection algorithm" or any other integrity protection algorithm is indicated in the 5G NAS security context.

If the "null integrity protection algorithm"5G-IA0 has been selected as an integrity protection algorithm, the receiver shall regard the NAS messages with the security header indicating integrity protection as integrity protected.

Details of the integrity protection and verification of NAS signalling messages are specified in 3GPP TS 33.501 [24].

When a NAS message needs to be sent both ciphered and integrity protected, the NAS message is first ciphered and then the ciphered NAS message and the NAS sequence number are integrity protected by calculating the MAC.

NOTE: NAS messages that are ciphered with the "null ciphering algorithm" 5G-EA0 are regarded as ciphered (see subclause 4.4.5).

When a NAS message needs to be sent only integrity protected and unciphered, the unciphered NAS message and the NAS sequence number are integrity protected by calculating the MAC.

When a 5GSM message is piggybacked in a 5GMM message, there is only one Sequence number IE and one Message authentication code IE for the 5GMM message piggybacking the 5GSM message.

4.4.4.2 Integrity checking of NAS signalling messages in the UE

Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the UE or forwarded to the 5GSM entity, unless the network has established secure exchange of 5GS NAS messages for the NAS signalling connection:

a) IDENTITY REQUEST (if requested identification parameter is SUCI);

b) AUTHENTICATION REQUEST;

c) AUTHENTICATION RESULT;

d) AUTHENTICATION REJECT;

e) REGISTRATION REJECT (if the 5GMM cause is not #76, #78, #81 or #82);

f) DEREGISTRATION ACCEPT (for non switch off); and

g) SERVICE REJECT (if the 5GMM cause is not #76 or #78).

NOTE: These messages are accepted by the UE without integrity protection, as in certain situations they are sent by the network before security can be activated.

Integrity protection is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

Once the secure exchange of NAS messages has been established, the receiving 5GMM entity in the UE shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS. If NAS signalling messages, having not successfully passed the integrity check, are received, then the NAS in the UE shall discard that message. The processing of the SECURITY MODE COMMAND message that has not successfully passed the integrity check is specified in subclause 5.4.2.5. If any NAS signalling message is received as not integrity protected even though the secure exchange of NAS messages has been established by the network, then the NAS shall discard this message.

4.4.4.3 Integrity checking of NAS signalling messages in the AMF

Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the AMF or forwarded to the 5GSM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

a) REGISTRATION REQUEST;

b) IDENTITY RESPONSE (if requested identification parameter is SUCI);

c) AUTHENTICATION RESPONSE;

d) AUTHENTICATION FAILURE;

e) SECURITY MODE REJECT;

f) DEREGISTRATION REQUEST; and

g) DEREGISTRATION ACCEPT;

NOTE 1: The REGISTRATION REQUEST message is sent by the UE without integrity protection, if the registration procedure is initiated due to an inter-system change in 5GMM-IDLE mode and no current 5G NAS security context is available in the UE. The other messages are accepted by the AMF without integrity protection, as in certain situations they are sent by the UE before security can be activated.

NOTE 2: The DEREGISTRATION REQUEST message can be sent by the UE without integrity protection, e.g. if the UE is registered for emergency services and there is no valid 5G NAS security context available, or if due to user interaction a registration procedure is cancelled before the secure exchange of NAS messages has been established. For these cases the network can attempt to use additional criteria (e.g. whether the UE is subsequently still performing periodic registration update or still responding to paging) before marking the UE as 5GMM-DEREGISTERED.

Integrity protection is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

Once a current 5G NAS security context exists, until the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving 5GMM entity in the AMF shall process the following NAS signalling messages, even if the MAC included in the message fails the integrity check or cannot be verified, as the 5G NAS security context is not available in the network:

a) REGISTRATION REQUEST;

b) IDENTITY RESPONSE (if requested identification parameter is SUCI);

c) AUTHENTICATION RESPONSE;

d) AUTHENTICATION FAILURE;

e) SECURITY MODE REJECT;

f) DEREGISTRATION REQUEST;

g) DEREGISTRATION ACCEPT;

h) SERVICE REQUEST; and

i) CONTROL PLANE SERVICE REQUEST;

NOTE 3: These messages are processed by the AMF even when the MAC that fails the integrity check or cannot be verified, as in certain situations they can be sent by the UE protected with a 5G NAS security context that is no longer available in the network.

If a REGISTRATION REQUEST message for initial registration fails the integrity check and it is not a registration request for emergency services, the AMF shall authenticate the subscriber before processing the registration request any further. Additionally, the AMF shall initiate a security mode control procedure, and include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. If authentication procedure is not successful the AMF shall maintain, if any, the 5GMM-context and 5G NAS security context unchanged.For the case when the registration procedure is for emergency services see subclause 5.5.1.2.3 and subclause 5.4.1.3.5.

If a REGISTRATION REQUEST message for mobility and periodic registration update fails the integrity check and the UE provided EPS NAS message container IE which was successfully verified by the source MME, the AMF may create a mapped 5G NAS security context and initiate a security mode control procedure to take the new mapped 5G NAS security context into use; otherwise if the UE has only a non-emergency PDU session established, the AMF shall initiate a primary authentication and key agreement procedure to create a new native 5G NAS security context. Additionally, the AMF shall initiate a security mode control procedure, and include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. If authentication procedure is not successful the AMF shall maintain, if any, the 5GMM-context and 5G NAS security context unchanged. For the case when the UE has an emergency PDU session see subclause 5.5.1.3.3 and subclause 5.4.1.3.5.

If a DEREGISTRATION REQUEST message fails the integrity check, the AMF shall proceed as follows:

- If it is not a deregistration request due to switch off, and the AMF can initiate an authentication procedure, the AMF should authenticate the subscriber before processing the deregistration request any further.

- If it is a deregistration request due to switch off, or the AMF does not initiate an authentication procedure for any other reason, the AMF may ignore the deregistration request and remain in state 5GMM-REGISTERED.

NOTE 4: The network can attempt to use additional criteria (e.g. whether the UE is subsequently still performing periodic registration update or still responding to paging) before marking the UE as 5GMM-DEREGISTERED.

If a SERVICE REQUEST or CONTROL PLANE SERVICE REQUEST message fails the integrity check and the UE has only non-emergency PDU sessions established, the AMF shall send the SERVICE REJECT message with 5GMM cause #9 "UE identity cannot be derived by the network" and keep the 5GMM-context and 5G NAS security context unchanged. For the case when the UE has an emergency PDU session and integrity check fails, the AMF may skip the authentication procedure even if no 5G NAS security context is available and proceed directly to the execution of the security mode control procedure as specified in subclause 5.4.2. Additionally, the AMF shall include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. After successful completion of the service request procedure, the network shall perform a local release of all non-emergency PDU sessions. The emergency PDU session shall not be released.

Once the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving 5GMM entity in the AMF shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS. If any NAS signalling message, having not successfully passed the integrity check, is received, then the NAS in the AMF shall discard that message. If any NAS signalling message is received, as not integrity protected even though the secure exchange of NAS messages has been established, then the NAS shall discard this message.

4.4.5 Ciphering of NAS signalling messages

The use of ciphering in a network is an operator option subject to AMF configuration. When operation of the network without ciphering is configured, the AMF shall indicate the use of "null ciphering algorithm" 5G-EA0 (see subclause 9.11.3.34) in the current 5G NAS security context for all UEs. For setting the security header type in outbound NAS messages, the UE and the AMF shall apply the same rules irrespective of whether the "null ciphering algorithm" or any other ciphering algorithm is indicated in the 5G NAS security context.

When the UE establishes a new N1 NAS signalling connection, it shall apply security protection to the initial NAS message as described in subclause 4.4.6.

The UE shall start the ciphering and deciphering of NAS messages when the secure exchange of NAS messages has been established for an N1 NAS signalling connection. From this time onward, unless explicitly defined, the UE shall send all NAS messages ciphered until the N1 NAS signalling connection is released, or the UE performs inter-system change to S1 mode.

The AMF shall start ciphering and deciphering of NAS messages as described in subclause 4.4.2.5. From this time onward, except for the SECURITY MODE COMMAND message, the AMF shall send all NAS messages ciphered until the N1 NAS signalling connection is released, or the UE performs inter-system change to S1 mode.

Ciphering is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

Once the encryption of NAS messages has been started between the AMF and the UE, the receiver shall discard the unciphered NAS messages which shall have been ciphered according to the rules described in this specification.

If the "null ciphering algorithm" 5G-EA0 has been selected as a ciphering algorithm, the NAS messages with the security header indicating ciphering are regarded as ciphered.

Details of ciphering and deciphering of NAS signalling messages are specified in 3GPP TS 33.501 [24].

4.4.6 Protection of initial NAS signalling messages

The 5GS supports protection of initial NAS messages as specified in 3GPP TS 33.501 [24]. The protection of initial NAS messages applies to the REGISTRATION REQUEST, DEREGISTRATION REQUEST, SERVICE REQUEST and CONTROL PLANE SERVICE REQUEST message, and is achieved as follows:

a) If the UE does not have a valid 5G NAS security context, the UE sends a REGISTRATION REQUEST message including cleartext IEs only. After activating a 5G NAS security context resulting from a security mode control procedure:

   1) if the UE needs to send non-cleartext IEs, the UE shall include the entire REGISTRATION REQUEST message (i.e. containing both cleartext IEs and non-cleartext IEs) in the NAS message container IE and shall include the NAS message container IE in the SECURITY MODE COMPLETE message; or

   2) if the UE does not need to send non-cleartext IEs, the UE shall include the entire REGISTRATION REQUEST message (i.e. containing cleartext IEs only) in the NAS message container IE and shall include the NAS message container IE in the SECURITY MODE COMPLETE message.

b) If the UE has a valid 5G NAS security context and:

   1) the UE needs to send non-cleartext IEs in a REGISTRATION REQUEST, DEREGISTRATION REQUEST, or SERVICE REQUEST message, the UE includes the entire REGISTRATION REQUEST, DEREGISTRATION REQUEST or SERVICE REQUEST message (i.e. containing both cleartext IEs and non-cleartext IEs) in the NAS message container IE and shall cipher the value part of the NAS message container IE. The UE shall then send a REGISTRATION REQUEST, DEREGISTRATION REQUEST, or SERVICE REQUEST message containing the cleartext IEs and the NAS message container IE;

   2) the UE needs to send non-cleartext IEs in a CONTROL PLANE SERVICE REQUEST message:

      i) if CIoT small data container IE is the only non-cleartext IE to be sent, the UE shall cipher the value part of the CIoT small data container IE. The UE shall then send a CONTROL PLANE SERVICE REQUEST message containing the cleartext IEs and the CIoT small data container IE;

      ii) otherwise, the UE includes non-cleartext IEs in the NAS message container IE and shall cipher the value part of the NAS message container IE. The UE shall then send a CONTROL PLANE SERVICE REQUEST message containing the cleartext IEs and the NAS message container IE;

   3) the UE does not need to send non-cleartext IEs in a REGISTRATION REQUEST, DEREGISTRATION REQUEST, or SERVICE REQUEST message, the UE sends the REGISTRATION REQUEST, DEREGISTRATION REQUEST, or SERVICE REQUEST message without including the NAS message container IE; or

4) the UE does not need to send non-cleartext IEs in a CONTROL PLANE SERVICE REQUEST message, the UE sends the CONTROL PLANE SERVICE REQUEST message without including the NAS message container IE and the CIoT small data container IE.

When the initial NAS message is a REGISTRATION REQUEST message, the cleartext IEs are:

- Extended protocol discriminator;
- Security header type;
- Spare half octet;
- Registration request message identity;
- 5GS registration type;
- ngKSI;
- 5GS mobile identity;
- UE security capability;
- Additional GUTI;
- UE status;
- EPS NAS message container;
- NID; and
- UE determined PLMN with disaster condition.

When the initial NAS message is a DEREGISTRATION REQUEST message, the cleartext IEs are:

- Extended protocol discriminator;
- Security header type;
- Spare half octet;
- De-registration request message identity;
- De-registration type;
- ngKSI; and
- 5GS mobile identity.

When the initial NAS message is a SERVICE REQUEST message, the cleartext IEs are:

- Extended protocol discriminator;
- Security header type;
- Spare half octet;
- ngKSI;
- Service request message identity;
- Service type; and
- 5G-S-TMSI.

When the initial NAS message is a CONTROL PLANE SERVICE REQUEST message, the cleartext IEs are:

- Extended protocol discriminator;
- Security header type;

- Spare half octet;
- ngKSI;
- Control plane service request message identity; and
- Control plane service type.

When the UE sends a REGISTRATION REQUEST, DEREGISTRATION REQUEST, SERVICE REQUEST or CONTROL PLANE SERVICE REQUEST message that includes a NAS message container IE, the UE shall set the security header type of the initial NAS message to "integrity protected".

When the AMF receives an integrity protected initial NAS message which includes a NAS message container IE, the AMF shall decipher the value part of the NAS message container IE. If the received initial NAS message is a REGISTRATION REQUEST, DEREGISTRATION REQUEST, or a SERVICE REQUEST message, the AMF shall consider the NAS message that is obtained from the NAS message container IE as the initial NAS message that triggered the procedure.

When the AMF receives a CONTROL PLANE SERVICE REQUEST message which includes a CIoT small data container IE, the AMF shall decipher the value part of the CIoT small data container IE and handle the message as specified in subclause 5.6.1.4.2.

If the UE:

a) has 5G-EA0 as a selected 5G NAS security algorithm; and

b) selects a PLMN other than Registered PLMN and EPLMN over one access;

the UE shall send an initial NAS message including cleartext IEs only via the access type associated with the newly selected PLMN as described in this subclause for the case when the UE does not have a valid 5G NAS security context.

If the UE:

a) has 5G-EA0 as a selected 5G NAS security algorithm; and

b) selects a PLMN other than Registered PLMN and EPLMN over one access, and the Registered PLMN or EPLMN is not registering or registered over other access;

the UE shall delete the 5G NAS security context.

NOTE: UE deletes the 5G NAS security context only if the UE is not in the connected mode.

4.4.7 Protection of NAS IEs

The network can provide the SOR transparent container IE during the registration procedure to the UE in the REGISTRATION ACCEPT message. The SOR transparent container IE is integrity protected by the HPLMN or subscribed SNPN as specified in 3GPP TS 33.501 [24].

The UE can provide the SOR transparent container IE during the registration procedure to the network in the REGISTRATION COMPLETE message. The SoR-MAC-I_{UE} in the SOR transparent container IE is generated by the UE as specified in 3GPP TS 33.501 [24].

The network can provide the Payload container IE during the Network-initiated NAS transport procedure to the UE in DL NAS TRANSPORT message. If the Payload container type IE is set to "SOR transparent container" or "UE parameters update transparent container", the Payload container IE is integrity protected by the HPLMN or subscribed SNPN as specified in 3GPP TS 33.501 [24]. If the Payload container type IE is set to "Multiple payloads" and the payload container type field of the payload container entry is set to "SOR transparent container" or "UE parameters update transparent container", the payload container entry contents field of the payload container entry is integrity protected correspondingly.

The UE can provide the Payload container IE during the UE-initiated NAS transport procedure to the network in UL NAS TRANSPORT message. If the Payload container type IE is set to "SOR transparent container" or "UE parameters update transparent container", the SoR-MAC-I_{UE} or UPU-MAC-I_{UE} in the Payload container IE is generated by the UE as specified in 3GPP TS 33.501 [24]. If the Payload container type IE is set to "Multiple payloads" and the payload container type field of the payload container entry is set to "SOR transparent container" or "UE parameters update

transparent container", the SoR-MAC-I_{UE} or UPU-MAC-I_{UE} in the payload container entry contents field of the payload container entry is generated by the UE correspondingly.

4.5 Unified access control

4.5.1 General

When the UE needs to access the 5GS, the UE not operating as an IAB-node (see 3GPP TS 23.501 [8]), not acting as a 5G ProSe layer-2 UE-to-network relay UE (see 3GPP TS 23.304 [6E]) whose access attempt is triggered by a 5G ProSe layer-2 remote UE, and not acting as an NCR-MT node (see 3GPP TS 38.300 [27]), first performs access control checks to determine if the access is allowed. Access control checks shall be performed for the access attempts defined by the following list of events:

NOTE 1: Although the UE operating as an IAB-node or as an NCR-MT node skips the access control checks, the UE operating as an IAB-node or as an NCR-MT node determines an access category and one or more access identities for each access attempt in order to derive an RRC establishment cause. In this case the NAS provides the RRC establishment cause but does not provide the access category and the one or more access identities to the lower layers.

NOTE 1A: Although the UE acting as a 5G ProSe layer-2 UE-to-network relay UE skips the access control checks, the UE determines an access category and one or more access identities for each access attempt in order to derive an RRC establishment cause.

a) the UE is in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication over 3GPP access and an event that requires a transition to 5GMM-CONNECTED mode occurs; and

b) the UE is in 5GMM-CONNECTED mode over 3GPP access or 5GMM-CONNECTED mode with RRC inactive indication and one of the following events occurs:

   1) 5GMM receives an MO-IMS-registration-related-signalling-started indication, an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication from upper layers;

   2) 5GMM receives a request from upper layers to send a mobile originated SMS over NAS unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode;

   3) 5GMM receives a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session establishment unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode;

   4) 5GMM receives a request from upper layers to send an UL NAS TRANSPORT message for the purpose of UE-requested PDU session modification procedure unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode;

   5) 5GMM receives a request to re-establish the user-plane resources for an existing PDU session;

   6) 5GMM is notified that an uplink user data packet is to be sent for a PDU session with suspended user-plane resources;

   7) 5GMM receives a request from upper layers to send a mobile originated location request unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode;

   8) 5GMM receives a request from upper layers to send a mobile originated signalling transaction towards the PCF by sending an UL NAS TRANSPORT message including a UE policy container (see 3GPP TS 24.587 [19B] and 3GPP TS 24.554 [19E]) unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode to 5GMM-CONNECTED mode; and

   9) 5GMM receives an indication from lower layers of the RAN timing synchronization status change, and decides to transition the UE from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode as specified in subclause 5.3.1.4.

NOTE 2: 5GMM specific procedures initiated by NAS in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication are not subject to access control, e.g. a registration procedure after PS handover will not be prevented by access control (see subclause 5.5).

NOTE 3: LPP messages, SLPP messages, or location event report messages transported in the UL NAS TRANSPORT message sent in response to a mobile terminating or network induced location request, and the corresponding access attempts are handled as MT access.

NOTE 4: Initiating a mobile originated signalling transaction towards the UDM by sending an UL NAS TRANSPORT message including an SOR transparent container is not supported. Therefore, access control for these cases has not been specified.

When the NAS detects one of the above events, the NAS needs to perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

NOTE 5: The NAS is aware of the above events through indications provided by upper layers or through determining the need to start 5GMM procedures through normal NAS behaviour, or both.

To determine the access identities and the access category for a request, the NAS checks the reason for access, types of service requested and profile of the UE including UE configurations, against a set of access identities and access categories defined in 3GPP TS 22.261 [3], namely:

a) a set of standardized access identities;

b) a set of standardized access categories; and

c) a set of operator-defined access categories, if available.

For the purpose of determining the applicable access identities from the set of standardized access identities defined in 3GPP TS 22.261 [3], the NAS shall follow the requirements set out in:

a) subclause 4.5.2 and the rules and actions defined in table 4.5.2.1, if the UE is not operating in SNPN access operation mode over 3GPP access; or

b) subclause 4.5.2A and the rules and actions defined in table 4.5.2A.1, if the UE is operating in SNPN access operation mode over 3GPP access.

In order to enable access barring checks for access attempts identified by lower layers in 5GMM-CONNECTED mode with RRC inactive indication, the UE provides the applicable access identities to lower layers.

NOTE 6: When and how the NAS provides the applicable access identities to lower layers is UE implementation specific.

NOTE 7: Although the UE operating as an IAB-node or as an NCR-MT node skips the access control checks, the UE provides the applicable access identities to lower layers for access attempts identified by lower layers in 5GMM-CONNECTED mode with RRC inactive indication.

For the purpose of determining the applicable access category from the set of standardized access categories and operator-defined access categories defined in 3GPP TS 22.261 [3], the NAS shall follow the requirements set out in:

a) subclause 4.5.2 and the rules and actions defined in table 4.5.2.2, if the UE is not operating in SNPN access operation mode over 3GPP access; or

b) subclause 4.5.2A and the rules and actions defined in table 4.5.2A.2, if the UE is operating in SNPN access operation mode over 3GPP access.

4.5.2 Determination of the access identities and access category associated with a request for access for UEs not operating in SNPN access operation mode over 3GPP access

When the UE needs to initiate an access attempt in one of the events listed in subclause 4.5.1, the UE shall determine one or more access identities from the set of standardized access identities, and one access category from the set of standardized access categories and operator-defined access categories, to be associated with that access attempt.

The set of the access identities applicable for the request is determined by the UE in the following way:

a) for each of the access identities 1, 2, 3, 11, 12, 13, 14 and 15 in table 4.5.2.1, the UE shall check whether the access identity is applicable in the selected PLMN, if a new PLMN is selected, or otherwise if it is applicable in the RPLMN or equivalent PLMN; and

b) if none of the above access identities is applicable, then access identity 0 is applicable.

Table 4.5.2.1: Access identities

Access Identity number	UE configuration
0	UE is not configured with any parameters from this table
1 (NOTE 1)	UE is configured for multimedia priority service (MPS).
2 (NOTE 2)	UE is configured for mission critical service (MCS).
3 (NOTE 4)	UE for which a disaster condition applies
4-10	Reserved for future use
11 (NOTE 3)	Access Class 11 is configured in the UE.
12 (NOTE 3)	Access Class 12 is configured in the UE.
13 (NOTE 3)	Access Class 13 is configured in the UE.
14 (NOTE 3)	Access Class 14 is configured in the UE.
15 (NOTE 3)	Access Class 15 is configured in the UE.
NOTE 1: Access identity 1 is valid when: - the USIM file EF_{UAC_AIC} indicates the UE is configured for access identity 1 and the selected PLMN, if a new PLMN is selected, or RPLMN is the HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present), or a visited PLMN of the home country; - the UE receives the 5GS network feature support IE with the MPS indicator bit set to "Access identity 1 valid" from the RPLMN as described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4; or - the UE receives the Priority indicator IE with the MPS indicator bit set to "Access identity 1 valid" from the RPLMN as described in subclause 5.4.4.3. NOTE 2: Access identity 2 is used by UEs configured for MCS and is valid when: - the USIM file EF_{UAC_AIC} indicates the UE is configured for access identity 2 and the selected PLMN, if a new PLMN is selected, or RPLMN is the HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present), or a visited PLMN of the home country; - the UE receives the 5GS network feature support IE with the MCS indicator bit set to "Access identity 2 valid" from the RPLMN as described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4;or - the UE receives the Priority indicator IE with the MCS indicator bit set to "Access identity 2 valid" from the RPLMN as described in subclause 5.4.4.3. NOTE 3: Access identities 11 and 15 are valid in HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present). Access Identities 12, 13 and 14 are only valid in HPLMN and visited PLMNs of home country only. NOTE 4: Access Identity 3 is valid when the UE is registering or registered for disaster roaming services (see 3GPP TS 23.122 [5]).	

The UE uses the MPS indicator bit of the 5GS network feature support IE or the Priority indicator IE to determine if access identity 1 is valid. Processing of the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message is described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4. Processing of the MPS indicator bit of the Priority indicator IE in the CONFIGURATION UPDATE COMMAND message is described in subclause 5.4.4.3.
When the UE is neither in the HPLMN (if the EHPLMN list is not present or is empty) nor in an EHPLMN (if the EHPLMN list is present) nor in a visited PLMN of the home country, and the USIM file EF_{UAC_AIC} indicates the UE is configured for access identity 1, then the UE shall not consider access identity 1 to be valid, until the UE receives the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message or of the Priority indicator IE in the CONFIGURATION UPDATE COMMAND message being set to "Access identity 1 valid" from the RPLMN or from an equivalent PLMN.

When the UE is in the HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, the contents of the USIM file EF_{UAC_AIC} as specified in 3GPP TS 31.102 [22] and the rules specified in table 4.5.2.1 are used to determine the applicability of access identity 1.
When the UE is in the HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, and the USIM file EF_{UAC_AIC} does not indicate the UE is configured for access identity 1, the UE uses the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message or of the Priority indicator IE in the CONFIGURATION UPDATE COMMAND message to determine if access identity 1 is valid. When the UE is in the HPLMN (if the EHPLMN list is not present or

is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, and the USIM file EF_{UAC_AIC} indicates the UE is configured for access identity 1, the MPS indicator bit of the 5GS network feature support IE and the Priority indicator IE are not applicable. When the UE is not in the HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, the contents of the USIM file EF_{UAC_AIC} are not applicable.

The UE uses the MCS indicator bit of the 5GS network feature support IE or of the Priority indicator IE to determine if access identity 2 is valid. Processing of the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message is described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4. Processing of the MCS indicator bit of the Priority indicator IE in the CONFIGURATION UPDATE COMMAND message is described in subclause 5.4.4.3. When the UE is neither in the HPLMN (if the EHPLMN list is not present or is empty) nor in an EHPLMN (if the EHPLMN list is present) nor in a visited PLMN of the home country, and the USIM file EF_{UAC_AIC} indicates the UE is configured for access identity 2, the UE shall not consider access identity 2 to be valid , until the UE receives the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message or of the Priority indicator IE in the CONFIGURATION UPDATE COMMAND message being set to "Access identity 2 valid" from the RPLMN or from an equivalent PLMN.

When the UE is in the HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, the contents of the USIM file EF_{UAC_AIC} as specified in 3GPP TS 31.102 [22] and the rules specified in table 4.5.2.1 are used to determine the applicability of access identity 2. When the UE is in the HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, and the USIM file EF_{UAC_AIC} does not indicate the UE is configured for access identity 2, the UE uses the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message or of the Priority indicator IE in the CONFIGURATION UPDATE COMMAND message to determine if access identity 2 is valid. When the UE is in the HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, and the USIM file EF_{UAC_AIC} indicates the UE is configured for access identity 2, the MCS indicator bit of the 5GS network feature support IE and the Priority indicator IE is not applicable. When the UE is not in the HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present) or in a visited PLMN of the home country, the contents of the USIM file EF_{UAC_AIC} are not applicable.

The UE checks the conditions specified in subclause 4.4.3.1.1 of 3GPP TS 23.122 [5] to determine if access identity 3 is valid, and the applicability of access identity 3.

When the UE is in its HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present), the contents of the USIM file EF_{ACC} as specified in 3GPP TS 31.102 [22] and the rules specified in table 4.5.2.1 are used to determine the applicability of access classes 11 and 15. When the UE is not in its HPLMN (if the EHPLMN list is not present or is empty) or in an EHPLMN (if the EHPLMN list is present), access classes 11 and 15 are not applicable.

When the UE is in the HPLMN or in a visited PLMN of the home country, the contents of the USIM file EF_{ACC} as specified in 3GPP TS 31.102 [22] and the rules specified in table 4.5.2.1 are used to determine the applicability of access classes 12 - 14. When the UE is neither in the HPLMN nor in a visited PLMN of the home country, access classes 12-14 are not applicable.

In order to determine the access category applicable for the access attempt, the NAS shall check the rules in table 4.5.2.2, and use the access category for which there is a match for barring check. If the access attempt matches more than one rule, the access category of the lowest rule number shall be selected. If the access attempt matches more than one operator-defined access category definition, the UE shall select the access category from the operator-defined access category definition with the lowest precedence value (see subclause 4.5.3).

NOTE: The case when an access attempt matches more than one rule includes the case when multiple events trigger an access attempt at the same time. When multiple events trigger an access attempt at the same time, how the access attempt is checked for multiple events is up to UE implementation.

Table 4.5.2.2: Mapping table for access categories

Rule #	Type of access attempt	Requirements to be met	Access Category
1	Response to paging or NOTIFICATION over non-3GPP access; 5GMM connection management procedure initiated for the purpose of transporting an LPP or SLPP message without an ongoing 5GC-MO-LR or SL-MO-LR procedure; Access attempt to handover of ongoing MMTEL voice call, MMTEL video call or SMSoIP from non-3GPP access; or Access attempt upon receipt of "call-pull-initiated" indication from the upper layers (see 3GPP TS 24.174 [13D])	Access attempt is for MT access, or handover of ongoing MMTEL voice call, MMTEL video call or SMSoIP from non-3GPP access; or Access attempt is made upon receipt of "call-pull-initiated" (3GPP TS 24.174 [13D])	0 (= MT_acc)
2	Emergency	UE is attempting access for an emergency session (NOTE 1, NOTE 2)	2 (= emergency)
3	Access attempt for operator-defined access category	UE stores operator-defined access category definitions valid in the current PLMN as specified in subclause 4.5.3, and access attempt is matching criteria of an operator-defined access category definition	32-63 (= based on operator classification)
3.1	Access attempt for MO exception data	UE is in NB-N1 mode and allowed to use exception data reporting (see the ExceptionDataReportingAllowed leaf of the NAS configuration MO in 3GPP TS 24.368 [17] or the USIM file $EF_{NASCONFIG}$ in 3GPP TS 31.102 [22]), and access attempt is for MO data or for MO signalling initiated upon receiving a request from upper layers to transmit user data related to an exceptional event.	10 (= MO exception data)
4	Access attempt for delay tolerant service	(a) UE is configured for NAS signalling low priority or UE supporting S1 mode is configured for EAB (see the "ExtendedAccessBarring" leaf of NAS configuration MO in 3GPP TS 24.368 [17] or 3GPP TS 31.102 [22]) where "EAB override" does not apply, and (b): the UE received one of the categories a, b or c as part of the parameters for unified access control in the broadcast system information, and the UE is a member of the broadcasted category in the selected PLMN or RPLMN/equivalent PLMN (NOTE 3, NOTE 5, NOTE 6, NOTE 7, NOTE 8)	1 (= delay tolerant)
5	MO MMTel voice call; or MT MMTel voice call	Access attempt is for MO MMTel voice call or MT MMTel voice call or for NAS signalling connection recovery during ongoing MO MMTel voice call or ongoing MT MMTel voice call (NOTE 2)	4 (= MO MMTel voice)
6	MO MMTel video call; or MT MMTel video call	Access attempt is for MO MMTel video call or MT MMTel video call or for NAS signalling connection recovery during ongoing MO MMTel video call or ongoing MT MMTel video call (NOTE 2)	5 (= MO MMTel video)

7	MO SMS over NAS or MO SMSoIP; or MT SMSoIP	Access attempt is for MO SMS over NAS (NOTE 4) or MO SMS over SMSoIP transfer or MT SMS over SMSoIP or for NAS signalling connection recovery during ongoing MO SMS or SMSoIP transfer or ongoing MT SMS over SMSoIP (NOTE 2)	6 (= MO SMS and SMSoIP)
7.1	MO IMS registration related signalling	Access attempt is for MO IMS registration related signalling (e.g. IMS initial registration, re-registration, subscription refresh) or for NAS signalling connection recovery during ongoing procedure for MO IMS registration related signalling (NOTE 2a)	9 (= MO IMS registration related signalling)
8	UE NAS initiated 5GMM specific procedures	Access attempt is for MO signalling	3 (= MO_sig)
8.1	Mobile originated location request	Access attempt is for mobile originated location request (NOTE 9)	3 (= MO_sig)
8.2	Mobile originated signalling transaction towards the PCF	Access attempt is for mobile originated signalling transaction towards the PCF (NOTE 10)	3 (= MO_sig)
8.3	Access attempt for RAN timing synchronization	Access attempt is for mobile originated signalling for the reconnection to the network due to RAN timing synchronization status change	3 (= MO_sig)
9	UE NAS initiated 5GMM connection management procedure or 5GMM NAS transport procedure	Access attempt is for MO data	7 (= MO_data)
10	An uplink user data packet is to be sent for a PDU session with suspended user-plane resources	No further requirement is to be met	7 (= MO_data)

NOTE 1: This includes 5GMM specific procedures while the service is ongoing and 5GMM connection management procedures required to establish a PDU session with request type = "initial emergency request" or "existing emergency PDU session", or to re-establish user-plane resources for such a PDU session. This further includes the service request procedure initiated with a SERVICE REQUEST message with the Service type IE set to "emergency services fallback".

NOTE 2: Access for the purpose of NAS signalling connection recovery during an ongoing service as defined in subclause 4.5.5, or for the purpose of NAS signalling connection establishment following fallback indication from lower layers during an ongoing service as defined in subclause 4.5.5, is mapped to the access category of the ongoing service in order to derive an RRC establishment cause, but barring checks will be skipped for this access attempt.

NOTE 2a: Access for the purpose of NAS signalling connection recovery during an ongoing procedure for MO IMS registration related signalling as defined in subclause 4.5.5, or for the purpose of NAS signalling connection establishment following fallback indication from lower layers during an ongoing procedure for MO IMS registration related signalling as defined in subclause 4.5.5, is mapped to the access category of the MO IMS registration related signalling in order to derive an RRC establishment cause, but barring checks will be skipped for this access attempt.

NOTE 3: If the UE selects a new PLMN, then the selected PLMN is used to check the membership; otherwise the UE uses the RPLMNor a PLMN equivalent to the RPLMN.

NOTE 4: This includes the 5GMM connection management procedures triggered by the UE-initiated NAS transport procedure for transporting the MO SMS.

NOTE 5: The UE configured for NAS signalling low priority is not supported in this release of specification. If a UE supporting both S1 mode and N1 mode is configured for NAS signalling low priority in S1 mode as specified in 3GPP TS 24.368 [17] or 3GPP TS 31.102 [22], the UE shall ignore the configuration for NAS signalling low priority when in N1 mode.

NOTE 6: If the access category applicable for the access attempt is 1, then the UE shall additionally determine a second access category from the range 3 to 7. If more than one access category matches, the access category of the lowest rule number shall be chosen. The UE shall use the second access category only to derive an RRC establishment cause for the access attempt.

NOTE 7: "EAB override" does not apply, if the UE is not configured to allow overriding EAB (see the "Override_ExtendedAccessBarring" leaf of NAS configuration MO in 3GPP TS 24.368 [17] or 3GPP TS 31.102 [22]), or if NAS has not received an indication from the upper layers to override EAB and the UE does not have a PDU session that was established with EAB override.

NOTE 8: For the definition of categories a, b and c associated with access category 1, see 3GPP TS 22.261 [3]. The categories associated with access category 1 are distinct from the categories a, b and c associated with EAB (see 3GPP TS 22.011 [1A]).

NOTE 9: This includes:
a) the UE-initiated NAS transport procedure for transporting a mobile originated location request;
b) the 5GMM connection management procedure triggered by a) above; and
c) NAS signalling connection recovery during an ongoing 5GC-MO-LR procedure.

NOTE 10: This includes:
a) the UE-initiated NAS transport procedure for transporting a mobile originated signalling transaction towards the PCF;
b) the 5GMM connection management procedure triggered by a) above; and
c) NAS signalling connection recovery during an ongoing UE-requested policy provisioning procedure for V2XP, ProSeP or both (see 3GPP TS 24.587 [19B] and see 3GPP TS 24.554 [19E]).

4.5.2A Determination of the access identities and access category associated with a request for access for UEs operating in SNPN access operation mode over 3GPP access

When the UE needs to initiate an access attempt in one of the events listed in subclause 4.5.1, the UE shall determine one or more access identities from the set of standardized access identities, and one access category from the set of standardized access categories and operator-defined access categories, to be associated with that access attempt.

The set of the access identities applicable for the request is determined by the UE in the following way:

a) for each of the access identities 1, 2, 11, 12, 13, 14 and 15 in table 4.5.2A.1, the UE shall check whether the access identity is applicable in the selected SNPN, if a new SNPN is selected, or otherwise if it is applicable in the RSNPN or equivalent SNPN; and

b) if none of the above access identities is applicable, then access identity 0 is applicable.

Table 4.5.2A.1: Access identities

Access Identity number	UE configuration
0	UE is not configured with any parameters from this table
1 (NOTE 1)	UE is configured for multimedia priority service (MPS).
2 (NOTE 2)	UE is configured for mission critical service (MCS).
3-10	Reserved for future use
11 (NOTE 3)	Access Class 11 is configured in the UE.
12 (NOTE 3)	Access Class 12 is configured in the UE.
13 (NOTE 3)	Access Class 13 is configured in the UE.
14 (NOTE 3)	Access Class 14 is configured in the UE.
15 (NOTE 3)	Access Class 15 is configured in the UE.

NOTE 1: Access identity 1 is valid when:
- the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, indicates the UE is configured for access identity 1 in the selected SNPN, if a new SNPN is selected, or RSNPN, and the selected SNPN or the RSNPN is the subscribed SNPN, an SNPN equivalent to the subscribed SNPN, or an non-subscribed SNPN of the same country as the subscribed SNPN if the MCC of the SNPN identity of the subscribed SNPN is not the MCC of value 999;
- the UE receives the 5GS network feature support IE with the MPS indicator bit set to "Access identity 1 valid" from the RSNPN as described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4; or
- the UE receives the Priority indicator IE with the MPS indicator bit set to "Access identity 1 valid" from the RPLMN as described in subclause 5.4.4.3.

NOTE 2: Access identity 2 is used by UEs configured for MCS and is valid when:
- the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, indicates the UE is configured for access identity 2 in the selected SNPN, if a new SNPN is selected, or RSNPN, and the selected SNPN or the RSNPN is the subscribed SNPN, or an SNPN equivalent to the subscribed SNPN, or an non-subscribed SNPN of the same country as the subscribed SNPN if the MCC of the SNPN identity of the subscribed SNPN is not the MCC of value 999; or
- the UE receives the 5GS network feature support IE with the MCS indicator bit set to "Access identity 2 valid" from the RSNPN as described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4.

NOTE 3: Access identities 11 and 15 are valid if indicated as configured for the UE in the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, in the selected SNPN, if a new SNPN is selected, or RSNPN, and the selected SNPN or the RSNPN is the subscribed SNPN. Access identities 12, 13 and 14 are valid if indicated as configured for the UE in the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, in the selected SNPN, if a new SNPN is selected, or RSNPN, and the selected SNPN or the RSNPN in the subscribed SNPN or an non-subscribed SNPN of the same country as the subscribed SNPN if the MCC of the SNPN identity of the subscribed SNPN is not the MCC of value 999.

The contents of the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, and the rules specified in table 4.5.2A.1 are used to determine the applicability of access identity 1 in the SNPN. When the contents of the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, do not indicate the UE is configured for access identity 1 for the SNPN, the UE uses the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message and the MPS indicator bit of the Priority indicator IE in the CONFIGURATION UPDATE COMMAND message to determine if access identity 1 is valid.

The contents of the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, and the rules specified in table 4.5.2A.1 are used to determine the applicability of access identity 2 in the SNPN. When the contents of the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, do not indicate the UE is configured for access identity 2 for the SNPN, the UE uses the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 2 is valid.

The contents of the unified access control configuration in the "list of subscriber data" stored in the ME (see 3GPP TS 23.122 [5]), if an entry of "list of subscriber data" is selected, or in the USIM (see 3GPP TS 31.102 [22]), if the PLMN subscription is selected, and the rules specified in table 4.5.2A.1 are used to determine the applicability of access classes 11 to 15 in the SNPN.

In order to determine the access category applicable for the access attempt, the NAS shall check the rules in table 4.5.2A.2, and use the access category for which there is a match for barring check. If the access attempt matches more than one rule, the access category of the lowest rule number shall be selected. If the access attempt matches more than one operator-defined access category definition, the UE shall select the access category from the operator-defined access category definition with the lowest precedence value (see subclause 4.5.3).

NOTE: The case when an access attempt matches more than one rule includes the case when multiple events trigger an access attempt at the same time. When multiple events trigger an access attempt at the same time, how the access attempt is checked for multiple events is up to UE implementation.

Table 4.5.2A.2: Mapping table for access categories

Rule #	Type of access attempt	Requirements to be met	Access Category
1	Response to paging or NOTIFICATION over non-3GPP access ; 5GMM connection management procedure initiated for the purpose of transporting an LPP or SLPP message without an ongoing 5GC-MO-LR or SL-MO-LR procedure; Access attempt to handover of MMTEL voice call, MMTEL video call or SMSoIP from non-3GPP access; Access attempt upon receipt of "call-pull-initiated" indication from the upper layers (see 3GPP TS 24.174 [13D])	Access attempt is for MT access, handover of ongoing MMTEL voice call, MMTEL video call or SMSoIP from non-3GPP access; or Access attempt is made upon receipt of "call-pull-initiated" indication (3GPP TS 24.174 [13D])	0 (= MT_acc)
2	Emergency	UE is attempting access for an emergency session (NOTE 1, NOTE 2)	2 (= emergency)
3	Access attempt for operator-defined access category	UE stores operator-defined access category definitions valid in the SNPN as specified in subclause 4.5.3, and access attempt is matching criteria of an operator-defined access category definition	32-63 (= based on operator classification)
4	Access attempt for delay tolerant service	(a) UE is configured for NAS signalling low priority, and (b) the UE received one of the categories a, b or c as part of the parameters for unified access control in the broadcast system information, and the UE is a member of the broadcasted category in the selected SNPN, RSNPN or equivalent SNPN (NOTE 3, NOTE 5, NOTE 6, NOTE 7, NOTE 8)	1 (= delay tolerant)
5	MO MMTel voice call; or MT MMTel voice call	Access attempt is for MO MMTel voice call or MT MMTel voice call or for NAS signalling connection recovery during ongoing MO MMTel voice call or ongoing MT MMTel voice call (NOTE 2)	4 (= MO MMTel voice)
6	MO MMTel video call; or MT MMTel video call	Access attempt is for MO MMTel video call or MT MMTel video call or for NAS signalling connection recovery during ongoing MO MMTel video call or ongoing MT MMTel video call (NOTE 2)	5 (= MO MMTel video)
7	MO SMS over NAS or MO SMSoIP; or MT SMSoIP	Access attempt is for MO SMS over NAS (NOTE 4) or MO SMS over SMSoIP transfer or MT SMS over SMSoIP or for NAS signalling connection recovery during ongoing MO SMS or SMSoIP transfer or MT SMS over SMSoIP (NOTE 2)	6 (= MO SMS and SMSoIP)
7.1	MO IMS registration related signalling	Access attempt is for MO IMS registration related signalling (e.g. IMS initial registration, re-registration, subscription refresh) or for NAS signalling connection recovery during ongoing procedure for MO IMS registration related signalling (NOTE 2a)	9 (= MO IMS registration related signalling)
8	UE NAS initiated 5GMM specific procedures	Access attempt is for MO signalling	3 (= MO_sig)
8.1	Mobile originated location request	Access attempt is for mobile originated location request (NOTE 9)	3 (= MO_sig)

8.2	Mobile originated signalling transaction towards the PCF	Access attempt is for mobile originated signalling transaction towards the PCF (NOTE 10)	3 (= MO_sig)
8.3	Access attempt for RAN timing synchronization	Access attempt is for mobile originated signalling for the reconnection to the network due to RAN timing synchronization status change	3 (= MO_sig)
9	UE NAS initiated 5GMM connection management procedure or 5GMM NAS transport procedure	Access attempt is for MO data	7 (= MO_data)
10	An uplink user data packet is to be sent for a PDU session with suspended user-plane resources	No further requirement is to be met	7 (= MO_data)

NOTE 1: Void

NOTE 2: Access for the purpose of NAS signalling connection recovery during an ongoing service as defined in subclause 4.5.5, or for the purpose of NAS signalling connection establishment following fallback indication from lower layers during an ongoing service as defined in subclause 4.5.5, is mapped to the access category of the ongoing service in order to derive an RRC establishment cause, but barring checks will be skipped for this access attempt.

NOTE 2a: Access for the purpose of NAS signalling connection recovery during an ongoing MO IMS registration related signalling as defined in subclause 4.5.5, or for the purpose of NAS signalling connection establishment following fallback indication from lower layers during an ongoing MO IMS registration related signalling as defined in subclause 4.5.5, is mapped to the access category of the MO IMS registration related signalling in order to derive an RRC establishment cause, but barring checks will be skipped for this access attempt.

NOTE 3: If the UE selects a new SNPN, then the selected SNPN is used to check the membership; otherwise the UE uses the RSNPN or an SNPN equivalent to the RSNPN.

NOTE 4: This includes the 5GMM connection management procedures triggered by the UE-initiated NAS transport procedure for transporting the MO SMS.

NOTE 5: The UE configured for NAS signalling low priority is not supported in this release of specification.

NOTE 6: If the access category applicable for the access attempt is 1, then the UE shall additionally determine a second access category from the range 3 to 7. If more than one access category matches, the access category of the lowest rule number shall be chosen. The UE shall use the second access category only to derive an RRC establishment cause for the access attempt.

NOTE 7: Void.

NOTE 8: For the definition of categories a, b and c associated with access category 1, see 3GPP TS 22.261 [3]. The categories associated with access category 1 are distinct from the categories a, b and c associated with EAB (see 3GPP TS 22.011 [1A]).

NOTE 9: This includes:
a) the UE-initiated NAS transport procedure for transporting a mobile originated location request;
b) the 5GMM connection management procedure triggered by a) above; and
c) NAS signalling connection recovery during an ongoing 5GC-MO-LR procedure.

NOTE 10: This includes:
a) the UE-initiated NAS transport procedure for transporting a mobile originated signalling transaction towards the PCF;
b) the 5GMM connection management procedure triggered by a) above; and
c) NAS signalling connection recovery during an ongoing UE-requested policy provisioning procedure for V2XP (see 3GPP TS 24.587 [19B]).

.

4.5.3 Operator-defined access categories

Operator-defined access category definitions can be signalled to the UE using NAS signalling. Each operator-defined access category definition consists of the following parameters:

a) a precedence value which indicates in which order the UE shall evaluate the operator-defined category definition for a match;

b) an operator-defined access category number, i.e. access category number in the 32-63 range that uniquely identifies the access category in the PLMN or SNPN in which the access categories are being sent to the UE;

c) criteria consisting of one or more access category criteria type and associated access category criteria type values. The access category criteria type can be set to one of the following:

1) DNN;

2) Void;

3) OS Id + OS App Id of application triggering the access attempt; or

4) S-NSSAI; and

NOTE 1: An access category criteria type can be associated with more than one access category criteria values.

d) optionally, a standardized access category. This standardized access category is used in combination with the access identities of the UE to determine the RRC establishment cause as specified in subclause 4.5.6.

If the access attempt is to establish a new PDU session i.e. it is triggered by:

- a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session establishment unless the request triggered a service request procedure (or a registration procedure if the UE is in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE) to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode; or

- a service request procedure (or a registration procedure if the UE is in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE) to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode triggered by a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session establishment,

then:

- the access attempt matches access category criteria type DNN if the DNN requested by the UE during the PDU session establishment procedure matches any of the access criteria type values associated with the access criteria type DNN; and

- the access attempt matches access category criteria type S-NSSAI if the S-NSSAI requested by the UE during the PDU session establishment procedure matches any of the access criteria type values associated with the access criteria type S-NSSAI.

If the access attempt is for an existing PDU session i.e. it is triggered by:

- a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session modification unless the request triggered a service request procedure (or a registration procedure if the UE is in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE) to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode;

- a service request procedure (or a registration procedure if the UE is in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE) to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode triggered by a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session modification;

- a service request procedure (or a registration procedure if the UE is in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE) to transition the UE from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication to 5GMM-CONNECTED mode triggered by a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session release;

- a service request procedure (or a registration procedure if the UE is in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE) requesting user-plane resources for a PDU session; or

- an uplink user data packet is to be sent for a PDU session with suspended user-plane resources,

then:

- the access attempt matches access category criteria type DNN if the DNN provided by the network in the PDU SESSION ESTABLISHMENT ACCEPT message matches any of the access criteria type values associated with the access criteria type DNN; and

- the access attempt matches access category criteria type S-NSSAI if the S-NSSAI associated with the PDU session matches any of the access criteria type values associated with the access criteria type S-NSSAI.

NOTE 2: In order to avoid having access attempts for non-always-on PDU sessions blocked due to access barring of always-on PDU sessions, it is recommended that the network assigns the highest precedence values to operator-defined access category definition which can be matched by always-on PDU sessions.

An access attempt matches the criteria of an operator-defined access category definition, if the access attempt matches all access category criteria types included in the criteria with any of the associated access criteria type values.

Each operator-defined access category definition has a different precedence value.

Several operator-defined access category definitions can have the same operator-defined access category number.

If:

- an access category in bullet d) is not provided;
- an access category in bullet d) is provided and is not a standardized access category; or
- an access category in bullet d) is provided, is a standardized access category and is not recognized by the UE;

the UE shall use instead access category 7 (MO_data) in combination with the access identities of the UE to determine the RRC establishment cause as specified in subclause 4.5.6.

The operator-defined access category definitions are valid in the PLMN which provided them and in a PLMN equivalent to the PLMN which provided them, or in the SNPN which provided them and in an SNPN equivalent to the SNPN which provided them, as specified in annex C.

If the UE stores operator-defined access category definitions valid in the selected PLMN or the RPLMN, or valid in the selected SNPN or RSNPN, then access control in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication will only be performed for the event a) defined in subclause 4.5.1. If the transition from 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication over 3GPP access to 5GMM-CONNECTED mode is due to a UE NAS initiated 5GMM specific procedure, then this access attempt shall be mapped to one of the standardized access categories in the range < 32, see subclause 4.5.2. I.e. for this case the UE shall skip the checking of operator-defined access category definitions.

If the UE stores operator-defined access category definitions valid in the selected PLMN or the RPLMN, or valid in the selected SNPN or RSNPN, then access control in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication will only be performed for the events 1) to 8) defined in subclause 4.5.1.

The UE shall handle the operator-defined access category definitions stored for the RPLMN or RSNPN as specified in subclause 5.4.4.3, subclause 5.5.1.2.4, and subclause 5.5.1.3.4.

When the UE is switched off, the UE shall keep the operator-defined access category definitions so that the operator-defined access category definitions can be used after switch on.

When the UE selects a new PLMN which is not equivalent to the previously selected PLMN, or selects a new SNPN which is not equivalent to the previously selected SNPN, the UE shall stop using the operator-defined access category definitions stored for the previously selected PLMN or SNPN and should keep the operator-defined access category definitions stored for the previously selected PLMN or SNPN.

NOTE 3: When the UE selects a new PLMN which is not equivalent to the previously selected PLMN, or selects a new SNPN which is not equivalent to the previously selected SNPN, the UE can delete the operator-defined access category definitions stored for the previously selected PLMN or SNPN e.g. if there is no storage space in the UE.

4.5.4 Access control and checking

4.5.4.1 Access control and checking in 5GMM-IDLE mode and in 5GMM-IDLE mode with suspend indication

When the UE is in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication, upon receiving a request from the upper layers for an access attempt, the NAS shall categorize the access attempt into access identities and an access category following:

a) subclause 4.5.2, table 4.5.2.1 and table 4.5.2.2, and subclause 4.5.3, if the UE is not operating in SNPN access operation mode over 3GPP access ; or

b) subclause 4.5.2A, table 4.5.2A.1 and table 4.5.2A.2, and subclause 4.5.3, if the UE is operating in SNPN access operation mode over 3GPP access ,

and provide the applicable access identities and the access category to the lower layers for the purpose of access control checking. In this request to the lower layer the NAS can also provide to the lower layer the RRC establishment cause determined as specified in subclause 4.5.6 of this specification.

NOTE 1: The access barring check is performed by the lower layers.

NOTE 2: As an implementation option, the NAS can provide the RRC establishment cause to the lower layers after being informed by the lower layers that the access attempt is allowed.

If the UE has uplink user data pending for one or more PDU sessions when it builds a REGISTRATION REQUEST or SERVICE REQUEST message as initial NAS message, the UE shall indicate the respective PDU sessions in the Uplink data status IE as specified in subclause 5.5.1.3.2 and 5.6.1.2.1, regardless of the access category for which the access barring check is performed.

If the UE is registered for 5GS services with control plane CIoT 5GS optimization has uplink user data pending for one or more PDU sessions when it builds a CONTROL PLANE SERVICE REQUEST message as initial NAS message, the UE shall indicate the respective PDU sessions as specified in subclause 5.6.1.2.2, regardless of the access category for which the access barring check is performed.

NOTE 3: The UE indicates pending user data for all the respective PDU sessions, even if barring timers are running for some of the corresponding access categories.

If the lower layers indicate that the access attempt is allowed, the NAS shall initiate the procedure to send the initial NAS message for the access attempt.

If the lower layers indicate that the access attempt is barred, the NAS shall not initiate the procedure to send the initial NAS message for the access attempt. Additionally:

a) if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication or an MO-MMTEL-video-call-started indication:

   1) if the UE is operating in the single-registration mode, the UE's usage setting is "voice centric" and the UE has not disabled its E-UTRA capability as specified in 3GPP TS 24.301 [15], the UE may attempt to select an E-UTRA cell connected to EPC. If the UE finds a suitable E-UTRA cell connected to EPC, it then proceeds with the appropriate EMM specific procedures and, if necessary, ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.2 and 3GPP TS 24.301 [15];

   2) if the UE is operating in the dual-registration mode, the UE may proceed in S1 mode with the appropriate EMM specific procedures and ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.3 and 3GPP TS 24.301 [15]; or

   3) otherwise, the NAS shall notify the upper layers that the access attempt is barred. In this case, upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS shall notify the upper layers that the barring is alleviated for the access category and may initiate the procedure to send the initial NAS message, if still needed;

b) if the event which triggered the access attempt was an MO-SMSoIP-attempt-started indication or an MO-IMS-registration-related-signalling-started indication:

   1) if the UE is operating in the single-registration mode, the UE may attempt to select an E-UTRA cell connected to EPC. If the UE finds a suitable E-UTRA cell connected to EPC, it then proceeds with the appropriate EMM specific procedures and, if necessary, ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.2 and 3GPP TS 24.301 [15];

   2) if the UE is operating in the dual-registration mode, the UE may proceed in S1 mode with the appropriate EMM specific procedures and ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.3 and 3GPP TS 24.301 [15]; or

3) otherwise, the NAS shall notify the upper layers that the access attempt is barred. In this case, upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS shall notify the upper layers that the barring is alleviated for the access category and may initiate the procedure to send the initial NAS message, if still needed; and

c) if the access attempt is for emergency:

1) the NAS shall notify the upper layers that the access attempt is barred. In this case, upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS shall notify the upper layers of that the barring is alleviated for the access category and may initiate the procedure to send the initial NAS message, if still needed.

NOTE 4: This can result in the upper layers requesting another emergency call attempt using domain selection as specified in 3GPP TS 23.167 [6] and 3GPP TS 24.229 [14].

NOTE 5: Barring timers, on a per access category basis, are run by the lower layers. At expiry of barring timers, the indication of alleviation of access barring is indicated to the NAS on a per access category basis.

4.5.4.2 Access control and checking in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication

When the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication, upon detecting one of events 1) through 8) listed in subclause 4.5.1, the NAS shall categorize the corresponding access attempt into access identities and an access category following:

a) subclause 4.5.2, table 4.5.2.1 and table 4.5.2.2, and subclause 4.5.3, if the UE is not operating in SNPN access operation mode over 3GPP access ; or

b) subclause 4.5.2A, table 4.5.2A.1 and table 4.5.2A.2, and subclause 4.5.3, if the UE is operating in SNPN access operation mode over 3GPP access ,

and provide the access identities and the access category to the lower layers for the purpose of access control checking. In this request to the lower layer the NAS can also provide to the lower layer the RRC establishment cause determined as specified in subclause 4.5.6 of this specification.

NOTE 1: As an implementation option, the NAS can provide the RRC establishment cause to the lower layers after being informed by the lower layers that the access attempt is allowed.

If the UE has uplink user data pending for one or more PDU sessions when it builds a REGISTRATION REQUEST or SERVICE REQUEST message for the access attempt, the UE shall indicate the respective PDU sessions in the Uplink data status IE as specified in subclause 5.5.1.3.2 and 5.6.1.2, regardless of the access category for which the access barring check is performed.

NOTE 2: The UE indicates pending user data for all the respective PDU sessions, even if barring timers are running for some of the corresponding access categories.

If the lower layers indicate that the access attempt is allowed, the NAS shall take the following action depending on the event which triggered the access attempt:

a) if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication, an MO-SMSoIP-attempt-started indication, or an MO-IMS-registration-related-signalling-started indication, the NAS shall notify the upper layers that the access attempt is allowed;

b) if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send the SMS in an UL NAS TRANSPORT message;

c) if the event which triggered the access attempt was a request from upper layers to establish a new PDU session, 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send the PDU SESSION ESTABLISHMENT REQUEST message;

d) if the event which triggered the access attempt was a request from upper layers to modify an existing PDU session, 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send the PDU SESSION MODIFICATION REQUEST message;

e) if the event which triggered the access attempt was a request to re-establish the user-plane resources for an existing PDU session, 5GMM shall initiate the service request procedure as specified in subclause 5.6.1;

f) if the event which triggered the access attempt was an uplink user data packet to be sent for a PDU session with suspended user-plane resources, 5GMM shall consider that the uplink user data packet is allowed to be sent;

g) if the event which triggered the access attempt was a request from upper layers to send a mobile originated location request, 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send an LCS message in an UL NAS TRANSPORT message; and

h) if the event which triggered the access attempt was a request from upper layers to send a mobile originated signalling transaction towards the PCF by sending an UL NAS TRANSPORT message including a UE policy container (see 3GPP TS 24.587 [19B] and 3GPP TS 24.554 [19E]), 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send the signalling transaction via an UL NAS TRANSPORT message.

If the lower layers indicate that the access attempt is barred, the NAS shall take the following action depending on the event which triggered the access attempt:

a) if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, or an MO-IMS-registration-related-signalling-started indication:

   1) if the UE is operating in the dual-registration mode, the UE may proceed in S1 mode with the appropriate EMM specific procedures and ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.3 and 3GPP TS 24.301 [15];

   2) otherwise, the NAS shall notify the upper layers that the access attempt is barred. In this case, upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS shall notify the upper layers that the barring is alleviated for the access category;

NOTE 3: In this case prohibiting the initiation of the MMTEL voice session, MMTEL video session or prohibiting sending of the SMS over IP or the IMS registration related signalling is performed by the upper layers.

b) if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, 5GMM shall not initiate the NAS transport procedure as specified in subclause 5.4.5 to send the SMS in an UL NAS TRANSPORT message. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, 5GMM may initiate the NAS transport procedure as specified in subclause 5.4.5 to send the SMS in an UL NAS TRANSPORT message, if still needed;

c) if the event which triggered the access attempt was a request from upper layers to establish a new PDU session, 5GMM shall not initiate the NAS transport procedure to send the PDU SESSION ESTABLISHMENT REQUEST message. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS may initiate the NAS transport procedure as specified in subclause 5.4.5, if still needed;

d) if the event which triggered the access attempt was a request from upper layers to modify an existing PDU session modification, 5GMM shall not initiate the NAS transport procedure to send the PDU SESSION MODIFICATION REQUEST message. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS may initiate the NAS transport procedure as specified in subclause 5.4.5, if still needed;

e) if the event which triggered the access attempt was a request to re-establish the user-plane resources for an existing PDU session, the NAS shall not initiate the service request procedure as specified in subclause 5.6.1. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS may initiate the service request procedure as specified in subclause 5.6.1, if still needed;

f) if the event which triggered the access attempt was an uplink user data packet to be sent for a PDU session with suspended user-plane resources, 5GMM shall consider that the uplink user data packet is not allowed to be sent. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with

which the access attempt was associated, the NAS shall consider that the barring is alleviated for the access category;

g) if the event which triggered the access attempt was a request from upper layers to send a mobile originated location request, 5GMM shall not initiate the NAS transport procedure as specified in subclause 5.4.5 to send an LCS message in an UL NAS TRANSPORT message. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, 5GMM may initiate the NAS transport procedure as specified in subclause 5.4.5 to send the LCS message in an UL NAS TRANSPORT message, if still needed; and

h) if the event which triggered the access attempt was a request from upper layers to send a mobile originated signalling transaction towards the PCF by sending an UL NAS TRANSPORT message including a UE policy container (see 3GPP TS 24.587 [19B] and 3GPP TS 24.554 [19E]), 5GMM shall not initiate the NAS transport procedure as specified in subclause 5.4.5 to send the mobile originated signalling transaction via an UL NAS TRANSPORT message. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, 5GMM may initiate the NAS transport procedure as specified in subclause 5.4.5 to send the mobile originated signalling transaction via an UL NAS TRANSPORT message, if still needed.

4.5.5 Exception handling and avoiding double barring

Access attempts are allowed to proceed without further access control checking in order to avoid double barring for any service request or registration procedure initiated for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclauses 5.3.1.2 and 5.3.1.4).

NOTE 1: The case of NAS signalling connection recovery also includes the cases where the UE was in S1 mode when the RRC connection failure occurred.

For any service request or registration procedure of this kind the UE determines an access category as specified in subclause 4.5.1 and 4.5.2 or 4.5.2A, unless a different access category is specified in the rest of the present subclause.

NOTE 2: Although the access control checking is skipped, the access category is determined for the specific access attempt in order to derive an RRC establishment cause.

There are several services or an MO IMS registration related signalling for which the NAS needs to be informed when the service starts and stops,

- because, while the service is ongoing or the MO IMS registration related signalling is ongoing, the mapping of other access attempts to a specific access category can be affected; and

- in order to avoid double barring at the start of these services or at the start of the MO IMS registration related signalling.

These services are:

a) emergency service;

b) MMTEL voice;

c) MMTEL video;

d) SMSoIP;

e) SMS over NAS;

f) 5GC-MO-LR procedure;

g) UE-requested policy provisioning procedure for V2XP, ProSeP or both; and

h) CIoT user data transfer over the control plane.

The UE considers an emergency service a) as started when 5GMM receives a request from upper layers to register for emergency services or to establish a PDU session with request type = "initial emergency request" or "existing emergency PDU session". It considers the emergency service as stopped when this PDU session is released.

In addition, the UE considers an emergency service a) as started when the 5GMM receives a request from the upper layers to perform emergency services fallback and performs emergency services fallback as specified in subclause 4.13.4.2 of 3GPP TS 23.502 [9]. In this case, the UE considers the emergency service as stopped when:

- the emergency PDU session established during the emergency services fallback is released if the UE has moved to an E-UTRA cell connected to 5GCN; or

- the service request procedure involved in the emergency services fallback is completed otherwise.

While an emergency service a) is ongoing, any access attempt triggered by the initiation of a registration, de-registration or service request procedure or by an uplink user data packet to be sent for an emergency PDU session with suspended user-plane resources is mapped to access category 2 = emergency.

Once the emergency service has successfully passed access control, then as long as the service is ongoing, the following access attempts are allowed to proceed without further access control checking in order to avoid double barring:

- any service request procedure related to the PDU session associated with request type = "initial emergency request" or "existing emergency PDU session"; and

- any uplink user data packet to be sent for a PDU session with suspended user-plane resources associated with request type = "initial emergency request" or "existing emergency PDU session".

NOTE 3: Although the access control checking is skipped, the mapping is performed in order to derive an RRC establishment cause.

For services b) to h) the 5GMM receives explicit start and stop indications from the upper layers.

For the case of handover of ongoing services b) to d) from non-3GPP access, the 5GMM receives an additional explicit handover of ongoing service from non-3GPP access indication from the upper layers.

The 5GMM may receive an additional explicit "call-pull-initiated" indication from the upper layers (see 3GPP TS 24.174 [13D]).

Once the service has successfully passed access control, then as long as the service is ongoing, the following access attempts are allowed to proceed without further access control checking in order to avoid double barring:

- for services b), c) and d):

  1) any service request procedure related to the PDU session established for DNN = "IMS" except between receiving from the lower layers an indication that access barring is applicable for all access categories except categories 0 and 2, or access barring is applicable for all access categories except category 0, and receiving from the lower layers an indication that the barring is alleviated for the access category determined for the access attempt;

  2) any uplink user data packet to be sent for a PDU session with suspended user-plane resources established for DNN = "IMS" except between receiving from the lower layers an indication that access barring is applicable for all access categories except categories 0 and 2, or access barring is applicable for all access categories except category 0, and receiving from the lower layers an indication that the barring is alleviated for the access category determined for the access attempt; and

  3) any start of the MO IMS registration related signalling;

- for service d), if the upper layers have indicated a DNN used for SMSoIP and the indicated DNN used for SMSoIP is different from "IMS":

  1) any service request procedure related to the PDU session established for the DNN used for SMSoIP except between receiving from the lower layers an indication that access barring is applicable for all access categories except categories 0 and 2, or access barring is applicable for all access categories except category 0, and receiving from the lower layers an indication that the barring is alleviated for access category 6; and

  2) any uplink user data packet to be sent for a PDU session with suspended user-plane resources established for the DNN used for SMSoIP except between receiving from the lower layers an indication that access barring is applicable for all access categories except categories 0 and 2, or access barring is applicable for all access category except category 0, and receiving from the lower layers an indication that the barring is alleviated for access category 6.

For the MO IMS registration related signalling, the 5GMM receives explicit start and stop indications from the upper layers.

Once the MO IMS registration related signalling has successfully passed access control, then as long as the MO IMS registration related signalling is ongoing, the following access attempts are allowed to proceed without further access control checking in order to avoid double barring:

1) any service request procedure related to the PDU session established for DNN = "IMS" and for the DNN used for SMSoIP, if the upper layers have indicated a DNN used for SMSoIP and the indicated DNN used for SMSoIP is different from "IMS", except between receiving from the lower layers an indication that access barring is applicable for all access categories except categories 0 and 2, or access barring is applicable for all access categories except category 0 and receiving from the lower layers an indication that the barring is alleviated for the access category determined for the access attempt; and

2) any uplink user data packet to be sent for a PDU session with suspended user-plane resources established for DNN = "IMS" and for the DNN used for SMSoIP except between receiving from the lower layers an indication that access barring is applicable for all access categories except categories 0 and 2, or access barring is applicable for all access categories except category 0 and receiving from the lower layers an indication that the barring is alleviated for the access category determined for the access attempt;

While an MMTEL voice call is ongoing:

- any service request procedure related to the PDU session established for DNN = "IMS" is mapped to access category 4;

- any uplink user data packet to be sent for a PDU session with suspended user-plane resources established for DNN = "IMS" is mapped to access category 4; and

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclause 5.3.1.2 and 5.3.1.4) is mapped to access category 4.

While an MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any service request procedure related to the PDU session established for DNN = "IMS" is mapped to access category 5;

- any uplink user data packet to be sent for a PDU session with suspended user-plane resources established for DNN = "IMS" is mapped to access category 5; and

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclause 5.3.1.2 and 5.3.1.4) is mapped to access category 5.

While an SMSoIP is ongoing, no MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any service request procedure related to the PDU session established:

  1) for DNN = "IMS"; or

  2) for the DNN used for SMSoIP, if the upper layers have indicated a DNN used for SMSoIP and the indicated DNN used for SMSoIP is different from "IMS";

  is mapped to access category 6; and

- any uplink user data packet to be sent for a PDU session with suspended user-plane resources established:

  1) for DNN = "IMS"; or

  2) for the DNN used for SMSoIP, if the upper layers have indicated a DNN used for SMSoIP and the indicated DNN used for SMSoIP is different from "IMS";

  is mapped to access category 6; and

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclause 5.3.1.2 and 5.3.1.4) is mapped to access category 6.

While an SMS over NAS is ongoing, no SMSoIP is ongoing, no MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclause 5.3.1.2 and 5.3.1.4) is mapped to access category 6.

While an MO IMS registration related signalling is ongoing, no SMSoIP is ongoing, no MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any service request procedure related to the PDU session established:

  1) for DNN = "IMS"; and

  2) for the DNN used for SMSoIP, if the upper layers have indicated a DNN used for SMSoIP and the indicated DNN used for SMSoIP is different from "IMS";

  is mapped to access category 9; and

- any uplink user data packet to be sent for a PDU session with suspended user-plane resources established:

  1) for DNN = "IMS"; and

  2) for the DNN used for SMSoIP, if the upper layers have indicated a DNN used for SMSoIP and the indicated DNN used for SMSoIP is different from "IMS";

  is mapped to access category 9; and

- if no SMS over NAS is ongoing, any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclause 5.3.1.2 and 5.3.1.4) is mapped to access category 9.

While a 5GC-MO-LR procedure is ongoing, no SMS over NAS is ongoing, no SMSoIP is ongoing, no MO IMS registration related signalling is ongoing, no MMTEL video call is ongoing, and no MMTEL voice call is ongoing:

- any:

  1) service request procedure; or

2) registration procedure;

initiated in 5GMM-IDLE mode or 5GMM-IDLE mode with suspend indication for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclauses 5.3.1.2 and 5.3.1.4) is mapped to access category 3.

While a UE-requested policy provisioning procedure for V2XP, ProSeP or both (see 3GPP TS 24.587 [19B] and 3GPP TS 24.554 [19E]), no 5GC-MO-LR procedure is ongoing, no SMS over NAS is ongoing, no SMSoIP is ongoing, no MMTEL video call is ongoing, and no MMTEL voice call is ongoing:

- any:

1) service request procedure; or

2) registration procedure;

initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery or following a fallback indication from the lower layers (see subclauses 5.3.1.2 and 5.3.1.4) is mapped to access category 3.

While CIoT user data transfer over the control plane is ongoing, no 5GC-MO-LR procedure is ongoing, no SMS over NAS is ongoing, no SMSoIP is ongoing, no MMTEL video call is ongoing, and no MMTEL voice call is ongoing, any service request procedure initiated in 5GMM-IDLE mode following a fallback indication from the lower layers (see subclause 5.3.1.4) is mapped to access category 7.

NOTE 3: Although the access control checking is skipped, the mapping is performed in order to derive an RRC establishment cause.

If an access category is determined and the access control checking is skipped, the NAS shall determine the RRC establishment cause from one or more determined access identities and the access category as specified in subclause 4.5.6, the NAS shall initiate the procedure to send the initial NAS message for the access attempt and shall provide the RRC establishment cause to lower layers.

If the UE receives from the lower layers an indication that access barring is applicable for all access categories except categories 0 and 2, or access barring is applicable for all access categories except category 0:

a) if an MMTEL voice call or MMTEL video call is ongoing:

1) if the UE is operating in the single-registration mode and the UE's usage setting is "voice centric", the UE may attempt to select an E-UTRA cell connected to EPC. If the UE finds a suitable E-UTRA cell connected to EPC, it then proceeds with the appropriate EMM specific procedures and, if necessary, ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.2 and 3GPP TS 24.301 [15]; and

2) if the UE is operating in the dual-registration mode, the UE may proceed in S1 mode with the appropriate EMM specific procedures and ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.3 and 3GPP TS 24.301 [15]; and

b) if SMSoIP is ongoing or an MO IMS registration related signalling is ongoing:

1) if the UE is operating in the single-registration mode, the UE may attempt to select an E-UTRA cell connected to EPC. If the UE finds a suitable E-UTRA cell connected to EPC, it then proceeds with the appropriate EMM specific procedures and, if necessary, ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.2 and 3GPP TS 24.301 [15]; and

2) if the UE is operating in the dual-registration mode, the UE may proceed in S1 mode with the appropriate EMM specific procedures and ESM procedures to make a PDN connection providing access to IMS available; see subclause 4.8.3 and 3GPP TS 24.301 [15].

4.5.6 Mapping between access categories/access identities and RRC establishment cause

When 5GMM requests the establishment of a NAS-signalling connection, the RRC establishment cause used by the UE shall be selected according to one or more access identities (see subclauses 4.5.2 and 4.5.2A) and the determined access category by checking the rules specified in table 4.5.6.1 and table 4.5.6.2. If the access attempt matches more than one

rule, the RRC establishment cause of the lowest rule number shall be used. If the determined access category is an operator-defined access category, then the RRC establishment cause used by the UE shall be selected according to table 4.5.6.1 and table 4.5.6.2 based on one or more access identities (see subclauses 4.5.2 and 4.5.2A) and the standardized access category determined for the operator-defined access category as described in subclause 4.5.3.

NOTE 1: Following an RRC release with redirection, the lower layers can set the RRC establishment cause or the resume cause to "mps-PriorityAccess" in the case of redirection to an NR cell connected to 5GCN (see 3GPP TS 38.331 [30]) or to "highPriorityAccess" in the case of redirection to an E-UTRA cell connected to 5GCN (see 3GPP TS 36.331 [25A]), if the network indicates to the UE during RRC connection release with redirection that the UE has an active MPS session.

NOTE 2: When the UE is acting as a 5G ProSe layer-2 UE-to-network relay UE, it is possible for the lower layer to decide an applicable RRC establishment cause according to the request from the 5G ProSe layer-2 remote UE or according to the indication from upper layers, including the case when the request from the 5G ProSe layer-2 remote UE is for emergency services, as specified in 3GPP TS 38.331 [30].

Table 4.5.6.1: Mapping table for access identities/access categories and RRC establishment cause when establishing N1 NAS signalling connection via NR connected to 5GCN

Rule #	Access identities	Access categories	RRC establishment cause is set to
1	1	Any category	mps-PriorityAccess
2	2	Any category	mcs-PriorityAccess
3	11, 15	Any category	highPriorityAccess
4	12,13,14,	Any category	highPriorityAccess
5	0	0 (= MT_acc)	mt-Access
		1 (= delay tolerant)	Not applicable (NOTE 1)
		2 (= emergency)	emergency
		3 (= MO_sig)	mo-Signalling
		4 (= MO MMTel voice)	mo-VoiceCall
		5 (= MO MMTel video)	mo-VideoCall
		6 (= MO SMS and SMSoIP)	mo-SMS
		7 (= MO_data)	mo-Data
		9 (= MO IMS registration related signalling)	mo-Data

NOTE 1: A UE using access category 1 for the access barring check will determine a second access category in the range 3 to 7 that is to be used for determination of the RRC establishment cause. See subclause 4.5.2, table 4.5.2.2, NOTE 6.
NOTE 2: See subclause 4.5.2, table 4.5.2.1 for use of the access identities of 0, 1, 2, and 11-15.

Table 4.5.6.2: Mapping table for access identities/access categories and RRC establishment cause when establishing N1 NAS signalling connection via E-UTRA connected to 5GCN

Rule #	Access identities	Access categories	RRC establishment cause is set to
1	1	Any category	highPriorityAccess
2	2	Any category	highPriorityAccess
3	11, 15	Any category	highPriorityAccess
4	12,13,14,	Any category	highPriorityAccess
5	0	0 (= MT_acc)	mt-Access
		1 (= delay tolerant)	Not applicable (NOTE 1)
		2 (= emergency)	emergency
		3 (= MO_sig)	mo-Signalling
		4 (= MO MMTel voice)	mo-VoiceCall
		5 (= MO MMTel video)	mo-VoiceCall
		6 (= MO SMS and SMSoIP)	mo-Data
		7 (= MO_data)	mo-Data
		9 (= MO IMS registration related signalling)	mo-Data
		10 (= MO exception data)	mo-ExceptionData (NOTE 3)

NOTE 1: A UE using access category 1 for the access barring check will determine a second access category in the range 3 to 7 that is to be used for determination of the RRC establishment cause. See subclause 4.5.2, table 4.5.2.2, NOTE 6.
NOTE 2: See subclause 4.5.2, table 4.5.2.1 for use of the access identities of 0, 1, 2, and 11-15.
NOTE 3: This applies to the UE in NB-N1 mode.

4.6 Network slicing

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 S-NSSAIs and NSSAIs are defined in 3GPP TS 23.501 [8]:

a) configured NSSAI;

b) requested NSSAI;

c) allowed NSSAI;

d) subscribed S-NSSAIs;

e) pending NSSAI;

f) alternative S-NSSAIs; and

g) partially allowed NSSAI.

The following S-NSSAIs and 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;

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

e) alternative NSSAI;

f) partially rejected NSSAI;

g) on-demand S-NSSAIs; and

h) on-demand NSSAI.

In roaming scenarios, rejected NSSAI for the current PLMN or SNPN, rejected NSSAI for the current registration area, rejected NSSAI for the maximum number of UEs reached, or partially rejected NSSAI includes one or more S-NSSAIs for the current PLMN and also contains a set of mapped S-NSSAI(s). 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:

a) the configured NSSAI per PLMN;

b) NSSRG information if the UE has indicated that it supports the subscription-based restrictions to simultaneous registration of network slices feature;

c) on-demand NSSAI if the UE has indicated it supports the network slice usage control feature;

d) S-NSSAI time validity information if the UE has indicated that it supports S-NSSAI time validity information; and

e) S-NSSAI location validity information if the UE has indicated that it supports S-NSSAI location validity information.

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. The support for NSSRG information by the UE and the network, respectively, is optional.

NOTE 0: In this version of the specification, the network slice usage control feature is not supported in roaming scenarios.

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 which is neither registering nor registered for onboarding services in SNPN with:

a) a configured NSSAI applicable to the SNPN;

b) NSSRG information if the UE has indicated that it supports the subscription-based restrictions to simultaneous registration of network slices feature;

c) S-NSSAI time validity information if the UE has indicated that it supports S-NSSAI time validity information;

d) on-demand NSSAI if the UE has indicated it supports the network slice usage control feature; and

e) S-NSSAI location validity information if the UE has indicated that it supports S-NSSAI location validity information.

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 support for NSSRG information by the UE and the network, respectively, is optional.

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, the rejected NSSAI for the current registration area, rejected NSSAI for the failed or revoked NSSAA and rejected NSSAI for the maximum number of UEs reached 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 NSSAI that has been in the pending NSSAI, the S-NSSAI will be moved to the allowed NSSAI or rejected NSSAI depending on the outcome of the procedure. The AMF sends the updated allowed NSSAI to the UE over the same access of the requested S-NSSAI. The AMF sends the updated partially allowed NSSAI to the UE only over the 3GPP access. The AMF sends the updated rejected NSSAI over either 3GPP access or non-3GPP access. 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 regardless of the access type. 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 regardless of the access type.

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.

If the UE has indicated that the UE supports network slice replacement feature and the AMF determines to provide the mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI to the UE, the network shall provide the UE with the alternative NSSAI. The alternative NSSAI is managed per access type independently, i.e. 3GPP access or non-3GPP access, and is applicable for the registration area.

If the UE has indicated that the UE supports the partial network slice feature and includes the S-NSSAI(s) in the requested NSSAI, the AMF determines the S-NSSAI(s) to be included in the partially allowed NSSAI or the partially rejected NSSAI as specified in subclause 4.6.2.11. When the AMF provides both the partially allowed NSSAI and the partially rejected NSSAI to the UE, each S-NSSAI shall be either in the partially allowed NSSAI or in the partially rejected NSSAI but not both. The number of S-NSSAIs included in the partially allowed NSSAI or the partially rejected NSSAI shall not exceed 7. The sum of the number of S-NSSAI(s) stored in the partially allowed NSSAI and the allowed NSSAI shall not exceed 8. The partially allowed NSSAI is only applicable to 3GPP access and is applicable for the registration area. The partially rejected NSSAI is only applicable to 3GPP access and is applicable for the 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 at least one 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.

4.6.2 Mobility management aspects

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.

In roaming scenarios, if the mapped S-NSSAI(s) associated to the allowed NSSAI or the configured NSSAI are missing, the UE shall locally set the mapped S-NSSAI to the same value as the received S-NSSAI. Additionally, if the UE receives a Rejected NSSAI IE or an Extended rejected NSSAI IE without associated mapped S-NSSAI(s), and the rejected NSSAI is different from the rejected NSSAI for the failed or revoked NSSAA, the UE shall locally set the mapped S-NSSAI(s) to the same value as the received S-NSSAI.

NOTE 1: The above occurs only when the UE is roaming and the AMF compliant with earlier versions of the specification omits providing to the UE a mapped S-NSSAI for one or more S-NSSAIs in, e.g., the allowed NSSAI or 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.

NOTE 2: If the UE did not receive a mapped S-NSSAI for one or more S-NSSAIs in the allowed NSSAI or configured NSSAI, the UE still uses the S-NSSAI as received from the serving network (i.e., without the locally set mapped S-NSSAI) in any NAS message.

The AMF verifies if the requested NSSAI is permitted based on the subscribed S-NSSAIs in the UE subscription and, in roaming scenarios 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. Additionally, if the AMF allows one or more subscribed S-NSSAIs for the UE, the AMF may include the allowed subscribed S-NSSAI(s) in the allowed NSSAI in the REGISTRATION ACCEPT message. 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 the subscribed 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) all default S-NSSAIs 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).

In roaming scenarios, if the mapped S-NSSAI(s) associated to requested NSSAI are missing, the AMF shall locally set the mapped S-NSSAI to the same value as the received S-NSSAI.

NOTE 3: In roaming scenarios, when the UE is compliant with earlier versions of the specification or when the serving network does not provide a mapped S-NSSAI for one or more S-NSSAIs in the allowed NSSAI or configured NSSAI, the UE can omit a mapped S-NSSAI for one or more S-NSSAIs in requested NSSAI.

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. 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 AMF does not include the allowed NSSAI during a registration procedure with the 5GS registration type IE indicating "mobility registration updating" for the UE in NB-N1 mode, except if the allowed NSSAI has changed for the UE.

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 "SNPN onboarding registration" or during a registration procedure when the UE is registered for onboarding services in SNPN.

The UE considers the last received allowed NSSAI as valid until the UE receives a new allowed NSSAI.

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:

a) associated NSSRG information, the NSSRG information shall also be stored in a non-volatile memory in the ME as specified in annex C;

b) associated NSAG information, the NSAG information shall be stored in the ME;

c) associated S-NSSAI time validity information, the S-NSSAI time validity information shall also be stored in a non-volatile memory in the ME as specified in annex C;

d) associated S-NSSAI location validity information, the S-NSSAI location validity information shall also be stored in a non-volatile memory in the ME as specified in annex C; and

e) associated on-demand NSSAI, the on-demand NSSAI shall also be stored in a non-volatile memory in the ME as specified in annex C.

Each of the configured NSSAI stored in the UE, including the default configured NSSAI, is a set composed of at most 16 S-NSSAIs. Each of the configured NSSAI, except the default configured 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, equivalent SNPNs or both, the selected entry of the "list of subscriber data" or the selected PLMN subscription.

The allowed NSSAI(s) should be stored in a non-volatile memory in the ME as specified in annex C. The partially allowed NSSAI(s) should be stored in a non-volatile memory in the ME as specified in annex C. For an allowed NSSAI, if there is associated alternative NSSAI, the alternative NSSAI should also be stored in a non-volatile memory in the ME as specified in annex C.

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, equivalent SNPNs or both, the selected entry of the "list of subscriber data" or the selected PLMN subscription. Each of the alternative NSSAI stored in the UE is a set composed of at most 8 pairs of S-NSSAI to be replaced and alternative S-NSSAI, 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, equivalent SNPNs or both, the selected

entry of the "list of subscriber data" or the selected PLMN subscription. Each of the partially allowed NSSAI stored in the UE is a set composed of at most 7 S-NSSAIs and a list of TAs for which S-NSSAI is supported, and is associated with a PLMN identity or SNPN identity, 3GPP access type and, if the UE supports access to an SNPN using credentials from a credentials holder, equivalent SNPNs or both, the selected entry of the "list of subscriber data" or the selected PLMN subscription. The sum of number of S-NSSAI(s) stored in the partially allowed NSSAI and the allowed NSSAI shall not exceed 8.

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, equivalent SNPNs or both, the selected entry of the "list of subscriber data" or the selected PLMN subscription.

Each of 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, equivalent SNPNs or both, 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 maximum number of UEs reached are further associated with the access type over which the rejected NSSAI was received. The S-NSSAI(s) in the partially rejected NSSAI are further associated with 3GPP access.

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 and partially 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 partially rejected NSSAI, and stop any timer T3526 associated with a deleted S-NSSAI in the rejected NSSAI for the maximum number of UEs reached if running;

   4A) delete any stored mapped S-NSSAI(s) for the rejected NSSAI; 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 or is in a non-subscribed SNPN);

   If the UE having a stored configured NSSAI for a PLMN ID, 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 and if the number of S-NSSAIs in the configured NSSAI is less than 16;

   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.

aa) The NSAG information shall be stored until:

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

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

The UE shall remove any S-NSSAI from the NSAG information which is not part of the configured NSSAI, if any.

NOTE 1A: If the UE is roaming or the current SNPN is a non-subscribed SNPN, the UE uses the S-NSSAI(s) in the configured NSSAI to compare against any S-NSSAI from the NSAG information.

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

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

The UE shall be able to store 32 NSAG entries in the NSAG information stored for the registered PLMN or the registered SNPN.

The UE shall be able to store TAI lists for up to 4 NSAG entries in the NSAG information stored for the registered PLMN or the registered SNPN.

The UE needs not to store the NSAG information when the UE is switched off or when the UE is deregistered from the registered PLMN or the registered SNPN.

NOTE 1B: The UE stores the NSAG information associated with the configured NSSAI for at least the registered PLMN and its equivalent PLMN(s) or the registered SNPN and its equivalent PLMN(s).

b) The allowed NSSAI shall be stored and the mapped S-NSSAI(s) for the allowed NSSAI (if available) shall be stored for a given PLMN and its equivalent PLMN(s) in the registration area or SNPN 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);

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; or

4) a new partially allowed NSSAI via 3GPP access is received for a given PLMN or SNPN.

b1) The UE shall delete the stored partially allowed NSSAI and stored mapped S-NSSAI(s) for partially allowed NSSAI over 3GPP access when:

1) new partially allowed NSSAI for a PLMN or SNPN is received and the new partially allowed NSSAI does not include any S-NSSAI(s);

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 partially allowed NSSAI.

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 and its equivalent PLMN(s) in the registration area or this SNPN 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 and its equivalent PLMN(s) in the registration area or this SNPN 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, rejected NSSAI for the maximum number of UEs reached and the partially rejected NSSAI, 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 or the partially rejected NSSAI is associated with one or more S-NSSAI(s) in the stored mapped rejected NSSAI or the stored mapped partially rejected NSSAI, and at least one of these mapped S-NSSAI(s) is not included in the mapped S-NSSAI(s) for the new allowed NSSAI, and stop any timer T3526 associated with a deleted S-NSSAI in the rejected 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 (if the UE is not roaming) or the current SNPN (if the SNPN is the subscribed SNPN) or the mapped S-NSSAI(s) for the new allowed NSSAI for the current PLMN (if the UE is roaming) or the current SNPN (if the SNPN is a non-subscribed SNPN);

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, the stored mapped S-NSSAI(s) for the partially rejected NSSAI and the mapped S-NSSAI(s) for the 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 (if the UE is roaming) or the current SNPN (if the SNPN is a non-subscribed SNPN), and stop any timer T3526 associated with a deleted S-NSSAI in the rejected NSSAI for the maximum number of UEs reached if running; and

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

NOTE 2: 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.

The network may provide to the UE the partially allowed NSSAI. When a new partially allowed NSSAI for a PLMN or SNPN is received and the new partially allowed NSSAI includes one or more S-NSSAI(s), the UE shall:

1) replace any stored partially allowed NSSAI for this PLMN and its equivalent PLMN(s) in the registration area or this SNPN via the 3GPP access with the new partially allowed NSSAI for this PLMN or SNPN;

2) delete any stored mapped S-NSSAI(s) for the partially allowed NSSAI for this PLMN and its equivalent PLMN(s) in the registration area or this SNPN for the 3GPP access type and, if available, store the mapped S-NSSAI(s) for the new partially allowed NSSAI;

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

the SNPN is the subscribed SNPN) or the mapped S-NSSAI(s) for the new partially allowed NSSAI for the current PLMN (if the UE is roaming) or the current SNPN (if the SNPN is a non-subscribed SNPN);

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, the stored mapped S-NSSAI(s) for the partially rejected NSSAI and the mapped S-NSSAI(s) for the 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 partially allowed NSSAI for the current PLMN (if the UE is roaming) or the current SNPN (if the SNPN is a non-subscribed SNPN), and stop any timer T3526 associated with a deleted S-NSSAI in the rejected NSSAI for the maximum number of UEs reached if running; and

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

ba) The alternative NSSAI and the mapped S-NSSAI(s) for the alternative NSSAI (if the UE is roaming) shall be stored for a given PLMN and its equivalent PLMN(s) or SNPN until a new alternative NSSAI for the same access type (i.e. 3GPP access or non-3GPP access) is received for a given PLMN or SNPN.

When a new alternative NSSAI for a given PLMN or SNPN is received and the new alternative NSSAI includes a list of mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI, the UE shall:

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

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

When a new alternative NSSAI for a given PLMN or SNPN is received and the new alternative NSSAI does not include any mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI, the UE shall delete any stored alternative NSSAI for this PLMN and its equivalent PLMN(s) or this SNPN for the same access type.

When the UE locally removes either the replaced S-NSSAI or the alternative S-NSSAI in the allowed NSSAI upon expiry of the associated slice deregistration inactivity timer, the UE shall delete the entry including the replaced S-NSSAI or the alternative S-NSSAI stored in the alternative NSSAI.

NOTE 3: Whether the UE stores the alternative NSSAI and the mapped S-NSSAI(s) for the alternative 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, or the partially rejected NSSAI in the REGISTRATION ACCEPT message or 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, or if the UE receives the S-NSSAI(s) included in the Partially rejected NSSAI IE in non-roaming case when not in SNPN access operation mode or in the subscribed SNPN, remove from the stored allowed NSSAI or partially allowed NSSAI for the current PLMN and its equivalent PLMN(s) in the registration area or the current SNPN, 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) rejected NSSAI for the current PLMN or SNPN, for each and every access type;

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

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

v) partially rejected NSSAI, associated with 3GPP access;

3) if the UE receives the S-NSSAI(s) included in the Extended rejected NSSAI IE or if the UE receives the S-NSSAI(s) included in the Partially rejected NSSAI IE in roaming case or in a non-subscribed SNPN, remove from the stored allowed NSSAI or partially allowed NSSAI for the current PLMN and its equivalent PLMN(s) in the registration area or the current SNPN, 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;

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

iv) partially rejected NSSAI, associated with 3GPP access;

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

4) remove from the stored mapped S-NSSAI(s) for the allowed NSSAI or partially allowed NSSAI (if available and if the UE is roaming or is a non-subscribed SNPN), 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;

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

v) partially rejected NSSAI, associated with 3GPP access;

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 when not in SNPN access operation mode or in the subscribed SNPN, remove from the stored pending NSSAI for the current PLMN and its equivalent PLMN(s) in the registration area or the current SNPN, 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) rejected NSSAI for the current PLMN or SNPN, for each and every access type;

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

iv) 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 or in a non-subscribed SNPN, remove from the stored pending NSSAI for the current PLMN and its equivalent PLMN(s) in the registration area or the current SNPN, 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 mapped S-NSSAI(s) for the pending NSSAI (if available and if the UE is roaming or is in a non-subscribed SNPN), 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;

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 and partially 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 a new SNPN;

3) enters state 5GMM-DEREGISTERED following an unsuccessful registration with a new PLMN or a new SNPN; 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 PLMN or SNPN, which provided the rejected NSSAI, 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 receives 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 6.5.1.3 of 3GPP TS 24.301 [15]), the UE shall remove the S-NSSAI associated with the PLMN ID from the rejected NSSAI for the current PLMN. When the UE receives 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 6.5.1.3 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 and the partially rejected NSSAI shall be deleted. When a new partially rejected NSSAI is received without any S-NSSAI(s), the UE shall delete any stored partially rejected NSSAI for the current registration area;

d) When the UE receives the pending NSSAI in the REGISTRATION ACCEPT 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 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 and its equivalent PLMN(s) in the registration area or this SNPN.

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 not in the list of equivalent PLMNs or a new SNPN;

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 PLMN or SNPN, which provided pending NSSAI, over another access, the pending NSSAI for the current PLMN and its equivalent PLMN(s) in the registration area or the current SNPN 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 any timer T3526 associated with a deleted S-NSSAI in the rejected 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);

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; and

g) When the UE receives the on-demand NSSAI in the REGISTRATION ACCEPT message or CONFIGURATION UPDATE COMMAND message, the UE shall replace any stored on-demand NSSAI for the serving PLMN with the new on-demand NSSAI.

4.6.2.3 Provision of NSSAI to lower layers in 5GMM-IDLE mode

The UE NAS layer may provide the lower layers with an NSSAI (either requested NSSAI or allowed NSSAI) when the UE in 5GMM-IDLE mode sends an initial NAS message.

The AMF may indicate, via the NSSAI inclusion mode IE of a REGISTRATION ACCEPT message, an NSSAI inclusion mode in which the UE shall operate over the current access within the current PLMN or SNPN, if any (see subclauses 5.5.1.2.4 and 5.5.1.3.4), where the NSSAI inclusion mode is chosen among the following NSSAI inclusion modes described in table 4.6.2.3.1.

Table 4.6.2.3.1: NSSAI inclusion modes and NSSAI which shall be provided to the lower layers

Initial NAS message	NSSAI inclusion mode A	NSSAI inclusion mode B	NSSAI inclusion mode C	NSSAI inclusion mode D
REGISTRATION REQUEST message: i) including the 5GS registration type IE set to "initial registration"	Requested NSSAI, if any	Requested NSSAI, if any	Requested NSSAI, if any	No NSSAI
REGISTRATION REQUEST message: i) including the 5GS registration type IE set to "mobility registration updating"; and ii) initiated by case other than case g) or n) in subclause 5.5.1.3.2	Requested NSSAI, if any	Requested NSSAI, if any	Requested NSSAI, if any	No NSSAI
REGISTRATION REQUEST message: i) including the 5GS registration type IE set to "mobility registration updating"; and ii) initiated by case g) or n) in subclause 5.5.1.3.2	Allowed NSSAI, and partially allowed NSSAI, if any	Allowed NSSAI, and partially allowed NSSAI, if any	No NSSAI	No NSSAI
REGISTRATION REQUEST message: i) including the 5GS registration type IE set to "periodic registration updating"	Allowed NSSAI, and partially allowed NSSAI, if any	Allowed NSSAI, and partially allowed NSSAI, if any	No NSSAI	No NSSAI
SERVICE REQUEST message	Allowed NSSAI, and partially allowed NSSAI, if any	See NOTE 1	No NSSAI	No NSSAI

NOTE 1: All the S-NSSAIs of the PDU sessions that have the user-plane resources requested to be re-established by the service request procedure or the S-NSSAIs of a control plane interaction triggering the service request is related to (see 3GPP TS 23.501 [8])

NOTE 2: For a REGISTRATION REQUEST message which is triggered by emergency services, a DEREGISTRATION REQUEST message, and a SERVICE REQUEST message which is triggered by emergency services (e.g. a SERVICE REQUEST message includes the service type IE set to "emergency services" or "emergency services fallback", a SERVICE REQUEST message triggered for emergency services includes the service type IE set to “high priority access” as specified in subclause 5.6.1.2.1), no NSSAI is provided to the lower layers. If the UE performs initial registration for onboarding services in SNPN or is registered for onboarding services in SNPN, the UE NAS layer shall not provide the lower layers with an NSSAI.

NOTE 3: The mapped configured S-NSSAI(s) from the S-NSSAI(s) of the HPLMN are not included as part of the S-NSSAIs in the requested NSSAI or the allowed NSSAI when it is provided to the lower layers.

The UE shall store the NSSAI inclusion mode:

a) indicated by the AMF, if the AMF included the NSSAI inclusion mode IE in the REGISTRATION ACCEPT message; or

b) if the AMF did not include the NSSAI inclusion mode IE in the REGISTRATION ACCEPT message:

   1) if the UE is pre-configured by operator to operate by default to according to mode C in the HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present), (see the DefaultNSSAIInclusionMode leaf of the NAS configuration MO in 3GPP TS 24.368 [17] or the USIM file $EF_{NASCONFIG}$ in 3GPP TS 31.102 [22]), then mode C;

   2) otherwise:

      i) mode D for 3GPP access and trusted non-3GPP access; or

      ii) mode B for untrusted non-3GPP access and wireline access.

together with the identity of the current PLMN or SNPN and access type in a non-volatile memory in the ME as specified in annex C.

The UE shall apply the NSSAI inclusion mode received in the REGISTRATION ACCEPT message over the current access within the current PLMN and its equivalent PLMN(s), if any, or the current SNPN in the current registration area.

When a UE performs a registration procedure to a PLMN which is not a PLMN in the current registration area or an SNPN, if the UE has no NSSAI inclusion mode for the PLMN or the SNPN stored in a non-volatile memory in the ME, the UE shall provide the lower layers with:

a) no NSSAI if the UE is performing the registration procedure over 3GPP access; or

b) requested NSSAI if the UE is performing the registration procedure over non-3GPP access.

When a UE performs a registration procedure after an inter-system change from S1 mode to N1 mode, if the UE has no NSSAI inclusion mode for the PLMN stored in a non-volatile memory in the ME and the registration procedure is performed over 3GPP access, the UE shall not provide the lower layers with any NSSAI over the 3GPP access.

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 the subscribed 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. The AMF informs the UE about S-NSSAI(s) for which NSSAA procedure is completed as success in the allowed NSSAI or in the partially allowed NSSAI. The AMF informs the UE about S-NSSAI(s) for which NSSAA procedure is completed as failure in the rejected NSSAI for the failed or revoked NSSAA. The AMF stores and handles allowed NSSAI, partially 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 partially allowed NSSAI and the rejected 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 AMF shall also include in the REGISTRATION ACCEPT message the partially allowed NSSAI containing one or more S-NSSAIs from the requested NSSAI which are allowed by the AMF in a list of TAs within the current registration area and for which network slice-specific authentication and authorization is not required, if any.

The network slice-specific re-authentication and re-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 re-authentication and re-authorization fails or network slice-specific authorization is revoked for some but not all S-NSSAIs in the allowed NSSAI or the partially allowed NSSAI,, the AMF updates the allowed NSSAI or the partially 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 re-authentication and re-authorization fails or network slice-specific authorization is revoked for all S-NSSAIs in the allowed NSSAI or the partially 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 or the partially 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 re-authentication and re-authorization fails or network slice-specific authorization is revoked for all S-NSSAIs in the allowed NSSAI or the partially allowed NSSAI and all default S-NSSAIs are subject to network slice-specific authentication and authorization, and the network slice-specific authentication and authorization has not been successfully performed for any of these default S-NSSAIs, 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 or the partially allowed NSSAI, if the UE still wants to use the S-NSSAI(s) from the allowed NSSAI or the partially 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 re-authentication and re-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 or for an S-NSSAI that is in the current partially allowed NSSAI for 3GPP access type, the AMF shall:

a) provide a new allowed NSSAI or a new partially 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.

4.6.2.5 Mobility management based network slice admission control

A serving PLMN or SNPN can perform network slice admission control for the S-NSSAI(s) subject to NSAC to monitor and control the number of registered UEs per network slice. The timing of the network slice admission control is managed by the EAC mode per network slice, which can be either activated or deactivated for the network performing network slice admission control. The EAC mode is activated when the number of UEs associated with the S-NSSAI reaches a certain threshold (see 3GPP TS 23.502 [9])

If the EAC mode is activated for an S-NSSAI, the AMF performs network slice admission control before the S-NSSAI subject to NSAC is included in the allowed NSSAI or the partially allowed NSSAI sent to the UE. During a registration procedure (including initial registration or mobility registration updating from another AMF), if the AMF determines that the maximum number of UEs has been reached for:

a) one or more S-NSSAIs but not all S-NSSAIs in the requested NSSAI, then the AMF includes the allowed NSSAI or the partially allowed NSSAI and the rejected NSSAI accordingly in the REGISTRATION ACCEPT message as specified in the subclauses 5.5.1.2.4 and 5.5.1.3.4;

b) all S-NSSAIs in the requested NSSAI but there are one or more default S-NSSAIs which can be allowed to the UE, then the AMF includes the allowed NSSAI or the partially allowed NSSAI containing these default S-NSSAIs and the rejected NSSAI accordingly in the REGISTRATION ACCEPT message as specified in the subclauses 5.5.1.2.4 and 5.5.1.3.4; or

c) all S-NSSAIs in the requested NSSAI and there are no default S-NSSAIs which can be allowed to the UE, then the AMF includes the rejected NSSAI accordingly in the REGISTRATION REJECT message as specified in the subclauses 5.5.1.2.5 and 5.5.1.3.5.

If the EAC mode is deactivated for an S-NSSAI, the AMF performs network slice admission control after the S-NSSAI subject to NSAC is included in the allowed NSSAI or the partially allowed NSSAI sent to the UE. While the AMF is waiting for response from the NSACF for the S-NSSAI, the AMF processes the NAS signalling message related to the S-NSSAI as usual i.e. like S-NSSAI in the allowed NSSAI or the partially allowed NSSAI. After the network performs the network slice admission control, if the AMF determines that the maximum number of UEs has been reached for:

a) one or more S-NSSAIs but not all S-NSSAIs in the allowed NSSAI or the partially allowed NSSAI, then the AMF updates the allowed NSSAI or the partially allowed NSSAI and the rejected NSSAI accordingly using the generic UE configuration update procedure as specified in the subclause 5.4.4;

b) for all S-NSSAIs in the allowed NSSAI or the partially allowed NSSAI but there are one or more default S-NSSAIs which can be allowed to the UE, then the AMF updates the allowed NSSAI or the partially 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; or

c) for all S-NSSAIs in the allowed NSSAI or the partially allowed NSSAI and there are no default S-NSSAIs which can be allowed to the UE, then the 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.

When the UE has an emergency PDU session established or the UE is establishing an emergency PDU session, the AMF updates the rejected NSSAI using the generic UE configuration update procedure as specified in the subclause 5.4.4 and informs the SMF to release all PDU sessions associated with the S-NSSAI. During the generic UE configuration update procedure, the AMF includes the 5GS registration result IE in the CONFIGURATION UPDATE COMMAND message and sets the Emergency registered bit of the 5GS registration result IE to "Registered for emergency services". 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.

Based on operator policy, the mobility management based network slice admission control is not applicable for the S-NSSAI used for emergency services, or the mobility management based network slice admission control result is ignored for the S-NSSAI used for emergency services.

Based on operator policy, the mobility management based network slice admission control is not applicable for the UEs configured for priority services, or the mobility management based network slice admission control result is ignored for the UEs configured for priority services.

NOTE: A UE configured for priority services can be identified based on the RRC establishment cause received from the NG-RAN or based on the MPS priority information in the user's subscription context obtained from the UDM.

The mobility management based network slice admission control is not applicable to a UE that is registering or registered for onboarding services in SNPN.

4.6.2.6 Provision of NSAG information to lower layers

The support for NSAG information by the UE and the network, respectively, is optional. The NSAG information provided by the network and stored in the UE includes a list of NSAGs each of which contains:

a) an NSAG ID;

b) a list of S-NSSAI(s), which are associated with the NSAG and shall be part of the configured NSSAI;

NOTE 0: An alternative S-NSSAI is added to the configured NSSAI if not included yet.

c) a priority value that is associated with the NSAG; and

NOTE 1: The AMF can take local configuration, UE 5GMM capabilities, subscribed S-NSSAIs, the mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI, HPLMN, etc. to determine the NSAG priority information for the associated NSAG to a UE.

d) optionally a list of TAIs in which the NSAG is valid. If it is not provided by the network, the NSAG is valid in the PLMN or SNPN which has sent the NSAG information and its equivalent PLMN(s).

NOTE 2: If the NSAG for the PLMN and its equivalent PLMN(s) have different associations with S-NSSAIs, then the AMF includes a list of TAIs in the NSAG information.

The UE NAS layer shall provide the lower layers with:

a) the most recent NSAG information stored in the UE (see subclause 4.6.2.2);

b) the allowed NSSAI and the partially allowed NSSAI (if any) or the requested NSSAI for the purpose of network slice-based cell reselection (see 3GPP TS 23.501 [8]); and

c) zero or more S-NSSAIs related to an access attempt for the purpose of network slice-based random access, when the access attempt is made by the UE in 5GMM-IDLE mode or 5GMM-CONNECTED mode with RRC inactive indication, determined as follows:

   i) requested NSSAI (if any), if an access attempt occurred due to the REGISTRATION REQUEST message;

   ii) NSSAI(s) associated with all the PDU sessions included in the Uplink data status IE (if any), PDU session status IE (if any), or Allowed PDU session status IE (if any), if an access attempt occurred due to the SERVICE REQUEST message or CONTROL PLANE SERVICE REQUEST message;

iii) the S-NSSAI associated with the PDU session, if an access attempt occurred due to:

- an uplink user data packet to be sent for a PDU session with suspended user-plane resources;
- an UL NAS TRANSPORT which carries a 5GSM message for a PDU session associated with an S-NSSAI (if any); or
- CIoT user data to be sent in a CONTROL PLANE SERVICE REQUEST message or an UL NAS TRANSPORT message;

iv) no S-NSSAI, if an access attempt occurred due to:

- the deregistration procedure;
- a PDU session establishment request not associated with an S-NSSAI;
- the service request procedure for the UE-initiated NAS transport procedure for sending SMS, LPP message, UPP-CMI container, SLPP message, SOR transparent container, UE policy container, UE parameters update transparent container, or a location services message; or
- emergency services; or

v) the allowed NSSAI (if any) and the partially allowed NSSAI (if any), if an access attempt occurred for other reason than those specified in bullets i) - iv).

4.6.2.7 Mobility management based network slice replacement

The support for network slice replacement by a UE or network is optional. If the UE and network support network slice replacement, and the AMF determines that an S-NSSAI included in the allowed NSSAI needs to be replaced with an alternative S-NSSAI, the AMF provides:

a) the alternative S-NSSAI in the allowed NSSAI, if not included yet;

b) the alternative S-NSSAI in the configured NSSAI, if not included yet;

c) the alternative S-NSSAI in the NSAG information, if not included yet and the UE supports NSAG; and

d) the alternative NSSAI including the mapping information between the S-NSSAI to be replaced and the corresponding alternative S-NSSAI,

to the UE, during the generic UE configuration update procedure or during the registration procedure as follows:

a) for non-roaming UE, the AMF provides the mapping information between the S-NSSAI included in the allowed NSSAI and the alternative S-NSSAI to the UE; or

NOTE 1: In non-roaming scenarios, the alternative S-NSSAI does not have to be part of the subscribed S-NSSAI(s) in the UE subscription.

b) for roaming UE:

1) if the S-NSSAI included in the allowed NSSAI needs to be replaced (i.e., the S-NSSAI to be replaced is part of the VPLMN S-NSSAIs), the AMF provides the mapping information between the S-NSSAI included in the allowed NSSAI and the alternative S-NSSAI to the UE; and

2) if the S-NSSAI included in the mapped S-NSSAI(s) for the allowed NSSAI needs to be replaced (i.e., the S-NSSAI to be replaced is part of the HPLMN S-NSSAIs), the AMF provides the mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI to the UE.

NOTE 1A: In roaming scenarios, the alternative S-NSSAI, being part of the HPLMN S-NSSAIs does not have to be part of the subscribed S-NSSAI(s) in the UE subscription.

NOTE 2: It is up to AMF local policy to determine when to provide the mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI to the UE, which can be either when the alternative S-NSSAI is available and there is no established PDU session associated with the S-NSSAI to be replaced, or when the UE has established the first PDU session associated with the S-NSSAI to be replaced.

If the requested NSSAI contains alternative S-NSSAI(s) that are not subscribed S-NSSAI(s), the AMF shall verify the alternative S-NSSAI(s) based on the stored alternative NSSAI.

If the alternative S-NSSAI is subject to NSSAA, the alternative S-NSSAI provided by AMF shall be part of the subscribed S-NSSAI(s) in the UE subscription. The AMF shall perform NSSAA procedure for such alternative S-NSSAI and perform network slice replacement as specified above after the NSSAA procedure for the alternative S-NSSAI is completed as success.

If re-NSSAA procedure is ongoing for the S-NSSAI to be replaced, the AMF shall continue with the re-NSSAA procedure and perform network slice replacement as specified above after the re-NSSAA procedure for the S-NSSAI to be replaced is completed as success.

NOTE 2A: When configuring the alternative S-NSSAI, the maximum number of S-NSSAIs defined for the allowed NSSAI and configured NSSAI in subclause 4.6.2.2 are applicable.

If the AMF determines that the replaced S-NSSAI is available again, the AMF provides the updated alternative NSSAI excluding the replaced S-NSSAI and the corresponding alternative S-NSSAI to the UE during the UE configuration update procedure or during the registration procedure.

If all the replaced S-NSSAI(s) in alternative NSSAI are available again, the AMF provides the alternative NSSAI with Length of Alternative NSSAI contents set to 0 in the UE configuration update procedure or registration procedure.

NOTE 3: If there is S-NSSAI location validity information for both the S-NSSAI to be replaced and the alternative S-NSSAI, the NS-AoS of the alternative S-NSSAI is the same as or larger than the NS-AoS of the S-NSSAI to be replaced.

If the UE is in a cell outside the NS-AoS of the replaced S-NSSAI but within the NS-AoS of the alternative S-NSSAI, the AMF provides the updated allowed NSSAI and partially allowed NSSAI excluding the replaced S-NSSAI, if included, in the allowed NSSAI or partially allowed NSSAI during the UE configuration update procedure or during the registration procedure.

If the alternative S-NSSAI is not part of the subscribed S-NSSAI(s), and:

a) the replaced S-NSSAI is removed from the allowed NSSAI or the partially allowed NSSAI; or

b) the replaced S-NSSAI is available again,

then the AMF shall provide updated allowed NSSAI or partially allowed NSSAI excluding the alternative S-NSSAI to the UE over the current access type during the UE configuration update procedure or during the registration procedure. Additionally, if the alternative S-NSSAI is not included in allowed NSSAI or partially allowed NSSAI over the other access type:

a) for case a), the AMF may also provide updated configured NSSAI excluding the alternative S-NSSAI to the UE during the UE configuration update procedure or during the registration procedure; or

b) for case b), the AMF shall also provide updated configured NSSAI excluding the alternative S-NSSAI to the UE during the UE configuration update procedure or during the registration procedure.

Based on SMF local configuration, if the replaced S-NSSAI is subject to NSAC or the alternative S-NSSAI is subject to NSAC or both, the SMF may perform NSAC for the replaced S-NSSAI or the alternative S-NSSAI or both.

4.6.2.8 Mobility management for optimised handling of temporarily available network slices

The UE and the network may support optimised handling of temporarily available network slices. The support for S-NSSAI time validity information by the UE and the network, respectively, is optional.

If the UE has indicated that it supports S-NSSAI time validity information, then the AMF may include the S-NSSAI time validity information for one or more S-NSSAIs included in the configured NSSAI in the REGISTRATION ACCEPT message or the CONFIGURATION UPDATE COMMAND message. If the AMF determines that the S-NSSAI time validity information for an S-NSSAI in the configured NSSAI is changed, the AMF may provide the UE with a new S-NSSAI time validity information for that S-NSSAI via the CONFIGURATION UPDATE COMMAND message.

If the UE supporting S-NSSAI time validity information, is configured with S-NSSAI time validity information for an S-NSSAI and:

a) the S-NSSAI time validity information indicates that the S-NSSAI is available, then the UE may request the S-NSSAI in the requested NSSAI in the Registration Request message;

b) the S-NSSAI time validity information indicates that the S-NSSAI is not available, then:

   i) the UE shall not include the S-NSSAI in the requested NSSAI in the REGISTRATION REQUEST message;

   ii) the UE shall remove the S-NSSAI from the stored allowed NSSAI (if any) and the stored partially allowed NSSAI (if any) in the non-volatile memory in the ME, as specified in annex C; and

   iii) the S-NSSAI time validity information indicates that the S-NSSAI will not become available again, then the UE shall remove the S-NSSAI from the stored configured NSSAI in the non-volatile memory in the ME, as specified in annex C.

NOTE 1: If the S-NSSAI to be removed is the only S-NSSAI in the allowed NSSAI and partially allowed NSSAI, if applicable, the UE can before the time validity expiry initiate the registration procedure for mobility and periodic registration update and include a different S-NSSAI from the configured NSSAI in the Requested NSSAI IE of the REGISTRATION REQUEST message. If the UE does not initiate the registration procedure for mobility and periodic registration update and the time validity for the only S-NSSAI in the allowed NSSAI and partially allowed NSSAI expires, the UE locally enters the state 5GMM-DEREGISTERED.

When the S-NSSAI time validity information of an S-NSSAI indicates that the S-NSSAI is not available, then:

a) if the AMF receives a requested NSSAI in the REGISTRATION REQUEST message with the S-NSSAI identifying the network slice, the AMF shall:

   i) to a UE which has indicated that it supports S-NSSAI time validity information, provide:

      1) a configured NSSAI including the S-NSSAI together with the S-NSSAI time validity information in the REGISTRATION ACCEPT message if the S-NSSAI will become available again; or

      2) a configured NSSAI not including the S-NSSAI in the REGISTRATION ACCEPT message if the S-NSSAI will not become available again; or

   ii) to a UE which has not indicated that it supports S-NSSAI time validity information, reject the S-NSSAI for the current PLMN or SNPN. If the registration request is accepted, the AMF shall include a configured NSSAI not including the S-NSSAI;

b) if the AMF detects that the S-NSSAI is included in the allowed NSSAI or the partially allowed NSSAI of a UE which has:

   i) indicated that it supports S-NSSAI time validity information, the AMF shall locally remove the S-NSSAI from the allowed NSSAI (if any) and the partially allowed NSSAI (if any); or

NOTE 2: If there is no S-NSSAI included in the allowed NSSAI and partially allowed NSSAI after local removal of the S-NSSAI from the allowed NSSAI or the partially allowed NSSAI, the network locally enters the state 5GMM-DEREGISTERED for the UE.

   ii) not indicated that it supports S-NSSAI time validity information, the AMF shall remove the S-NSSAI from the stored configured NSSAI (if any), allowed NSSAI (if any), and partially allowed NSSAI (if any) by sending the CONFIGURATION UPDATE COMMAND message.

When the S-NSSAI time validity information of an S-NSSAI indicates that the S-NSSAI becomes available again, the AMF shall update the configured NSSAI including the S-NSSAI to a UE which has not indicated that it supports S-NSSAI time validity information by sending CONFIGURATION UPDATE COMMAND message if the UE is subscribed to the S-NSSAI.

The S-NSSAI time validity information is applicable for the current PLMN or SNPN regardless of the access type.

4.6.2.9 Mobility management based network slice usage control

If the network supports network slice usage control, the AMF monitors network slice usage by running a slice deregistration inactivity timer per S-NSSAI and access type. If the UE supports network slice usage control, the AMF may also provide on-demand NSSAI to the UE in the REGISTRATION ACCEPT message or in the CONFIGURATION UPDATE COMMAND message. The on-demand NSSAI consists of one or more on-demand S-NSSAIs and, optionally, the slice deregistration inactivity timer per on-demand S-NSSAI.

The slice deregistration inactivity timer is started using the stored slice deregistration inactivity timer value as follows:

a) for a PDU session which is released using 5GSM signalling, after a PDU session is released and there is no established PDU session, including any MA PDU session, associated with the S-NSSAI over the corresponding access type;

b) for a PDU session which is released locally:

   1) when the UE or AMF indicates via the PDU session status IE that a PDU session is now in 5GSM state PDU SESSION INACTIVE and there is no established PDU session, including any MA PDU session, associated with the S-NSSAI over the corresponding access type; or

   2) when the UE or AMF receives the the PDU session status IE for which a PDU session that was previously in 5GSM state PDU SESSION ACTIVE is now indicated as being in 5GSM state PDU SESSION INACTIVE and there is no established PDU session, including any MA PDU session, associated with the S-NSSAI over the corresponding access type; or

c) when there is no established PDU session, including any MA PDU session, associated with the S-NSSAI included in the allowed NSSAI or in the partially allowed NSSAI over the corresponding access type.

The slice deregistration inactivity timer is stopped and reset:

a) when at least a PDU session, including any MA PDU session, associated with the S-NSSAI is successfully established over the corresponding access type(s) or the S-NSSAI is removed from the allowed NSSAI or the partially allowed NSSAI; or

b) when the UE enters the state 5GMM-DEREGISTERED.

If the slice deregistration inactivity timer value is updated, the AMF updates the stored timer value and may provide the updated timer value to the UE in the REGISTRATION ACCEPT message, in a current or the next registration procedure for mobility and periodic registration update, or the CONFIGURATION UPDATE COMMAND message.

When the UE receives an updated slice deregistration inactivity timer value in the REGISTRATION ACCEPT message or the CONFIGURATION UPDATE COMMAND message from the AMF, the UE shall update the stored timer value.

Upon expiry of the slice deregistration inactivity timer, the AMF:

a) for UE supporting network slice usage control, shall locally remove the S-NSSAI from the allowed NSSAI over the corresponding access type. In addition, the AMF may send the CONFIGURATION UPDATE COMMAND message to the UE with the new allowed NSSAI; and

b) for UE not supporting network slice usage control, shall provide the updated allowed NSSAI excluding the S-NSSAI in the CONFIGURATION UPDATE COMMAND message to the UE.

If the AMF locally removes either the replaced S-NSSAI or the alternative S-NSSAI in the allowed NSSAI upon expiry of the associated slice deregistration inactivity timer, the AMF shall delete the entry including the replaced S-NSSAI or the alternative S-NSSAI stored in the alternative NSSAI.

The UE includes the on-demand S-NSSAI which the UE requests in the requested NSSAI during the registration procedure. Upon expiry of the slice deregistration inactivity timer, the UE shall locally remove the S-NSSAI from the allowed NSSAI over the corresponding access type. If the locally removed on-demand S-NSSAI is included in the entry of the stored alternative NSSAI, the UE shall delete the entry as specified in subclause 4.6.2.2.

NOTE 0: If the UE determines the on-demand S-NSSAI for a PDU session establishment as specified in subclause 4.2.2 of 3GPP TS 24.526 [19], the UE includes the on-demand S-NSSAI in the requested NSSAI during the registration procedure.

On-demand NSSAI is associated with the configured NSSAI. The on-demand S-NSSAI(s) is deleted by the UE from the stored on-demand NSSAI, when the associated configured S-NSSAI(s) is deleted by the UE from the stored configured NSSAI.

NOTE 1: Based on regulatory requirements and operator policy, the AMF ensures that the network slice usage control does not apply for the S-NSSAI used for emergency services.

NOTE 2: In this version of the specification, the network slice usage control feature is not supported in roaming scenarios.

4.6.2.10 Mobility management aspects of handling network slices with NS-AoS not matching deployed tracking areas

An operator can choose to let the NS-AoS of an S-NSSAI not match the existing tracking area boundaries (see subclause 5.15.18 of 3GPP TS 23.501 [8]). In order to support this deployment option, the operator has to ensure that an AMF covering the NS-AoS operates as described below.

The support for S-NSSAI location validity information by the UE and the network, respectively, is optional. If a UE supports S-NSSAI location validity information, the UE indicates that it supports S-NSSAI location validity information during the registration procedure (see subclause 5.5.1). The AMF can provide a UE which has indicated that it supports S-NSSAI location validity information with S-NSSAI location validity information (see subclauses 5.4.4 and 5.5.1). The S-NSSAI location validity information consists of, for each of the applicable S-NSSAI(s) in the configured NSSAI:

a) an S-NSSAI; and

b) a list of cell identities of TA(s) belonging to the registration area where the related S-NSSAI(s) is available in some cells but not all cells of one or more TAs, which represents the NS-AoS of the S-NSSAI.

The UE shall consider itself to be inside the NS-AoS if the cell identity of the current serving cell matches any of the identities in the S-NSSAI location validity information. Otherwise, the UE shall consider itself to be outside the NS-AoS of an S-NSSAI.

NOTE 1: The cell identity of the current serving cell is received from the lower layers.

For an S-NSSAI in the S-NSSAI location validity information, even if the S-NSSAI is included in the rejected NSSAI with a rejection cause value set to "S-NSSAI not available in the current registration area" or is included in the partially rejected NSSAI, the UE is allowed to request the S-NSSAI if the UE determines that it is inside the NS-AoS of the S-NSSAI.

For an S-NSSAI limited by NS-AoS, if the UE in 5GMM-CONNECTED mode does not support S-NSSAI location validity information and the AMF determines that:

a) the UE is outside the NS-AoS, then the AMF may:

   1) provide the UE with an allowed NSSAI or a partially allowed NSSAI excluding the S-NSSAI, and optionally a configured NSSAI excluding the S-NSSAI; and

NOTE 2: If excluding the S-NSSAI limited by NS-AoS results in an empty allowed NSSAI or partially allowed NSSAI, the AMF includes one or more default S-NSSAIs in the provided allowed NSSAI or partially allowed NSSAI.

   2) indicate to the SMF to release all PDU sessions associated with the S-NSSAI; or

b) the UE is in the NS-AoS, then the AMF may update the configured NSSAI to include the S-NSSAI in the configured NSSAI.

If the UE that does not support S-NSSAI location validity information requests a PDU session establishment for an S-NSSAI limited by NS-AoS and the AMF determines that the UE is outside the NS-AoS of an S-NSSAI, the AMF may perform S-NSSAI based congestion control for the S-NSSAI as specified in subclauses 5.3.11 and 5.4.5.

The S-NSSAI location validity information is only applicable to 3GPP access.

4.6.2.11 Mobility management for partial network slice

A serving PLMN or SNPN can indicate the S-NSSAI(s) is allowed or rejected in some TA(s) but not all TAs of the registration area to the UE during the registration procedure as specified in subclause 5.5.1 and the generic UE configuration update procedure as specified in subclause 5.4.4. The support for the partial network slice by a UE or an AMF is optional.

If the UE supports the partial network slice and includes the S-NSSAI(s) in the requested NSSAI and:

a) if the S-NSSAI(s) is allowed in the current TA but not all TAs of the registration area, and

   1) if the S-NSSAI(s) is subject to NSAC for the maximum number of UEs, the AMF should include the S-NSSAI(s) in the allowed NSSAI to the UE and limit the registration area so that the S-NSSAI(s) is allowed in all the TAs of the registration area;

   2) if the S-NSSAI(s) is subject to NSSAA, the AMF shall include the S-NSSAI(s) in:

      i) the pending NSSAI to the UE when the AMF is going to perform the network slice-specific authentication and authorization for the S-NSSAI(s); or

      ii) the partially allowed NSSAI to the UE after the network slice-specific authentication and authorization for the S-NSSAI(s) has been successfully performed; and

   3) otherwise, the AMF shall include the S-NSSAI(s) in the partially allowed NSSAI to the UE; or

b) if the S-NSSAI(s) is rejected in the current TA but not all TAs of the registration area; and

   1) if the S-NSSAI is subject to NSAC for the maximum number of UEs, the AMF should include the S-NSSAI(s) in the partially rejected NSSAI to the UE;

   2) if the S-NSSAI(s) is subject to NSSAA, the AMF shall include the S-NSSAI(s) in:

      i) the partially rejected NSSAI to the UE when the AMF determines not to perform the network slice-specific authentication and authorization for the S-NSSAI(s);

      ii) the pending NSSAI to the UE when the AMF is going to perform the network slice-specific authentication and authorization for the S-NSSAI(s); or

      iii) either the partially allowed NSSAI or the partially rejected NSSAI to the UE after the network slice-specific authentication and authorization for the S-NSSAI(s) has been successfully performed;

NOTE 1: The AMF determines whether to perform the network slice-specific authentication and authorization procedure for the partial network slice based on its own local policy.

   3) if the S-NSSAI(s) is associated with a slice deregistration inactivity timer on the AMF side as specified in subclause 4.6.2.9, the AMF shall include the S-NSSAI(s) in the partially rejected NSSAI to the UE; and

   4) otherwise, the AMF shall include the S-NSSAI(s) in either the partially allowed NSSAI or the partially rejected NSSAI to the UE; or

c) if the partially allowed NSSAI, the partially rejected NSSAI, or both are changed, the AMF shall provide the new partially allowed NSSAI, the new partially rejected NSSAI, or both to the UE.

   Upon receiving the partially allowed NSSAI, the UE shall regard the S-NSSAI(s) included in partially allowed NSSAI, if any, as the allowed S-NSSAI(s) for the current registration area and store the received partially allowed NSSAI as specified in subclause 4.6.2.2.

   Upon receiving the partially rejected NSSAI, the UE shall store the received partially rejected NSSAI as specified in subclause 4.6.2.2. The UE shall not attempt to include the S-NSSAI, if any, in the requested NSSAI if the current TAI is in the list of TAs for which S-NSSAI is rejected.

The AMF shall ensure that there is also at least one S-NSSAI in the allowed NSSAI allocated to the UE as specified in subclause 5.15.2.1 of 3GPP TS 23.501 [8].

The mobility management for partial network slice is only applicable to 3GPP access.

The mobility management for partial network slice is not applicable to a UE that is registering or registered for onboarding services in SNPN.

4.6.3 Session management aspects

4.6.3.0 General

In order to enable PDU transmission in a network slice, the UE may request establishment of a PDU session in a network slice towards a data network (DN) which is associated with an S-NSSAI and a data network name (DNN) if there is no established PDU session adequate for the PDU transmission. The S-NSSAI included is part of allowed NSSAI of the serving PLMN or SNPN, which is an S-NSSAI value valid in the serving PLMN or SNPN, and in roaming scenarios the mapped S-NSSAI is also included for the PDU session if available. See subclause 6.4.1 for further details. The UE determines whether to establish a new PDU session or use one of the established PDU session(s) based on the URSP rules which include S-NSSAIs, if any (see subclause 6.2.9), or based on UE local configuration, as described in subclause 4.2.2 of 3GPP TS 24.526 [19].

4.6.3.1 Session management based network slice admission control

A serving PLMN or the HPLMN, or SNPN can perform network slice admission control for the S-NSSAI(s) subject to NSAC to monitor and control the total number of established PDU sessions per network slice. The SMF performs network slice admission control on the S-NSSAI during the PDU session establishment procedure. If the maximum number of PDU sessions on a network slice associated with an S-NSSAI has been already reached, the SMF rejects the PDU session establishment request using S-NSSAI based congestion control as specifed in subclause 6.2.8 and 6.4.1.4.2.

The SMF performs network slice admission control on the S-NSSAI for a PDU session that is associated with the non-3GPP access, when the UE requests to transfer a session from the non-3GPP access to the 3GPP access with the Allowed PDU session status IE as described in subclause 5.6.1.4. If the maximum number of PDU sessions on a network slice associated with an S-NSSAI has been already reached, the SMF rejects the request to establish the user-plane resources (see 3GPP TS 29.502 [20A]).

Based on operator policy, the session management based network slice admission control is not applicable for the PDU session for emergency services, or the session management based network slice admission control result is ignored for the PDU session for emergency services.

Based on operator policy, the session management based network slice admission control is not applicable for the PDU session for priority services, or the session management based network slice admission control result is ignored for the PDU session for priority services.

NOTE 1: The SMF can use the Sbi-Message-Priority field, as defined in TS 29.500 [20AA], to determine whether the PDU session is for priority services.

The session management based network slice admission control is not applicable to PDU session established for onboarding services in SNPN.

NOTE 2: For the MA PDU session during the PDU session establishment procedure, the SMF performs network slice admission control only when it is newly established over the associated access type.

NOTE 3: For a set of redundant PDU sessions, the SMF performs network slice admission control for each PDU session independently.

4.6.3.2 Support of network slice admission control and interworking with EPC

If EPS counting is required for a network slice, the network performs network slice admission control for the S-NSSAI(s) subject to NSAC to monitor and control the number of UEs per network slice and number of PDU sessions per network slice during the PDN connection establishment procedure. If the maximum number of UEs on a network slice associated with an S-NSSAI or the maximum number of PDU sessions on a network slice associated with an S-NSSAI have already been reached, the network rejects the PDN connectivity request using ESM cause #26 "insufficient resources" as specifed in 3GPP TS 24.301 [15].

NOTE: If there are more than one S-NSSAI associated with the APN used in the PDN connectivity request and some of but not all associated S-NSSAIs are not available due to either maximum number of UEs reached or maximum number of PDU sessions reached, the network can use the associated S-NSSAI for which maximum number of UEs and maximum number of PDU sessions have not reached to avoid PDN connectivity request rejection.

4.6.3.3 Session management based network slice data rate limitation control

A serving PLMN or the HPLMN can perform network slice data rate limitation control for the S-NSSAI(s) subject to network slice data rate limitation control to monitor and control the total data rate of established PDU sessions per network slice as specified in 3GPP TS 23.503 [10]. If the maximum data rate of PDU sessions on a network slice associated with an S-NSSAI has been exceeded during the PDU session establishment procedure, the SMF may reject the PDU session establishment request using S-NSSAI based congestion control as specified in subclause 6.2.8 and 6.4.1.4.2.

A serving PLMN or the HPLMN can perform management of Slice-Maximum Bit Rate per UE (UE-Slice-MBR) as specified in 3GPP TS 23.503 [10]. When the UE-Slice-MBR for the UE and S-NSSAI to which the PDU session is allocated is exceeded during the PDU session establishment procedure, the SMF may reject the PDU session establishment request using S-NSSAI based congestion control as specified in subclause 6.2.8 and 6.4.1.4.2.

NOTE 1: Based on operator policy, the network slice data rate limitation control can be not applicable for the S-NSSAI(s) used for emergency services or priority services.

NOTE 2: The network slice data rate limitation control and UE-Slice-MBR management are performed by the PCF.

4.6.3.4 Session management based network slice replacement

If:

a) the UE and network support network slice replacement;

b) the UE is provided with the mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI; and

c) the UE decides to establish a new PDU session with the S-NSSAI to be replaced,

the UE provides both the S-NSSAI to be replaced and the alternative S-NSSAI during PDU session establishment procedure. If the timer T3584 or timer T3585 is running for the S-NSSAI to be replaced, the UE should not stop the timer during PDU session establishment procedure. If the SMF receives both the S-NSSAI to be replaced and the alternative S-NSSAI during PDU session establishment procedure, the SMF proceeds with the PDU session establishment procedure with the alternative S-NSSAI. If the PDU session establishment request is accepted, the SMF includes the alternative S-NSSAI in the PDU session establishment accept message. The S-NSSAI for the established PDU session is the S-NSSAI to be replaced and the alternative S-NSSAI on the UE side.

If the UE is provided with the mapping of the VPLMN S-NSSAI to a VPLMN alternative S-NSSAI, the UE provides both the VPLMN alternative S-NSSAI and the VPLMN S-NSSAI during PDU session establishment procedure. The AMF sends both VPLMN alternative S-NSSAI and VPLMN S-NSSAI to the SMF. If the UE is provided with the mapping of the HPLMN S-NSSAI to a HPLMN Alternative S-NSSAI, the UE provides both the HPLMN alternative S-NSSAI and the HPLMN S-NSSAI during PDU session establishment procedure. The AMF sends both HPLMN alternative S-NSSAI and HPLMN S-NSSAI to the SMF.

If the SMF receives from the AMF an alternative S-NSSAI for existing PDU session and:

a) if the SMF decides to retain the existing PDU session (i.e. the SMF can serve both the alternative S-NSSAI and the S-NSSAI to be replaced with), the SMF sends the alternative S-NSSAI to the UE during network-requested PDU session modification procedure; or

b) if the SMF decides to re-activate the existing PDU session and:

   1) if the SSC mode of the PDU session is SSC mode 3, the SMF initiates PDU session modification procedure to trigger PDU session reactivation by the UE; or

2) if the SSC mode of the PDU session is SSC mode 1 or SSC mode 2, the SMF initiates PDU session release procedure to trigger PDU session reactivation by the UE, and the UE provides both the S-NSSAI to be replaced and the alternative S-NSSAI during PDU session establishment procedure.

When the replaced S-NSSAI becomes available again, if the SMF receives from the AMF the replaced S-NSSAI for the existing PDU session and:

a) if the SMF decides to retain the existing PDU session (i.e. the SMF can serve the replaced S-NSSAI), the SMF sends the replaced S-NSSAI to the UE during network-requested PDU session modification procedure; or

b) if the SMF decides to re-activate the existing PDU session and:

1) if the SSC mode of PDU session is SSC mode 3, the SMF sends the replaced S-NSSAI to the UE during PDU session modification procedure to trigger PDU session reactivation by the UE; or

2) if the SSC mode of the PDU session is SSC mode 1 or SSC mode 2, the SMF sends the replaced S-NSSAI to the UE during PDU session release procedure to trigger PDU session reactivation by the UE; and the UE provides the replaced S-NSSAI during PDU establishment procedure.

If the timer T3584 or timer T3585 is running for the replaced S-NSSAI and the replaced S-NSSAI in alternative NSSAI is available and the AMF provides the updated allowed NSSAI and configured NSSAI to the UE, the UE should stop the timer.

4.6.3.5 Session management for optimized handling of temporarily available network slices

A network slice can be available temporarily. Subclause 4.6.2.8 addresses how the allowed NSSAI and partially allowed NSSAI are managed based on the S-NSSAI time validity information.

If the S-NSSAI time validity information indicates that the S-NSSAI is available, the UE may initiate a UE-requested PDU session establishment procedure to establish a PDU session associated with the S-NSSAI.

If the S-NSSAI time validity information indicates that the S-NSSAI is not available, then the UE shall:

a) initiate UE-requested PDU session release procedure to release any PDU session associated with the S-NSSAI, if the UE is in 5GMM-CONNECTED mode or in 5GMM-CONNECTED mode with RRC inactive indication; or

b) locally release any PDU session associated with the S-NSSAI, if the UE is in 5GMM-IDLE mode.

When the S-NSSAI time validity information in the AMF indicates that the S-NSSAI is not available, independent of whether the UE is in 5GMM-CONNECTED mode, 5GMM-CONNECTED mode with RRC inactive indication or in 5GMM-IDLE mode, the AMF shall request the SMF to release any PDU session associated with the S-NSSAI.

4.6.3.6 Session management for partial network slice

If the S-NSSAI is included in the partially allowed NSSAI and:

a) if the current TAI is in the list of TAs for which the S-NSSAI is allowed, the UE may initiate the UE-requested PDU session establishment procedure for the S-NSSAI; or

b) if the current TAI is not in the list of TAs for which the S-NSSAI is allowed, the UE shall not initiate the UE-requested PDU session establishment procedure for the S-NSSAI.

If an existing PDU session is established for the S-NSSAI included in the partially allowed NSSAI and the current TAI is in the list of TAs for which the S-NSSAI is allowed:

a) the UE:

1) may initiate the service request procedure to re-establish the user plane resources for the established PDU session; or

2) may initiate either the UE-initiated NAS transport procedure to send CIoT user data to the SMF (see subclause 5.4.5.2.1 case h) or the service request procedure to send CIoT user data to the SMF (see subclause 5.6.1.1 case d); and

b) the SMF may initiate the network-initiated NAS transport procedure to send CIoT user data to the UE (see subclause 5.4.5.3.1 case l).

If an existing PDU session is established for the S-NSSAI included in the partially allowed NSSAI and the current TAI is not in the list of TAs for which the S-NSSAI is allowed:

a) the UE:

1) shall maintain the 5GSM contexts for the established PDU session;

2) shall not initiate the UE-initiated NAS transport procedure to send CIoT user data to the SMF (see subclause 5.4.5.2.1 case h) nor the service request procedure to send CIoT user data to the SMF (see subclause 5.6.1.1 case d); and

3) may initiate:

i) the UE-requested PDU session release procedure; or

ii) the UE-requested PDU session modification procedure to set the 3GPP PS data off status to "deactivated" as specified in 3GPP TS 24.008 [13]; and

b) the SMF:

1) shall maintain the 5GSM contexts for the established PDU session;

2) shall not initiate the network-initiated NAS transport procedure to send CIoT user data to the UE (see subclause 5.4.5.3.1 case l); and

3) may initiate the network-requested PDU session release procedure.

If the SMF cannot determine that the UE is located in a TA within the list of TAs associated with the S-NSSAI of an existing PDU session established for this S-NSSAI, the SMF may according to operator's policy:

a) attempt to establish the user plane resources for the PDU session; or

b) initiate the network-initiated NAS transport procedure to send CIoT user data to the UE (see subclause 5.4.5.3.1 case l).

If the SMF determines that:

a) the UE is located in a TA within the list of TAs associated with the S-NSSAI of an existing always-on PDU session;

b) the UE is in 5GMM-CONNECTED mode; and

c) the user-plane resources for the always-on PDU session are not established,

the SMF shall attempt to establish the user plane resources for the always-on PDU session associated with the S-NSSAI included in the partially allowed NSSAI.

NOTE: The session management for partial network slice is not applicable to the PDU session established for onboarding services in SNPN.

4.6.3.7 Session management aspect of handling network slices with NS-AoS not matching deployed tracking areas

If a UE is outside the NS-AoS of an S-NSSAI (see subclause 4.6.2.10), the UE shall not:

a) attempt to request the establishment of user plane resources of any PDU session associated with the S-NSSAI; and

b) initiate the UE-initiated NAS transport procedure to send CIoT user data to the SMF (see subclause 5.4.5.2.1 case h) nor the service request procedure to send CIoT user data to the SMF (see subclause 5.6.1.1 case d).

If a UE is outside the NS-AoS of an S-NSSAI (see subclause 4.6.2.10), the SMF shall not:

a) attempt to establish user plane resources of any PDU session associated with the S-NSSAI; and

b) initiate the network-initiated NAS transport procedure to send CIoT user data to the UE (see subclause 5.4.5.3.1 case l).

If a UE is outside the NS-AoS of an S-NSSAI (see subclause 4.6.2.10), the UE may initiate the UE-initiated NAS transport procedure carrying the following 5GSM messages for the PDU session associated with the S-NSSAI:

a) a PDU SESSION RELEASE REQUEST message; or

b) a PDU SESSION MODIFICATION REQUEST message to set the 3GPP PS data off status to "deactivated" as specified in 3GPP TS 24.008 [13].

NOTE: A PDU session associated with an S-NSSAI is not released solely because a UE is outside the NS-AoS of the S-NSSAI.

If the SMF cannot determine that the UE is located inside the NS-AoS of the S-NSSAI of an existing PDU session established for this S-NSSAI, the SMF may according to operator's policy:

a) attempt to establish the user plane resources for the PDU session; or

b) initiate the network-initiated NAS transport procedure to send CIoT user data to the UE (see subclause 5.4.5.3.1 case l).

If the SMF determines that:

a) the UE is located inside the NS-AoS of the S-NSSAI of an existing always-on PDU session;

b) the UE is in 5GMM-CONNECTED mode; and

c) the user plane resources for the always-on PDU session are not established,

the SMF shall attempt to establish the user-plane resources for the always-on PDU session associated with the S-NSSAI with S-NSSAI location validity information.

4.7 NAS over non-3GPP access

4.7.1 General

From the UE's NAS perspective, in general the procedures and messages defined for 5GMM and 5GSM are used over non-3GPP access as over 3GPP access. However, a number of aspects are different as described in the following subclauses.

4.7.2 5GS mobility management aspects

4.7.2.1 General

The mobility management procedures defined over 3GPP access are re-used over non-3GPP access with the following exceptions:

a) the registration status, and the 5GMM parameters of the UE's 3GPP access and non-3GPP access 5GMM state machine instances are independent in each of these accesses and can be different;

b) single-registration mode and dual-registration mode do not apply for 5GMM over non-3GPP access;

c) the RPLMN over non-3GPP access can be different from the RPLMN over 3GPP access. The MCC of the RPLMN over 3GPP access and the MCC of the RPLMN over the non-3GPP access can also be different;

d) the registration for 3GPP access and for non-3GPP access are performed separately. Like for 3GPP access, an access stratum connection exists before the UE can perform the registration procedure for non-3GPP access. As at registration over non-3GPP access the UE is allocated a registration area, which is associated with a single TAI, list management of registration areas is not required, and registration updating due to registration area

change with the registered PLMN is not performed. Furthermore, the registration procedure for periodic registration update is also not performed. New registration at change of PLMN is required;

e) the 5GMM over non-3GPP access in the UE considers that the N1 NAS signalling connection is established when the lower layers indicate that the access stratum connection is established succcessfully;

f) the UE-initiated service request procedure via non-3GPP access is supported. Upon indication from the lower layers of non-3GPP access, that the access stratum connection is established between the UE and the network, the UE in 5GMM-REGISTERED state and in 5GMM-IDLE mode over non-3GPP access shall initiate the service request procedure via non-3GPP access. The UE may indicate with the service request message the PDU session(s) associated with non-3GPP access to re-establish user-plane resources for which the UE has pending user data to be sent;

g) paging procedure is not performed via non-3GPP access;

h) service area restrictions do not apply for non-3GPP access other than the wireline access;

i) the establishment cause for non-3GPP access is determined according to subclause 4.7.2.2;

j) eCall inactivity procedure is not performed via non-3GPP access;

k) local area data network (LADN) does not apply for non-3GPP access;

l) the Allowed PDU session IE shall not be included in the REGISTRATION REQUEST message or the SERVICE REQUEST message sent over non-3GPP access;

m) DRX parameters do not apply for non-3GPP access;

n) Mobile initiated connection only mode (MICO) does not apply for non-3GPP access;

o) CIoT 5GS optimizations do not apply for non-3GPP access;

p) unified access control does not apply for non-3GPP access;

q) UE radio capability signalling optimisation (RACS) does not apply for non-3GPP access;

r) Closed access group (CAG) does not apply for non-3GPP access;

s) the N1 NAS signalling connection release, the paging indication for voice services and reject the paging request do not apply for non-3GPP access. The Paging restriction IE shall not be included in the REGISTRATION REQUEST message, the SERVICE REQUEST message or the CONTROL PLANE SERVICE REQUEST message sent over non-3GPP access. The AMF shall not delete any stored paging restriction preferences for the UE and shall not stop restricting paging when receiving REGISTRATION REQUEST message, SERVICE REQUEST message or CONTROL PLANE SERVICE REQUEST message over non-3GPP access;

t) the partially allowed NSSAI and the partially rejected NSSAI do not apply for non-3GPP access; and

u) support for unavailability period (see subclause 5.3.26) does not apply for non-3GPP access.

4.7.2.2 Establishment cause for non-3GPP access

When establishment of an N1 NAS signalling connection over non-3GPP access is initiated, the UE shall:

a) determine one or more access identities to be associated with the establishment of the N1 NAS signalling connection as specified in subclause 4.5.2 and table 4.5.2.1;

b) select the establishment cause for non-3GPP access from the determined one or more access identities and the event which triggered initiation of the N1 NAS signalling connection over non-3GPP access by checking the rules specified in table 4.7.2.2.1; and

c) provide the selected establishment cause for non-3GPP access to the lower layers.

While an MMTEL voice call is ongoing:

- any:

1) service request procedure; or

2) registration procedure;

initiated in 5GMM-IDLE mode is mapped to "MO MMTel voice call" type access attempt.

While an MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode is mapped to "MO MMTel video call" type access attempt.

While an SMSoIP is ongoing, no MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode is mapped to "MO SMS over IP" type access attempt.

If the access attempt matches more than one rule, the establishment cause for non-3GPP access of the lowest rule number shall be used.

Table 4.7.2.2.1: Mapping table for determination of establishment cause for non-3GPP access

Rule #	Access identities	Type of access attempt	Requirements to be met	Establishment cause for non-3GPP access
1	1	Any	Any	mps-PriorityAccess
2	2	Any	Any	mcs-PriorityAccess
3	11, 15	Any	Any	highPriorityAccess
4	12,13,14,	Any	Any	highPriorityAccess
5	0	Emergency	UE is attempting access for an emergency session (NOTE 1)	emergency
		UE NAS initiated 5GMM specific procedures	Access attempt is for MO signalling	mo-Signalling
		UE NAS initiated 5GMM connection management procedures or 5GMM NAS transport procedure	Access attempt is for MO data	mo-Data
		MO SMS over NAS or MO SMS over IP	Access attempt is for MO SMS over NAS or MO SMS over IP	mo-SMS
		MO MMTel voice call	Access attempt is for MO MMTel voice call	mo-VoiceCall
		MO MMTel video call	Access attempt is for MO MMTel video call	mo-Videocall
NOTE 1: This includes 5GMM specific procedures while the service is ongoing and 5GMM connection management procedures required to establish a PDU session with request type = "initial emergency request" or "existing emergency PDU session", or to re-establish user-plane resources for such a PDU session. NOTE 2: See subclause 4.5.2, table 4.5.2.1 for use of the access identities of 0, 1, 2, and 11-15.				

4.7.3 5GS session management aspects

The session management procedures defined over 3GPP access are re-used over non-3GPP access with the following exceptions:

a) Serving PLMN rate control does not apply for non-3GPP access;

b) Small data rate control does not apply for non-3GPP access;

c) Handling of 5GSM cause value #82 "maximum data rate per UE for user-plane integrity protection is too low" does not apply for non-3GPP access;

d) MBS does not apply for non-3GPP access;

e) Support of redundant PDU sessions does not apply for non-3GPP access; and

f) PDU set handling does not apply for non-3GPP access.

4.7.4 Limited service state over non-3GPP access

There are a number of situations in which the UE is unable to obtain normal service from a PLMN over non-3GPP access and the UE enters the limited service state over non-3GPP access. These include:

a) no USIM in the ME;

b) an "illegal UE" or "illegal ME" is received when registration, network-initiated de-registration or service request is performed (any USIM in the ME is then considered "invalid");

c) a "5GS services not allowed" is received when a registration, network-initiated de-registration or service request is performed;

d) a "PLMN not allowed" is received when registration, network-initiated de-registration or service request is performed;

e) a "Tracking area not allowed" is received when a registration, network-initiated de-registration or service request is performed;

f) a "Roaming not allowed in this tracking area" is received when a registration, network-initiated de-registration or service request is performed;

g) void; or

h) a "Serving network not authorized" is received when a registration or service request is performed.

In limited service state with a valid USIM in the UE, the network selection is performed as defined in 3GPP TS 24.502 [18].

With the exception of performing initial registration for emergency services, no registration requests are made until a valid USIM is present. For registration for emergency services, the PLMN of the current N3IWF or TNGF is considered as the selected PLMN for the duration the UE is registered for emergency services.

4.7.5 NAS signalling using trusted WLAN access network

A trusted WLAN interworking function (TWIF) provides functionalities for a non-5G capable over WLAN (N5CW) device to access 5GCN, including:

a) NAS signalling over N1 NAS signalling connection with AMF; and

b) PDU session establishment, modification and release on behalf of the N5CW device, over N2 connection with the AMF.

The TWIF registers on behalf of the N5CW device to an AMF according to subclause 5.5.1 by populating the parameters for the registration by using implementation specific default values which are the same for N5CW devices.

The TWIF may request to establish a PDU session as specified in subclause 6.4.1.2 on behalf of the N5CW device upon receipt of an IP configuration request from the N5CW device by populating either all the required parameters or part of the required parameters for the PDU session establishment by using implementation specific default values from the TWIF's configuration. Only one PDU session is supported when N5CW device accessing 5GCN via the TWIF.

NOTE 1: If part of the required parameters for the PDU session establishment is provided by the TWIF, the remaining of the required parameters are determined by the AMF or the SMF based on the N5CW device's subscription information.

Upon loss of the IP address of the N5CW device, the TWIF acting on behalf of the N5CW device shall initiate the UE-requested PDU session release procedure as defined in subclause 6.4.3.

NOTE 2: The established PDU session on behalf of the N5CW device can be modified by the TWIF or the network.

4.8 Interworking with E-UTRAN connected to EPC

4.8.1 General

In order to interwork with E-UTRAN connected to EPC, the UE supporting both S1 mode and N1 mode can operate in single-registration mode or dual-registration mode (see 3GPP TS 23.501 [8]). Support of single-registration mode is mandatory for UEs supporting both S1 mode and N1 mode.

During the EPS attach procedure (see 3GPP TS 24.301 [15]) or initial registration procedure (see subclause 5.5.1.2), the mode for interworking is selected if the UE supports both S1 mode and N1 mode, and the network supports interworking. The mode for interworking may also be selected during the EPS tracking area updating procedure (see 3GPP TS 24.301 [15]) or registration procedure for mobility and periodic registration update (see subclause 5.5.1.3).

For interworking between E-UTRAN connected to EPC and TNGF or N3IWF connected to 5GCN, the UE shall operate as specified in either subclause 4.8.2.3 or subclause 4.8.3. Which subclause the UE follows is chosen by the UE irrespective of the interworking without N26 interface indicator.

4.8.2 Single-registration mode

4.8.2.1 General

If the UE receives the indication that "interworking without N26 interface not supported" (see 3GPP TS 24.301 [15]), the UE operates as described in subclause 4.8.2.2.

If the UE receives the indication that "interworking without N26 interface supported" and

a) the UE does not support dual-registration mode; or

b) the UE supporting dual-registration mode determines to operate in single-registration mode,

the UE operates as described in subclause 4.8.2.3.

4.8.2.2 Single-registration mode with N26 interface

See subclause 5.1.4.2 for coordination between 5GMM and EMM and subclause 6.1.4.1 for coordination between 5GSM and ESM.

4.8.2.3 Single-registration mode without N26 interface

4.8.2.3.1 Interworking between NG-RAN and E-UTRAN

At inter-system change from N1 mode to S1 mode in EMM-IDLE mode when:

a) the UE supports non-IP PDN type and at least one PDU session of Unstructured PDU session type is active;

b) the UE supports IPv4 PDN type and at least one PDU session of IPv4 PDU session type is active;

c) the UE supports IPv6 PDN type and at least one PDU session of IPv6 PDU session type is active;

d) the UE supports IPv4v6 PDN type and at least one PDU session of IPv4v6 PDU session type is active; or

e) at least one PDU session of Ethernet PDU session type is active and:

1) the UE supports non-IP PDN type; or

2) the UE and the network support Ethernet PDN type in S1 mode;

the UE shall proceed as follows:

a) if the UE supports sending an ATTACH REQUEST message containing a PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer a PDU session from N1 mode to S1 mode and the UE has received an "interworking without N26 interface supported" indication from the network, the UE shall:

1) enter substates EMM-DEREGISTERED.NORMAL-SERVICE and 5GMM- DEREGISTERED.NO-CELL-AVAILABLE for 3GPP access;

NOTE: Since MM context transfer is not possible between MME and AMF in a network that indicates "Interworking without N26 supported", it is up to the UE implementation as to how to keep the 5GMM and EMM states in the UE in sync.

2) map the PDU session(s) which the UE intends to transfer to EPS to the default EPS bearer context of the corresponding PDN connection(s) as specified in subclause 6.1.4.2; and

3) initiate an EPS attach procedure and include in the ATTACH REQUEST message a PDN CONNECTIVITY REQUEST message with:

- the request type set to "handover of emergency bearer services" to activate a default EPS bearer context for an active emergency PDU session, if the session to be transferred is an emergency PDU session; or

- the request type set to "handover" message to activate a default EPS bearer context for an active non-emergency PDU session, if the session to be transferred is a non-emergency PDU session. If the selected PDU session is an MA PDU session established over 3GPP access, the UE shall include the ATSSS request parameter in the Protocol configuration options IE or the Extended protocol configuration options IE of the ESM INFORMATION RESPONSE message.

After successful completion of the EPS attach procedure, the UE shall reset the registration attempt counter for 3GPP access and the attach attempt counter (see 3GPP TS 24.301 [15]), enter substates EMM-REGISTERED.NORMAL-SERVICE and 5GMM-REGISTERED.NO-CELL-AVAILABLE for 3GPP access and attempt to activate each of the other default EPS bearer contexts, if any, by initiating a stand-alone PDN connectivity procedure with request type set to "handover" for non-emergency PDU session or "handover of emergency bearer services" for emergency PDU session in the PDN CONNECTIVITY REQUEST message. If the EPS attach procedure is unsuccessful the UE shall enter substates EMM-DEREGISTERED.NORMAL-SERVICE and 5GMM-DEREGISTERED.NO-CELL-AVAILABLE for 3GPP access; and

b) otherwise, enter substates EMM-REGISTERED.NORMAL-SERVICE and 5GMM-REGISTERED.NO-CELL-AVAILABLE for 3GPP access and initiate a tracking area update procedure (see 3GPP TS 24.301 [15]).

At inter-system change from N1 mode to S1 mode in EMM-IDLE mode when:

a) the UE does not support non-IP PDN type or no PDU session of Unstructured PDU session type is active;

b) the UE does not support IPv4 PDN type or no PDU session of IPv4 PDU session type is active;

c) the UE does not support IPv6 PDN type or no PDU session of IPv6 PDU session type is active;

d) the UE does not support IPv4v6 PDN type or no PDU session of IPv4v6 PDU session type is active; and

e) no PDU session of Ethernet PDU session type is active or:

1) the UE does not support non-IP PDN type; and

2) the UE, the network or both do not support Ethernet PDN type in S1 mode;

the UE shall enter substates EMM-DEREGISTERED.NORMAL-SERVICE and 5GMM-DEREGISTERED.NO-CELL-AVAILABLE for 3GPP access, and initiate an attach procedure.

At inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE shall:

a) enter substate 5GMM-REGISTERED.NORMAL-SERVICE for 3GPP access and substate EMM-REGISTERED.NO-CELL-AVAILABLE;

b) map the default EPS bearer context(s) of the PDN connection(s) which the UE intends to transfer to 5GS, if any, to the corresponding PDU session(s) as specified in subclause 6.1.4.2; and

c) initiate the registration procedure for mobility and periodic registration update over 3GPP access indicating "mobility registration updating" in the 5GS registration type IE of the REGISTRATION REQUEST message (see subclause 5.5.1.3).

After having successfully registered in N1 mode over 3GPP access, the UE shall reset the registration attempt counter for 3GPP access, and the attach attempt counter or tracking area updating attempt counter (see 3GPP TS 24.301 [15]) and:

a) if the UE supports the PDU session establishment procedure with request type set to "existing PDU session" or "existing emergency PDU session" to transfer a PDN connection from S1 mode to N1 mode and the UE has received an "interworking without N26 interface supported" indication from the network, attempt to transfer the PDN connection(s) which the UE intends to transfer to 5GS, if any, from S1 mode to N1 mode by:

   - if the PDN connection which the UE intends to transfer is a PDN connection for emergency bearer services, initiating the PDU session establishment procedure with request type set to "existing emergency PDU session" to transfer the PDN connection for emergency bearer services; and

   - if the PDN connection which the UE intends to transfer is a non-emergency PDN connection, initiating the PDU session establishment procedure with request type set to:

      1) "MA PDU request", if the PDN connection to be transferred is a user-plane resource of an MA PDU session; or

      2) "existing PDU session" to transfer the non-emergency PDN connection; and

b) otherwise, establish PDU session(s) corresponding to the PDN connection(s) which the UE intends to transfer to 5GS, if any, by initiating the PDU session establishment procedure with request type set to "initial request".

See subclause 5.1.4.3 for coordination between 5GMM and EMM and subclause 6.1.4.2 for coordination between 5GSM and ESM.

4.8.2.3.2 Interworking between TNGF or N3IWF connected to 5GCN and E-UTRAN

If:

a) the UE has registered in neither N1 mode over 3GPP access nor S1 mode yet; and

b) the UE has at least one active PDU session associated with non-3GPP access which the UE intends to transfer to EPS,

the UE shall initiate an EPS attach procedure and include a PDN CONNECTIVITY REQUEST message with a request type in the ATTACH REQUEST message to activate a default EPS bearer context for one of the active PDU sessions which the UE intends to transfer to EPS (see 3GPP TS 24.301 [15]). The request type is set as follows:

- if the PDU session which the UE intends to transfer is a non-emergency PDU session, the request type is set to "handover"; and

- if the PDU session which the UE intends to transfer is an emergency PDU session, the request type is set to "handover of emergency bearer services" and the default bearer to be activated is the default EPS bearer context for the emergency PDU session.

NOTE 1: It is necessary for the UE to support sending an ATTACH REQUEST message containing a PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer a PDU session from N1 mode to S1 mode for interworking between TNGF or N3IWF connected to 5GCN and E-UTRAN.

NOTE 2: The order of PDU sessions to be tranferred to EPS is up to UE implementation.

After successful completion of the EPS attach procedure where the activated default EPS bearer context is not for emergency service, the UE shall initiate a UE requested PDN connectivity procedure with request type set to "handover" for non-emergency PDU session or "handover of emergency bearer services" for emergency PDU session in the PDN CONNECTIVITY REQUEST message to transfer each of the other PDU sessions which the UE intends to transfer to EPS, if any.

If:

a) the UE has not registered in N1 mode over non-3GPP access yet; and

b) the UE has at least one active PDN connection which the UE intends to transfer to TNGF or N3IWF connected to 5GCN,

the UE shall initiate an initial registration procedure over non-3GPP access (see subclause 5.5.1.2).

After successful completion of the 5GS initial registration in N1 mode over non-3GPP access, the UE shall initiate a UE-requested PDU session establishment procedure with a request type to transfer each of the PDN connections which the UE intends to transfer to TNGF or N3IWF connected to 5GCN, if any. The request type is set as follows:

- if the PDN connection which the UE intends to transfer is a PDN connection for emergency bearer services, the request type is set to "existing emergency PDU session" to transfer the PDN connection for emergency bearer services; and

- if the PDN connection which the UE intends to transfer is a non-emergency PDN connection, the request type is set to "existing PDU session" to transfer the non-emergency PDN connection.

NOTE 3: If the UE has no active PDU session associated with non-3GPP access which the UE in N1 mode intends to transfer to EPS or no active PDN connection associated with 3GPP access which the UE in S1 mode intends to transfer to TNGF or N3IWF connected to 5GCN, the interworking between TNGF or N3IWF connected to 5GCN and E-UTRAN is not supported.

See subclause 6.1.4.2 for coordination between 5GSM and ESM.

4.8.3 Dual-registration mode

If both 5GMM and EMM are enabled, a UE, operating in the dual-registration mode shall maintain independent contexts for 5GMM and EMM and this includes independent lists of equivalent PLMNs. Coordination between 5GMM and EMM is not needed, except as specified in the present subclause, subclause 5.1.5 and 5.3.13A.

For dual-registration mode the following applies:

a) a UE operating in the dual-registration mode may register to N1 mode only, S1 mode only, or to both N1 mode and S1 mode;

b) when the UE decides to operate in dual-registration mode (see subclause 5.5.1.2.4), NAS informs the lower layers about this;

c) if a UE is registered in N1 mode only, then for registration in S1 mode the UE shall use:

   1) the same PLMN to which it is registered in N1 mode; or

   2) an equivalent PLMN; and

d) if a UE is registered in S1 mode only, then for registration in N1 mode the UE shall use:

   1) the same PLMN to which it is registered in S1 mode; or

   2) an equivalent PLMN.

NOTE 1: It is up to UE implementation how to handle the case when the UE is registered in both N1 mode and S1 mode and the PLMNs to which the UE is registered, are not equivalent, e.g. search for a PLMN which is the same or equivalent to any of the registered ones.

When no PDU session is active and the UE has not registered to S1 mode yet, the UE may initiate the EPS attach procedure with PDN connection establishment if EMM-REGISTERED without PDN connection is not supported by the

MME. If EMM-REGISTERED without PDN connection is supported by the MME, the UE may initiate either the EPS attach procedure without PDN connection establishment or the attach procedure with PDN connection establishment.

When at least one PDU session is active and the UE has not registered to S1 mode yet, the UE may initiate the EPS attach procedure. If necessary, the UE may transfer an active PDU session from N1 mode to S1 mode by initiating the EPS attach procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message. After successfully attached in S1 mode, if necessary, the UE may transfer other active PDU sessions from N1 mode to S1 mode by initiating the PDN connectivity procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message.

NOTE 2: It is up to UE implementation to determine which active PDU session is transferred from N1 mode to S1 mode.

When the UE has not registered to N1 mode, the UE may initiate the initial registration procedure. After successfully registered in N1 mode, if necessary, the UE may transfer one or more active PDN connections from S1 mode to N1 mode by initiating the PDU session establishment procedure with request type set to "existing PDU session".

NOTE 3: It is up to UE implementation to determine which active PDN connection is transferred from S1 mode to N1 mode.

If the MME supports EMM-REGISTERED without PDN connection, the UE that transferred all PDN connections to the 5GS, may stay in state EMM-REGISTERED. Otherwise, the UE shall enter state EMM-DEREGISTERED upon transferring all PDN connection to the 5GS.

NOTE 4: When the UE has registered in both N1 mode and S1 mode, it is up to UE implementation to maintain the registration update to date in both N1 mode and S1 mode.

See subclause 6.1.4 for coordination between 5GSM and ESM.

See subclause 4.8.2.3.2 for interworking between TNGF or N3IWF connected to 5GCN and E-UTRAN.

4.8.4 Core Network selection for UEs not using CIoT 5GS optimizations

If the UE is capable of both N1 mode and S1 mode, when the UE needs to use one or more functionalities not supported in 5GS but supported in EPS and the UE is in 5GMM-IDLE mode, the UE may disable the N1 mode capability for 3GPP access (see subclause 4.9.2).

If the UE is capable of both N1 mode and S1 mode and lower layers provide an indication that the current E-UTRA cell is connected to both EPC and 5GCN without also providing an indication that a target core network type was received from the NG-RAN, the UE shall select a core network type (EPC or 5GCN) based on the PLMN selection procedures as specified in 3GPP TS 23.122 [5] and provide the selected core network type information to the lower layer during the initial registration procedure.

If the UE is capable of both N1 mode and S1 mode and the lower layers have provided an indication that the current E-UTRA cell is connected to both EPC and 5GCN and an indication of whether the network supports IMS emergency services via either EPC or 5GCN or both (see 3GPP TS 36.331 [25A]), the UE selects a core network type (EPC or 5GCN) as specified in 3GPP TS 23.167 [6] annex H.2 for initiating emergency calls when in the state 5GMM-DEREGISTERED.LIMITED-SERVICE or EMM-DEREGISTERED.LIMITED-SERVICE.

NOTE 1: If the PLMN selection information provisioned in the USIM does not contain any prioritization between E-UTRAN and NG-RAN for a PLMN, which core network type to select for that PLMN is up to UE implementation.

If the UE is capable of both N1 mode and S1 mode and lower layers provide an indication that the current E-UTRA cell is connected to both EPC and 5GCN with:

1) an indication that target core network type EPC was received from the NG-RAN, the UE shall select the EPC and proceed with the appropriate EMM procedure as specified in 3GPP TS 24.301 [15]; or

2) an indication that target core network type 5GCN was received from the NG-RAN, the UE shall select the 5GCN and proceed with the appropriate 5GMM procedure.

NOTE 2: The NG-RAN can provide a target core network type to the UE during RRC connection release with redirection (see 3GPP TS 36.331 [25A] and 3GPP TS 38.331 [30]).

4.8.4A Core Network selection and redirection for UEs using CIoT optimizations

4.8.4A.1 Core network selection

A UE that supports CIoT optimizations performs core network selection (i.e. it selects EPC or 5GCN) if the lower layers have provided an indication that the current E-UTRA cell is connected to both EPC and 5GCN as specified in 3GPP TS 23.501 [8].

When selecting a PLMN as described in 3GPP TS 23.122 [5], the UE shall select a core network type (EPC or 5GCN) based on:

a) indication from the lower layers about the CIoT EPS optimizations supported in EPC;

b) indication from the lower layers about the CIoT 5GS optimizations supported in 5GCN;

c) the CIoT EPS optimizations supported by the UE;

d) the CIoT 5GS optimizations supported by the UE;

e) the UE's preferred CIoT network behaviour for EPC; and

f) the UE's preferred CIoT network behaviour for 5GCN.

The UE shall provide the selected core network type information to the lower layer during the initial registration procedure.

4.8.4A.2 Redirection of the UE by the core network

The network that supports CIoT optimizations can redirect a UE between EPC and 5GCN as specified in subclause 5.31.3 of 3GPP TS 23.501 [8]. The network can take into account the UE's N1 mode capability or S1 mode capability, the CIoT network behaviour supported and preferred by the UE or the CIoT network behaviour supported by the network to determine the redirection.

NOTE: It is assumed that the network would avoid redirecting the UE back and forth between EPC and 5GCN.

The network redirects the UE to EPC by rejecting the registration request or service request with the 5GMM cause #31 "Redirection to EPC required" as specified in subclause 5.5.1.2.5, 5.5.1.3.5 and 5.6.1.5. Upon receipt of reject message, the UE disables the N1 mode capability for 3GPP access as specified in subclause 4.9.2 and enables the E-UTRA capability if it was disabled in order to move to EPC.

When there is no ongoing registration procedure or service request procedure for a UE in 5GMM-CONNECTED mode, if the AMF determines to redirect the UE to EPC, the AMF shall initiate the generic UE configuration update procedure to indicate registration requested and release of the N1 NAS signalling connection not requested as described in subclause 5.4.4. The network then redirects the UE to EPC by rejecting the registration request as specified in subclause 5.5.1.3.5.

The network that supports CIoT optimizations can also redirect a UE from EPC to 5GCN as specified in subclause 5.3.19.2 of 3GPP TS 24.301 [15].

4.9 Disabling and re-enabling of UE's N1 mode capability

4.9.1 General

The UE shall re-enable the N1 mode capability when the UE powers off and powers on again, the USIM is removed or an entry of the "list of subscriber data" with the SNPN identity of the SNPN is updated.

4.9.2 Disabling and re-enabling of UE's N1 mode capability for 3GPP access

The UE shall only disable the N1 mode capability for 3GPP access when in 5GMM-IDLE mode.

When the UE is disabling the N1 mode capability for 3GPP access for a PLMN not due to redirection to EPC, it should proceed as follows:

a) select an E-UTRA cell connected to EPC, or for the UE which supports CIoT EPS optimization select a satellite E-UTRA cell connected to EPC via "WB-E-UTRAN(LEO)", "WB-E-UTRAN(MEO)", or "WB-E-UTRAN(GEO)", of the registered PLMN or a PLMN from the list of equivalent PLMNs, if the UE supports S1 mode and the UE has not disabled its E-UTRA capability as specified in 3GPP TS 24.301 [15];

b) if an E-UTRA cell connected to EPC, or for the UE which supports CIoT EPS optimization if a satellite E-UTRA cell connected to EPC via "WB-E-UTRAN(LEO)", "WB-E-UTRAN(MEO)", or "WB-E-UTRAN(GEO)", of the registered PLMN or a PLMN from the list of equivalent PLMNs cannot be found, the UE does not support S1 mode or the UE has disabled its E-UTRA capability as specified in 3GPP TS 24.301 [15], the UE may select another RAT of the registered PLMN or a PLMN from the list of equivalent PLMNs that the UE supports;

c) if another RAT of the registered PLMN or a PLMN from the list of equivalent PLMNs cannot be found, then enter the state 5GMM-REGISTERED.PLMN-SEARCH or 5GMM-DEREGISTERED.PLMN-SEARCH, or the UE does not have a registered PLMN, then enter the state 5GMM-DEREGISTERED.PLMN-SEARCH and perform PLMN selection as specified in 3GPP TS 23.122 [5]. If disabling of the N1 mode capability for 3GPP access was not due to a UE-initiated de-registration procedure for 5GS services over 3GPP access not due to switch-off, the UE may re-enable the N1 capability for this PLMN selection. As an implementation option, if the UE does not have a registered PLMN, instead of performing PLMN selection, the UE may select another RAT of the selected PLMN if the UE has chosen a PLMN and the RAT is supported by the UE; or

d) if no other allowed PLMN and RAT combinations are available, then the UE may re-enable the N1 mode capability for 3GPP access and indicate to lower layers to remain camped in NG-RAN or satellite NG-RAN of the registered PLMN, and may periodically scan for another PLMN and RAT combination which can provide EPS services or non-EPS services (if the UE supports EPS services or non-EPS services). How this periodic scanning is done, is UE implementation dependent.

When the UE is disabling the N1 mode capability for 3GPP access for an SNPN, it should proceed as follows:

a) enter the state 5GMM-REGISTERED.PLMN-SEARCH or 5GMM-DEREGISTERED.PLMN-SEARCH and perform SNPN selection as specified in 3GPP TS 23.122 [5]. If disabling of the N1 mode capability for 3GPP access was not due to a UE-initiated de-registration procedure for 5GS services over 3GPP access not due to switch-off, the UE may re-enable the N1 capability for this SNPN selection; or

b) if no other SNPN is available, then the UE may re-enable the N1 mode capability for 3GPP access and indicate to lower layers to remain camped in NG-RAN of the registered SNPN.

When the UE is disabling the N1 mode capability upon receiving cause value #31 "Redirection to EPC required" as specified in subclauses 5.5.1.2.5, 5.5.1.3.5 and 5.6.1.5, it should proceed as follows:

a) If the UE is in NB-N1 mode:

   1) if lower layers do not provide an indication that the current E-UTRA cell is connected to EPC or lower layers do not provide an indication that the current E-UTRA cell supports CIoT EPS optimizations that are supported by the UE, search for a suitable NB-IoT cell connected to EPC according to 3GPP TS 36.304 [25C];

   2) if lower layers provide an indication that the current E-UTRA cell is connected to EPC and the current E-UTRA cell supports CIoT EPS optimizations that are supported by the UE, perform a core network selection to select EPC as specified in subclause 4.8.4A.1; or

   3) if lower layers cannot find a suitable NB-IoT cell connected to EPC or there is no suitable NB-IoT cell connected to EPC which supports CIoT EPS optimizations that are supported by the UE, the UE, as an implementation option, may indicate to lower layers to remain camped in E-UTRA cell connected to 5GCN, may then start an implementation-specific timer and enter the state 5GMM-REGISTERED.LIMITED-SERVICE. The UE may may re-enable the N1 mode capability for 3GPP access at expiry of the

implementation-specific timer, if the timer had been started, and may then proceed with the appropriate 5GMM procedure.

b) If the UE is in WB-N1 mode:

1) if lower layers do not provide an indication that the current E-UTRA cell is connected to EPC or lower layers do not provide an indication that the current E-UTRA cell supports CIoT EPS optimizations that are supported by the UE, search for a suitable E-UTRA cell connected to EPC, or for the UE which supports CIoT EPS optimization select a satellite E-UTRA cell connected to EPC via "WB-E-UTRAN(LEO)", "WB-E-UTRAN(MEO)", or "WB-E-UTRAN(GEO)", according to 3GPP TS 36.304 [25C];

2) if lower layers provide an indication that the current E-UTRA cell is connected to EPC and the current E-UTRA cell supports CIoT EPS optimizations that are supported by the UE, then perform a core network selection to select EPC as specified in subclause 4.8.4A.1; or

3) if lower layers cannot find a suitable E-UTRA cell connected to EPC, or if the lower layers cannot find a suitable satellite E-UTRA cell via "WB-E-UTRAN(LEO)", "WB-E-UTRAN(MEO)", or "WB-E-UTRAN(GEO)", or there is no suitable E-UTRA cell connected to EPC, or there is no suitable satellite E-UTRA cell connected to EPC via "WB-E-UTRAN(LEO)", "WB-E-UTRAN(MEO)", or "WB-E-UTRAN(GEO)", which supports CIoT EPS optimizations that are supported by the UE, the UE, as an implementation option, may indicate to lower layers to remain camped in E-UTRA cell connected to 5GCN, may then start an implementation-specific timer and enter the state 5GMM-REGISTERED.LIMITED-SERVICE. The UE may re-enable the N1 mode capability for 3GPP access at expiry of the implementation-specific timer, if the timer had been started, and may then proceed with the appropriate 5GMM procedure.

When the UE supporting both N1 mode and S1 mode needs to stay in E-UTRA connected to EPC (e.g. due to the domain selection for UE originating sessions as specified in subclause 4.3.2), in order to prevent unintentional handover or cell reselection from E-UTRA connected to EPC to NG-RAN connected to 5GCN, the UE operating in single-registration mode shall disable the N1 mode capability for 3GPP access and:

a) shall set the N1mode bit to "N1 mode for 3GPP access not supported" in the UE network capability IE (see 3GPP TS 24.301 [15]) of the ATTACH REQUEST message and the TRACKING AREA UPDATE REQUEST message in EPC; and

b) the UE NAS layer shall indicate the access stratum layer(s) of disabling of the N1 mode capability for 3GPP access.

If the UE is required to disable the N1 mode capability for 3GPP access and select E-UTRA or another RAT, and the UE is in the 5GMM-CONNECTED mode,

- if the UE has a persistent PDU session, then the UE waits until the radio bearer associated with the persistent PDU session has been released;

- otherwise the UE shall locally release the established NAS signalling connection;

and enter the 5GMM-IDLE mode before selecting E-UTRA or another RAT.

If the UE is disabling its N1 mode capability for 3GPP access before selecting E-UTRA or another RAT, the UE shall not perform the UE-initiated de-registration procedure of subclause 5.5.2.2.

The UE shall re-enable the N1 mode capability for 3GPP access when the UE performs PLMN selection, SNPN selection or SNPN selection for onboarding services over 3GPP access, unless:

a) disabling of the N1 mode capability for 3GPP access was due to a UE-initiated de-registration procedure for 5GS services over 3GPP access not due to switch-off;

b) the UE has already re-enabled the N1 mode capability for 3GPP access when performing items c) or d) above; or

c) the UE disables the N1 mode capability for 3GPP access for cases described in subclauses 5.5.1.2.7 and 5.5.1.3.7.

If the disabling of N1 mode capability for 3GPP access was due to IMS voice is not available over 3GPP access and the UE's usage setting is "voice centric", the UE shall re-enable the N1 mode capability for 3GPP access when the UE's usage setting is changed from "voice centric" to "data centric", as specified in subclauses 4.3.3.

The UE should memorize the identity of the PLMN or SNPN where N1 mode capability for 3GPP access was disabled and should use that stored information in subsequent PLMN or SNPN selections as specified in 3GPP TS 23.122 [5].

If the disabling of N1 mode capability for 3GPP access was due to successful completion of an emergency services fallback, the criteria to enable the N1 mode capability again are UE implementation specific.

The UE shall disable the N1 mode capability for 3GPP access if requested by the upper layers (e.g. see subclause U.2.2.6.4 in 3GPP TS 24.229 [14]). If the UE disabled the N1 mode capability for 3GPP access based on the request from the upper layers (e.g. see subclause U.2.2.6.4 in 3GPP TS 24.229 [14]), the criteria to re-enable the N1 mode capability for 3GPP access after the completion of an emergency service are UE implementation specific.

If the N1 mode capability for 3GPP access was disabled due to the UE initiated de-registration procedure for 3GPP access or for 3GPP access and non-3GPP access and the UE is operating in single-registration mode (see subclause 5.5.2.2.3), upon request of the upper layers to re-register for 5GS services over 3GPP access or the UE needs to come out of unavailability period and resume normal services, the UE shall enable the N1 mode capability for 3GPP access again.

As an implementation option, the UE may start a timer for enabling the N1 mode capability for 3GPP access when the UE disables the N1 mode capability for 3GPP access. The UE should memorize the identity of the PLMNs or SNPNs where N1 mode capability for 3GPP access was disabled. On expiry of this timer:

a) if the UE is in Iu mode or A/Gb mode and is in idle mode as specified in 3GPP TS 24.008 [13], the UE should enable the N1 mode capability for 3GPP access;

b) if the UE is in Iu mode and a PS signalling connection exists, but no RR connection exists, the UE may abort the PS signalling connection before enabling the N1 mode capability for 3GPP access;

c) if the UE is in S1 mode and is in EMM-IDLE mode as specified in 3GPP TS 24.301 [15], the UE should enable the N1 mode capability for 3GPP access; and

d) If the UE is in Iu mode or A/Gb mode and an RR connection exists, the UE should delay enabling the N1 mode capability for 3GPP access until the RR connection is released. If the UE is in S1 mode and is in EMM-CONNECTED mode as specified in 3GPP TS 24.301 [15], the UE should delay enabling the N1 mode capability for 3GPP access until the NAS signalling connection in S1 mode is released.

When the UE enables the N1 mode capability for 3GPP access, the UE shall remove the PLMN or SNPN from the memorized identity of the PLMNs or SNPNs where N1 mode capability for 3GPP access was disabled.

NOTE 1: As described in 3GPP TS 23.122 [5], if the UE is in automatic PLMN selection mode or automatic SNPN selection mode, the UE does not consider the memorized PLMNs as PLMN selection candidates for NG-RAN access technology or satellite NG-RAN access technology or the memorized SNPN as SNPN selection candidates till the timer expires.

The UE may disable the N1 mode capability for currently camped PLMN or SNPN over 3GPP access (see 3GPP TS 23.122 [5]) if no network slice is available for the camped PLMN or SNPN (see subclauses 5.5.1.2.5 and 5.5.1.3.5). If the disabling of N1 mode capability for 3GPP access was due to no network slices available, the UE should memorize the identity of the PLMN or SNPN where N1 mode is disabled due to no available network slices or the list of SNPNs where N1 mode is disabled due to no available network slices, respectively. As an implementation option, the UE may start a timer T_{NSU} for enabling the N1 mode capability that was disabled due to no available network slices for the 3GPP access. The value of timer T_{NSU} is UE implementation specific. The UE should remove the memorized identity of the PLMNs or SNPNs where N1 mode is disabled due to no available network slice upon:

a) the expiry of the timer TNSU; or

b) receiving REGISTRATION ACCEPT message containing the Network slicing indication IE with the Network slicing subscription change indication set to “Network slicing subscription changed”.

NOTE 1A: If a network slice is temporarily unavailable to the UE due to the S-NSSAI time validity information or the S-NSSAI location validity information as described in subclauses 4.6.2.8 and 4.6.2.10 respectively, and no other network slice is available to the UE for the camped PLMN or SNPN, as an implementation option the UE can keep the N1 mode capability enabled for currently camped PLMN or SNPN over 3GPP access.

If the UE receives 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 6.5.1.3 of 3GPP TS 24.301 [15]), the UE may remove the PLMN ID from the memorized identity of the PLMNs where N1 mode is disabled due to no available network slices.

If the UE attempts to establish an emergency PDU session in a PLMN or SNPN where N1 mode capability was disabled due to the UE's registration attempt counter have reached 5, the UE may enable N1 mode capability for that PLMN memorized by the UE.

NOTE 2: If N1 mode capability is disabled due to the UE's registration attempt counter reaches 5, the value of the timer for re-enabling N1 mode capability is recommended to be the same as the value of T3502 which follows the handling specified in subclause 5.3.8. If the value of T3502 is indicated as zero by the network, an implementation specific non-zero value can be used for the timer for re-enabling N1 mode capability.

If the UE supports access to an SNPN providing access for localized services in SNPN and access for localized services in SNPN is enabled, then:

- the UE may re-enable the N1 mode capability for 3GPP access if disabled for that SNPN when:

  1) the validity information of the SNPN contained in the "credentials holder controlled prioritized list of preferred SNPNs for access for localized services in SNPN" changes from not met to met; or

  2) the validity information of a GIN broadcasted by an SNPN contained in the "credentials holder controlled prioritized list of preferred GINs for access for localized services in SNPN" changes from not met to met; and

- the UE need not re-enable N1 mode capability for 3GPP access for that SNPN if the N1 mode capability for 3GPP access for that SNPN was disabled due to 5GMM cause value #27 (N1 mode not allowed).

NOTE 3: If the UE receives a reject message with a 5GMM cause value and the N1 mode capability is disabled again for the SNPN, it is up to UE implementation whether to re-enable N1 mode capability for the SNPN if the validity information of the SNPN is still met.

4.9.3 Disabling and re-enabling of UE's N1 mode capability for non-3GPP access

When the UE disables the N1 mode capability for non-3GPP access, the UE NAS layer shall not initiate any 5GS NAS procedures towards the network over non-3GPP access.

When the UE supporting both N1 mode and S1 mode needs to stay in non-3GPP access connected to EPC (e.g. due to the domain selection for UE originating sessions as specified in subclause 4.3.2), in order to prevent unintentional selection of a non-3GPP access network connected to 5GCN, the UE operating in single-registration mode shall not transfer any PDN connection to a non-3GPP access network connected to the 5GCN.

If the disabling of N1 mode capability for non-3GPP access was due to IMS voice is not available over non-3GPP access in 5GS and the UE's usage setting is "voice centric", the UE shall re-enable the N1 mode capability for non-3GPP access when the UE's usage setting is changed from "voice centric" to "data centric" as specified in subclauses 4.3.3.

The UE shall re-enable the N1 mode capability for non-3GPP access when a new PLMN or SNPN is selected over non-3GPP access.

The UE may disable the N1 mode capability for the currently camped PLMN or SNPN over non-3GPP access if no network slice is available for the camped PLMN or SNPN.

As an implementation option, the UE may start a timer for re-enabling the N1 mode capability for non-3GPP access, after the N1 mode capability for non-3GPP access was disabled. On the expiry of this timer, the UE should re-enable the N1 mode capability for non-3GPP access.

4.9.4 Disabling and re-enabling of UE's satellite NG-RAN capability

Disable of the satellite NG-RAN capability shall only be performed when the UE is in 5GMM-IDLE mode.

When disabling the satellite NG-RAN capability, the UE:

a) may disable the NR NTN access capability (see 3GPP TS 38.304 [28] and 3GPP TS 38.306 [28A]);

b) shall memorize the identity of the PLMN where the satellite NG-RAN capability was disabled; and

c) shall use that stored information in subsequent PLMN selections as specified in 3GPP TS 23.122 [6].

NOTE: As an implementation option, the UE can disable satellite NG-RAN capability by disabling N1 mode capability for satellite NG-RAN access.

As an implementation option, the UE may start a timer for enabling satellite NG-RAN capability and on expiry of this timer UE shall remove the PLMN from the memorized identity of the PLMNs where the satellite NG-RAN capability was disabled.

4.10 Interworking with ePDG connected to EPC

In order to interwork with ePDG connected to EPC, the UE shall operate as specified in either subclause 4.8.2.3 or subclause 4.8.3. Which subclause the UE follows is chosen by the UE irrespective of the interworking without N26 interface indicator.

The UE shall not attempt to transfer PDU sessions with PDU session type "Ethernet" or "Unstructured" to an ePDG connected to EPC.

NOTE 1: PDU sessions with PDU session type "Ethernet" or "Unstructured" cannot be transferred to an ePDG connected to EPC because PDN connections with PDN type "non-IP" or PDN type "Ethernet" are not supported over ePDG connected to EPC.

The UE shall not attempt to transfer PDU sessions with the selected SSC mode set to "SSC mode 2" or "SSC mode 3" to an ePDG connected to EPC.

NOTE 2: Interworking between N1 mode over non-3GPP access and ePDG connected to EPC is not specified in this release of the specification.

4.11 UE configuration parameter updates

The 5GS in a PLMN supports updating UE parameters via NAS signalling. The feature enables the HPLMN to securely and dynamically re-configure the UE configuration parameters stored on the USIM and the ME.

- In this release of the specification, updates of the following USIM configuration parameters are supported:
  - routing indicator.
- In this release of specification, updates of the following ME configuration parameters are supported:
  - default configured NSSAI.
  - disaster roaming information.

The 5GS in an SNPN supports updating UE parameters via NAS signalling. The feature enables the SNPN to securely and dynamically re-configure the UE configuration parameter stored on the USIM if the UE used the USIM for registration to the SNPN.

- In this release of the specification, updates of the following USIM configuration parameters are supported:
  - routing indicator.
- In this release of specification, updates of the following ME configuration parameters are supported:
  - routing indicator.
  - default configured NSSAI.

The update of UE configuration parameters is initiated by the network using the network-initiated downlink NAS transport procedure as described in subclause 5.4.5.3. The ME acknowledgement of successful reception of the updated

UE configuration parameter information is sent back to the network using the UE-initiated uplink NAS transport procedure as described in subclause 5.4.5.2.

4.12 Access traffic steering, switching and splitting (ATSSS)

The ATSSS feature is an optional feature that may be supported by the UE and the 5GCN.

The ATSSS feature enables a multi-access PDU connectivity service, which can exchange PDUs between the UE and a data network by simultaneously using one 3GPP access network and one non-3GPP access network. The multi-access PDU connectivity service is realized by establishing a multi-access PDU session, i.e. a PDU session that can have user-plane resources on two access networks.

NOTE 1: MA PDU session is not applicable for CIoT 5GS optimization in this release of specification.

The UE can request an MA PDU session when the UE is registered via both 3GPP and non-3GPP accesses, or when the UE is registered via one access only. The MA PDU session management is performed based on the PDU session management procedures.

The detailed description of the procedures for ATSSS between the UE and the network across one 3GPP access network and one non-3GPP access network are specified in 3GPP TS 24.193 [13B].

NOTE 2: In this version of the specification, PDU set handling is not supported in an MA PDU session.

4.13 Support of NAS signalling using wireline access network

A 5G-RG, a W-AGF acting on behalf of an FN-RG or a W-AGF acting on behalf of an N5GC device can use wireline access network to access the 5GCN by using NAS signalling procedures as described in 3GPP TS 23.501 [8], 3GPP TS 23.502 [9] and 3GPP TS 23.316 [6D].

Wireline access is a type of non-3GPP access.

A 5G-RG simultaneously connected to the same 5GCN of a PLMN over a 3GPP access and a wireline access is connected to a single AMF.

5G-RG maintains the N1 NAS signalling connection with the AMF over the wireline access network after all the PDU sessions for the 5G-RG over that access have been released or handed over to 3GPP access.

The 5G-RG connected to 5GCN via NG-RAN is specified in 3GPP TS 23.316 [6D].

When accessing the 5GCN over 3GPP access, in addition to requirements specified for the 5G-RG in the present document, the 5G-RG shall also perform requirements specified in the present document for a UE accessing 5GCN over 3GPP access. When accessing the 5GCN over wireline access, in addition to requirements specified for the 5G-RG in the present document, the 5G-RG shall also perform requirements specified in the present document for a UE accessing 5GCN over non-3GPP access. If a requirement specified for the 5G-RG in the present document contradicts a requirement specified for the UE in the present document, the 5G-RG shall perform the requirement specified in the present document for the 5G-RG.

For the scenario of FN-RG, which does not support N1 mode, the W-AGF acting on behalf of the FN-RG exchanges NAS signalling messages with an AMF.

For the scenario of N5GC device, which does not support N1 mode, the W-AGF acting on behalf of the N5GC device exchanges NAS signalling messages with an AMF.

For the scenario of AUN3 device, which does not support N1 mode, the 5G-RG acting on behalf of the AUN3 device exchanges NAS signalling messages with an AMF. If the 5G-RG is not registered and connected to the 5GCN over wireline access, the 5G-RG acting on behalf of an AUN3 device shall not initiate the initial registration procedure on behalf of the AUN3 device.

NOTE 1: The 5G-RG acting on behalf of an AUN3 device maintains a 5GMM context for each AUN3 device behind it. The AMF maintains a 5GMM context for each AUN3 device. The AMF is not aware of any association between the 5GMM context of the 5G-RG and the 5GMM context of the AUN3 device.

When the 5G-RG acting on behalf of an AUN3 device initiates the initial registration procedure on behalf of the AUN3 device, the 5G-RG shall not include the requested NSSAI in the REGISTRATION REQUEST message.

For the scenario of NAUN3 device, which does not support N1 mode, the 5G-RG acting on behalf of a connectivity group consisting of one or more NAUN3 devices exchanges NAS signalling messages with an AMF.

NOTE 2: It is also possible for 5G-RG that is connected to 5GCN via NG-RAN to act on behalf of a connectivity group consisting of one or more NAUN3 devices as specified in 3GPP TS 23.316 [6D].

In addition to requirements specified for the W-AGF acting on behalf of the FN-RG (or on behalf of the N5GC device) in the present document, the W-AGF acting on behalf of the FN-RG (or on behalf of the N5GC device) shall also perform requirements specified in the present document for a UE accessing 5GCN over non-3GPP access. If a requirement specified for the W-AGF acting on behalf of the FN-RG (or on behalf of the N5GC device) in the present document contradicts a requirement specified for the UE in the present document, the W-AGF acting on behalf of the FN-RG (or on behalf of the N5GC device) shall perform requirement specified in the present document for the W-AGF acting on behalf of the FN-RG (or on behalf of the N5GC device).

The PDU session authentication and authorization procedure is not supported in a PDU session established by the W-AGF acting on behalf of the FN-RG or on behalf of the N5GC device.

The W-AGF acting on behalf of the N5GC device requests the establishment of a PDU Session on behalf of the N5GC device upon registration. Only one PDU session per N5GC device is supported.

The 5G-RG acting on behalf of an AUN3 device requests the establishment of a PDU Session on behalf of the AUN3 device upon registration. Only one PDU session per AUN3 is supported.

The 5G-RG acting on behalf of a connectivity group consisting of one or more NAUN3 devices requests the establishment of a PDU Session on behalf of the connectivity group. Only one PDU session per the connectivity group is supported, where all the NAUN3 devices in the connectivity group share the same PDU session.

A 5G-RG or an FN-RG provide a non-3GPP access network to UEs. A UE connected to a non-3GPP access network provided by the 5G-RG or the FN-RG can access to the 5GCN via the N3IWF or via the TNGF as described in 3GPP TS 23.316 [6D].

The 5G-RG or the W-AGF acting on behalf of the FN-RG shall indicate "ANDSP not supported by the UE" in the UE policy classmark IE during the UE-initiated UE state indication procedure as specified in subclause D.2.2.

The 5G-RG or the W-AGF acting on behalf of the FN-RG shall indicate "Reporting URSP rule enforcement not supported by the UE" in the UE policy classmark IE during the UE-initiated UE state indication procedure as specified in subclause D.2.2.

The Non-3GPP QoS Assistance Information (N3QAI) is introduced to enable a 5G-RG to perform the QoS differentiation for the UE behind the 5G-RG, the AUN3 device behind the 5G-RG or the NAUN3 device behind the 5G-RG. The network may provide the N3QAI associated with the QoS flow during the PDU session establishment procedure as defined in subclause 6.4.1 or during the PDU session modification procedure as defined in subclause 6.4.2.

NOTE 3: How the 5G-RG applies N3QAI is outside the scope of the present document.

If the AMF receives an indication from the W-AGF that there is no 5G-RG connected to the same wireline for an AUN3 device as specified in 3GPP TS 23.316 [6D], the AMF shall locally de-register the AUN3 device.

4.14 Non-public network (NPN)

4.14.1 General

Two types of NPN can be deployed using 5GS: SNPN (see subclause 4.14.2) and PNI-NPN (see subclause 4.14.3).

4.14.2 Stand-alone non-public network (SNPN)

If the UE is not SNPN enabled, the UE is always considered to be not operating in SNPN access operation mode. If the UE is SNPN enabled, the UE can operate in SNPN access operation mode. Details of activation and deactivation of SNPN access operation mode at the SNPN-enabled UE are up to UE implementation.

The functions and procedures of NAS described in the present document are applicable to an SNPN and an SNPN-enabled UE unless indicated otherwise. The key differences brought by the SNPN to the NAS layer are as follows:

a) instead of the PLMN selection process, the SNPN selection process is performed by a UE operating in SNPN access operation mode (see 3GPP TS 23.122 [5] and 3GPP TS 24.502 [18] for further details on the SNPN selection);

b) a "permanently forbidden SNPNs" list and a "temporarily forbidden SNPNs" list are managed per access type independently (i.e. 3GPP access or non-3GPP access) and, if the UE supports access to an SNPN using credentials from a credentials holder, equivalent SNPNs or both, per entry of the "list of subscriber data" or, if the UE supports access to an SNPN using credentials from a credentials holder, per the PLMN subscription, by a UE operating in SNPN access operation mode instead of forbidden PLMN lists. If the UE supports onboarding services in SNPN, an additional "permanently forbidden SNPNs for onboarding services in SNPN" list and an additional "temporarily forbidden SNPNs for onboarding services in SNPN" list are managed. If the UE supports access to an SNPN providing access for localized services in SNPN, an additional "permanently forbidden SNPNs for access for localized services in SNPN" list and an additional "temporarily forbidden SNPNs for access for localized services in SNPN" list per entry of the "list of subscriber data" and per the PLMN subscription are managed for 3GPP access only. These lists shall be maintained across activation and deactivation of SNPN access operation mode;

NOTE 0: On timer T3245 expiry when the UE supports access to an SNPN using credentials from a credentials holder using PLMN subscription, and the UE is not operating in SNPN access operation mode, as an implementation option the UE can delete the list of "temporarily forbidden SNPNs" and "permanently forbidden SNPNs" and additionally the list of "permanently forbidden SNPNs for access for localized services in SNPN" and list of "temporarily forbidden SNPNs for access for localized services in SNPN" if the UE supports access to an SNPN providing access for localized services in SNPN.

c) inter-system change to and from S1 mode is not supported;

d) void;

e) CAG is not supported in SNPN access operation mode;

f) with respect to the 5GMM cause values:

   1) 5GMM cause values #74 "Temporarily not authorized for this SNPN" and #75 "Permanently not authorized for this SNPN" are supported whereas these 5GMM cause values cannot be used in a PLMN; and

   2) 5GMM cause values #11 "PLMN not allowed", #31 "Redirection to EPC required", #73 "Serving network not authorized", and #76 "Not authorized for this CAG or authorized for CAG cells only" are not supported whereas these 5GMM cause values can be used in a PLMN;

g) a list of "5GS forbidden tracking areas for roaming" and a list of "5GS forbidden tracking areas for regional provision of service" are managed per SNPN and, if the UE supports access to an SNPN using credentials from a credentials holder, equivalent SNPNs or both, entry of the "list of subscriber data" or, if the UE supports access to an SNPN using credentials from a credentials holder,PLMN subscription (see 3GPP TS 23.122 [5]);

h) when accessing SNPN services via a PLMN using 3GPP access, access to 5GCN of the SNPN is performed using 5GMM procedures for non-3GPP access, 5GMM parameters for non-3GPP access, the UE is performing access to SNPN over non-3GPP access and the UE is not operating in SNPN access operation mode over 3GPP access. When accessing PLMN services via a SNPN using 3GPP access, access to 5GCN of the PLMN is performed using 5GMM procedures for non-3GPP access, 5GMM parameters for non-3GPP access, the UE is not performing access to SNPN over non-3GPP access, and the UE is operating in SNPN access operation mode over 3GPP access. From the UE's NAS perspective, accessing PLMN services via an SNPN and accessing SNPN services via a PLMN are treated as untrusted non-3GPP access. If the UE is accessing the PLMN using non-3GPP access, the access to 5GCN of the SNPN via PLMN is not specified in this release of the specification.

   Emergency services are not supported in an SNPN when a UE accesses SNPN services via a PLMN;

i) when registered to an SNPN, the UE shall use only the UE policies provided by the registered SNPN;

j) inclusion of a TAI of an SNPN other than the registered SNPN, into the registration area is not supported. The AMF of an SNPN shall only include into the registration area one or more TAIs of the registered SNPN;

j1) inclusion of a TAI of an SNPN other than the registered SNPN, into the LADN service area is not supported. The AMF of an SNPN shall only include one or more TAIs of the registered SNPN into the LADN service area;

j2) inclusion of a TAI of an SNPN other than the registered SNPN, into the allowed area or the non-allowed area, of the 3GPP access service area restrictions is not supported. The AMF of an SNPN shall include only one or more TAIs of the registered SNPN into the allowed area or the non-allowed area, of the 3GPP access service area restrictions;

k) void;

l) void;

m) UE mobility between SNPNs in 5GMM-CONNECTED mode is supported when the SNPNs are equivalent SNPNs for the selected entry of the "list of subscriber data" or the selected PLMN subscription. UE mobility between SNPNs in 5GMM-IDLE mode is supported when the UE supports access to an SNPN using credentials from a credentials holder or when the SNPNs are equivalent SNPNs or both for the selected entry of the "list of subscriber data" or the selected PLMN subscription. UE mobility between an SNPN and a PLMN is not supported;

n) CIoT 5GS optimizations are not supported;

o) void;

p) when registering or registered to an SNPN, the UE shall handle the 5GS mobile identity as described in subclause 5.5.1.2.2;

q) when registering or registered to an SNPN, the UE shall only consider:

   1) a last visited registered TAI visited in the same SNPN as an available last visited registered TAI; or

   2) a last visited registered TAI visited using the same entry of the "list of subscriber data" or the same PLMN subscription as an available last visited registered TAI, if the UE supports access to an SNPN using credentials from a credentials holder, equivalent SNPNs or both;

NOTE 1: If the last visited registered TAI is assigned by an SNPN other than the current SNPN, the serving AMF can determine the SNPN assigning the last visited registered TAI using the NID provided by the UE.

r) emergency service fallback is not supported;

s) when registering or registered for onboarding services in SNPN, the UE shall not provide the requested NSSAI to the network;

s1) when performing initial registration for onboarding services in SNPN, the UE shall set the 5GS registration type value to "SNPN onboarding registration";

t) when registering or registered for onboarding services in SNPN, the AMF shall not provide the configured NSSAI, the allowed NSSAI or the rejected NSSAI to the UE, shall use the S-NSSAI included in the AMF onboarding configuration data for onboarding services in SNPN and shall not perform NSSAA procedure for S-NSSAI used for onboarding services in SNPN;

u) the UE can access an SNPN indicating that onboarding is allowed using default UE credentials for primary authentication in order for the UE to be configured with one or more entries of the "list of subscriber data";

x) eCall over IMS is not supported in SNPN access operation mode and the UE ignores any USIM configuration for eCall only mode;

y) when registering or registered for onboarding services in SNPN, the AMF shall store in the 5GMM context of the UE an indication that the UE is registered for onboarding services in SNPN;

z) a UE with multiple valid entries of "list of subscriber data", or one or more valid USIMs and one or more valid entries of "list of subscriber data", capable of initiating and maintaining simultaneous separate registration states over 3GPP access with PLMN(s) or SNPN(s), using identities and credentials associated with those entries of "list of subscriber data", or USIMs and entries of "list of subscriber data", and supporting one or more of the N1 NAS signalling connection release, the paging indication for voice services, the reject paging request, the paging restriction and the paging timing collision control may use procedures defined for MUSIM UE, even if the UE does not include multiple valid USIMs;

za) when the UE is registering or registered for onboarding services in SNPN, the network slice admission control is not performed;

NOTE 2: If the network determines that the UE cannot register to the onboarding SNPN due to lack of resources for the network slice used for onboarding, the AMF can reject the UE with 5GMM cause #22 "congestion".

zb) when the UE is registered for onboarding services in SNPN (as specified in subclause 3.1), the UE determines that the number dialled is an emergency number, and emergency services are not supported in the SNPN, the UE shall perform a local de-registration and utilize the procedures specified in 3GPP TS 23.167 [6] and 3GPP TS 24.229 [14] to select a domain for the emergency session attempt; and

NOTE 3: The UE can select PS domain for emergency session attempt.

v) proximity based services (5G ProSe as specified in 3GPP TS 24.554 [19E]) are not supported.

4.14.3 Public network integrated non-public network (PNI-NPN)

A PNI-NPN is made available by means of e.g. dedicated DNNs or by one or more S-NSSAIs allocated for it. A CAG can be optionally used in order to prevent UEs not allowed to access a PNI-NPN from accessing the PNI-NPN. The key enablers for the CAG in the NAS layer are as follows:

a) CAG selection (see 3GPP TS 23.122 [5]); and

b) provisioning of a "CAG information list" as specified in 3GPP TS 23.122 [5], from network to UE via the generic UE configuration update procedure, the registration procedure, the service request procedure, and the network-initiated de-registration procedure.

The "CAG information list" provisioned by the network, if available, is stored in the non-volatile memory in the ME as specified in annex C. The "CAG information list" stored in the ME is kept when the UE enters 5GMM-DEREGISTERED state. Annex C specifies condition under which the "CAG information list" stored in the ME is deleted. Additionally, when a USIM is inserted, if:

- no "CAG information list" is stored in the non-volatile memory of the ME; or

- the SUPI from the USIM does not match the SUPI stored together with the "CAG information list" in the non-volatile memory of the ME;

and the UE has a "CAG information list" stored in the USIM (see 3GPP TS 31.102 [22]), the UE shall store the "CAG information list" from the USIM into the ME, as specified in annex C. The "Allowed CAG list" included in the entry for the HPLMN or EHPLMN in "CAG information list" stored in the USIM can contain a range of CAG-IDs.

The UE supporting CAG may perform the initial registration for emergency services via a non-CAG cell in a PLMN for which the UE has an "indication that the UE is only allowed to access 5GS via CAG cells" or via a CAG cell for which none of CAG-ID(s) is authorized based on the "Allowed CAG list" (see 3GPP TS 23.122 [5]) for the selected PLMN. If a UE supporting CAG having an emergency PDU session is camping on:

a) a CAG cell and none of the CAG-ID(s) of the CAG cell is authorized based on the "Allowed CAG list" for the current PLMN in the UE's subscription; or

b) a non-CAG cell in a PLMN for which the UE's subscription contains an "indication that the UE is only allowed to access 5GS via CAG cells";

the AMF shall behave as specified in subclause 5.4.4.2, 5.5.1.3.4 or 5.6.1.4.1.

NOTE: The emergency services in a PLMN for which the UE's subscription contains an "indication that the UE is only allowed to access 5GS via CAG cells" can be subject to local regulation.

Proximity based services (5G ProSe as specified in 3GPP TS 24.554 [19E]) are not supported in this release of the specification when a UE is camping on a CAG cell.

If a UE supporting enhanced CAG information is in a CAG cell with a CAG-ID which:

a) was authorized based on the "Allowed CAG list" associated with the current PLMN in the "CAG information list" stored in the ME; and

b) becomes not authorized based on the "Allowed CAG list" (e.g., time validity information no longer matches UE's current time); and

none of the CAG-ID(s) supported by the current CAG cell is currently authorized based on the "Allowed CAG list" of the entry for the current PLMN in the stored "CAG information list", and:

a) the entry for the current PLMN in the "CAG information list" does not include an "indication that the UE is only allowed to access 5GS via CAG cells", then the UE shall abort ongoing UE initialted 5GMM procedures, if any, locally release the NAS signalling connection, if any, 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 stored "CAG information list"; or

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

   1) one or more CAG-ID(s) are authorized based on the "Allowed CAG list" of the entry for the current PLMN in the stored "CAG information list", the UE shall abort ongoing UE initialted 5GMM procedures, if any, locally release the NAS signalling connection, if any, 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 stored "CAG information list"; or

   2) no CAG-ID is authorized based on the "Allowed CAG list" of the entry for the current PLMN in the stored "CAG information list" and:

      i) the UE does not have an emergency PDU session, then the UE shall abort ongoing UE initialted 5GMM procedures, if any, locally release the NAS signalling connection, if any, enter the state 5GMM-REGISTERED.PLMN-SEARCH and shall apply the PLMN selection process defined in 3GPP TS 23.122 [5] with the stored "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;

4.15 Time synchronization and time sensitive communication

4.15.1 General

A 5GS can support time synchronization and TSC (see 3GPP TS 23.501 [8], 3GPP TS 23.502 [9], and 3GPP TS 23.503 [10]). This subclause describes NAS-specific aspects of the 5GS features to support time synchronization and TSC. Interworking with EPS is not supported for a PDU session for time synchronization or TSC.

4.15.2 Void

4.15.2.1 Void

4.15.2.2 Void

4.15.2.3 Void

4.15.3 Time synchronization

Two types of synchronization processes are supported by the 5GS: 5GS synchronization and (g)PTP domain synchronization (see 3GPP TS 23.501 [8]).

For 5GS synchronization, the lower layers provide the 5G internal system clock signalled via the NG-RAN (see 3GPP TS 38.331 [30]) and the UE forwards the 5G internal system clock to the DS-TT(s).

For (g)PTP domain synchronization, the UE supports forwarding (g)PTP messages (see 3GPP TS 23.501 [8], 3GPP TS 23.502 [9], and 3GPP TS 24.535 [19A]). For all (g)PTP domains associated with a PDU session:

a) if the UE receives (g)PTP message via the PDU session, the UE forwards the (g)PTP messages to the DS-TT associated with the PDU session; or

b) if the UE receives (g)PTP messages from the DS-TT associated with the PDU session, the UE forwards the (g)PTP messages via the PDU session.

Depending on the 5G access stratum-based time distribution or (g)PTP-based time distribution, the network timing synchronization status of the nodes involved in the operation (e.g., NG-RAN nodes, NW-TTs) may change. Using the 5GMM protocol, the network can request a supporting UE to reconnect to the network upon receiving an indication of a change in the RAN timing synchronization status.

4.15.4 User plane node management

A 5G system (5GS) can act as a user plane node of an external network (e.g. IEEE TSN bridge) or a 5GS can be independently used to enable TSC. For these purposes, information available at a UE is provided to the network and port management information containers are exchanged between a DS-TT and a TSN AF or a TSCTSF (see 3GPP TS 24.539 [19BA]).

During a UE-requested PDU session establishment procedure, if the UE supports transfer of port management information containers, then the UE indicates that transfer of port management information container is supported and the UE provides a DS-TT Ethernet port MAC address (if the PDU session type is Ethernet), port management information container, and a UE-DS-TT residence time (if available) to the network (see subclause 6.4.1.2).

Once the UE has successfully established a PDU session and the UE has indicated that transfer of port management information container is supported during the UE-requested PDU session establishment procedure (see subclause 6.4.1.2), then port management information containers are exchanged via a UE-requested PDU session modification procedure and a network-requested PDU session modification procedure (see subclauses 6.3.2 and 6.4.2). The UE receiving a port management information container from the network shall forward the port management information container to the DS-TT. The SMF receiving a port management information container from the UE shall operate as described in 3GPP TS 23.502 [9].

4.16 UE radio capability signalling optimisation

UE radio capability signalling optimisation (RACS) is a feature that is optional at both the UE and the network and which aims to optimise the transmission of UE radio capability over the radio interface (see 3GPP TS 23.501 [8]). RACS works by assigning an identifier to represent a set of UE radio capabilities. This identifier is called the UE radio capability ID. A UE radio capability ID can be either manufacturer-assigned or network-assigned. The UE radio capability ID is an alternative to the signalling of the radio capabilities container over the radio interface.

In this release of the specification, RACS is applicable to neither NB-N1 mode nor non-3GPP access.

If the UE supports RACS:

a) the UE shall indicate support for RACS by setting the RACS bit to "RACS supported" in the 5GMM capability IE of the REGISTRATION REQUEST message;

b) if the UE performs a registration procedure for initial registration and the UE has an applicable UE radio capability ID for the current UE radio configuration in the selected network, the UE shall include the UE radio capability ID in the UE radio capability ID IE as a non-cleartext IE in the REGISTRATION REQUEST message. If both a network-assigned UE radio capability ID and a manufacturer-assigned UE Radio Capability ID are applicable, the UE shall include the network-assigned UE radio capability ID in the REGISTRATION REQUEST message;

c) if the radio configuration at the UE changes (for instance because the UE has disabled a specific radio capability) then:

   1) if the UE has an applicable UE radio capability ID for the new UE radio configuration, the UE shall initiate a registration procedure for mobility and periodic registration update. The UE shall include the applicable UE radio capability ID in the UE radio capability ID IE of the REGISTRATION REQUEST message and shall include the 5GS update type IE in the REGISTRATION REQUEST message with the NG-RAN-RCU bit set to "UE radio capability update needed". If both a network-assigned UE radio capability ID and a

manufacturer-assigned UE Radio Capability ID are applicable, the UE shall include the network-assigned UE radio capability ID in the REGISTRATION REQUEST message; and

2) if the UE does not have an applicable UE radio capability ID for the new UE radio configuration, the UE shall initiate a registration procedure for mobility and periodic registration update and include the 5GS update type IE in the REGISTRATION REQUEST message with the NG-RAN-RCU bit set to "UE radio capability update needed";

NOTE: Performing the registration procedure for mobility and periodic registration update and including the 5GS update type IE in the REGISTRATION REQUEST message with the NG-RAN-RCU bit set to "UE radio capability update needed" without a UE radio capability ID included in the REGISTRATION REQUEST message can trigger the network to assign a new UE radio capability ID to the UE.

d) upon receiving a network-assigned UE radio capability ID in the REGISTRATION ACCEPT message or the CONFIGURATION UPDATE COMMAND message, the UE shall store the network-assigned UE radio capability ID and the PLMN ID or SNPN identity of the serving network and, if the UE supports access to an SNPN using credentials from a credentials holder, equivalent SNPNs or both, the selected entry of the "list of subscriber data" or the selected PLMN subscription along with a mapping to the current UE radio configuration in its non-volatile memory as specified in annex C. The UE shall be able to store at least the last 16 received network-assigned UE radio capability IDs with the associated PLMN ID or SNPN identity and, if the UE supports access to an SNPN using credentials from a credentials holder, equivalent SNPNs or both, the selected entry of the "list of subscriber data" or the selected PLMN subscription and the mapping to the corresponding UE radio configuration;

e) the UE shall not use a network-assigned UE radio capability ID assigned by a PLMN in PLMNs equivalent to the PLMN which assigned it or by an SNPN in SNPNs equivalent to the SNPN which assigned it;

f) upon receiving a UE radio capability ID deletion indication IE set to "Network-assigned UE radio capability IDs deletion requested" in the REGISTRATION ACCEPT message or the CONFIGURATION UPDATE COMMAND message, the UE shall delete all network-assigned UE radio capability IDs stored at the UE for the serving network, initiate a registration procedure for mobility and periodic registration update and include an applicable manufacturer-assigned UE radio capability ID for the current UE radio configuration, if available at the UE, in the UE radio capability ID IE of the REGISTRATION REQUEST message; and

g) if the UE performs a registration procedure for mobility and periodic registration update due to entering a tracking area that is not in the list of tracking areas that the UE previously registered in the AMF and the UE has an applicable UE radio capability ID for the current UE radio configuration in the selected network, the UE shall include the UE radio capability ID in the UE radio capability ID IE as a non-cleartext IE in the REGISTRATION REQUEST message. If both a network-assigned UE radio capability ID and a manufacturer-assigned UE Radio Capability ID are applicable, the UE shall include the network-assigned UE radio capability ID in the REGISTRATION REQUEST message.

If the network supports RACS:

a) the network may assign a network-assigned UE radio capability ID to a UE which supports RACS by including a UE radio capability ID IE in the REGISTRATION ACCEPT message or in the CONFIGURATION UPDATE COMMAND message;

b) the network may trigger the UE to delete all network-assigned UE radio capability IDs stored at the UE for the serving network by including a UE radio capability ID deletion indication IE set to "Network-assigned UE radio capability IDs deletion requested" in the REGISTRATION ACCEPT message or in the CONFIGURATION UPDATE COMMAND message; and

c) the network may send an IDENTITY REQUEST message to the UE that supports RACS to retrieve the PEI, if not available in the network.

4.17 5GS mobility management in NB-N1 mode

A UE in NB-N1 mode (see 3GPP TS 36.331 [25A]) shall calculate the value of the applicable NAS timer indicated in table 10.2.1 plus 240s.

The timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not re-calculate the use of the NAS timer value until the NAS procedure is completed, restarted or aborted.

When an AMF that supports NB-N1 mode performs NAS signalling with a UE, which is using NB-N1 mode, the AMF shall calculate the value of the applicable NAS timer indicated in table 10.2.2 plus 240s.

The timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not re-calculate the use of the NAS timer value until the NAS procedure is completed, restarted or aborted.

4.18 5GS session management in NB-N1 mode

A UE in NB-N1 mode (see 3GPP TS 36.331 [25A]) shall calculate the value of the applicable NAS timer indicated in table 10.3.1 plus 180s.

The timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not re-calculate the use of the NAS timer value until the NAS procedure is completed, restarted or aborted.

When an SMF that supports NB-N1 mode performs NAS signalling with a UE, which is using NB-N1 mode, the SMF shall calculate the value of the applicable NAS timer indicated in table 10.3.2 plus 180s.

The timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not re-calculate the use of the NAS timer value until the NAS procedure is completed, restarted or aborted.

4.19 5GS mobility management in WB-N1 mode for IoT

In WB-N1 mode, a UE operating in category CE can operate in either CE mode A or CE mode B (see 3GPP TS 36.306 [25D]). If a UE that supports CE mode B and operates in WB-N1 mode, the UE's usage setting is not set to "voice centric" (see 3GPP TS 23.501 [8]), and:

a) the use of enhanced coverage is not restricted by the network; or

b) CE mode B is not restricted by the network (see 3GPP TS 23.501 [8]);

the UE shall apply the value of the applicable NAS timer indicated in table 10.2.1 for WB-N1/CE mode.

A UE that supports CE mode B and operates in WB-N1 mode shall not apply the value of the applicable NAS timer indicated in table 10.2.1 for WB-N1/CE mode before receiving an indication from the network that the use of enhanced coverage is not restricted, or CE mode B is not restricted, as described in this subclause.

The NAS timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure, and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

The support of CE mode B by a UE is indicated to the AMF by lower layers and shall be stored by the AMF. When an AMF that supports WB-N1 mode performs NAS signalling with a UE, which supports CE mode B and operates in WB-N1 mode, the UE's usage setting is not set to "voice centric" (see 3GPP TS 23.501 [8]) and the AMF determines that:

a) the use of enhanced coverage is not restricted for the UE; or

b) CE mode B is not restricted for the UE (see 3GPP TS 23.501 [8]);

the AMF shall calculate the value of the applicable NAS timer indicated in table 10.2.2 for WB-N1/CE mode.

The NAS timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

4.20 5GS session management in WB-N1 mode for IoT

In WB-N1 mode, a UE operating in category CE can operate in either CE mode A or CE mode B (see 3GPP TS 36.306 [25D]). If a UE that supports CE mode B and operates in WB-N1 mode and the UE's usage setting is not set to "voice centric" (see 3GPP TS 23.501 [8]), and:

a) the use of enhanced coverage is not restricted by the network; or

b) CE mode B is not restricted by the network (see 3GPP TS 23.501 [8]);

the UE shall apply the value of the applicable NAS timer indicated in table 10.3.1 for WB-N1/CE mode.

A UE that supports CE mode B and operates in WB-N1 mode shall not apply the value of the applicable NAS timer indicated in table 10.3.1 for WB-N1/CE mode before receiving an indication from the network that the use of enhanced coverage is not restricted, or CE mode B is not restricted, as described in this subclause.

The NAS timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure, and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

If the use of extended NAS timer is indicated by the AMF (see 3GPP TS 23.501 [8] and 3GPP TS 23.502 [9]), the SMF shall calculate the value of the applicable NAS timer indicated in table 10.3.2 for WB-N1/CE mode.

The NAS timer value obtained is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

4.21 Authentication and Key Management for Applications (AKMA)

The UE may support AKMA.

The purpose of AKMA is to provide authentication and key management to applications based on 3GPP credentials used for 5GS access as specified in 3GPP TS 33.535 [24A], which allows the UE to securely exchange data with an AKMA application function.

Upon receiving a request from the upper layers to obtain AKMA Anchor Key (K_{AKMA}) and AKMA Key Identifier (A-KID), the UE supporting AKMA shall derive the K_{AKMA} and the AKMA Temporary Identifier (A-TID) from the valid K_{AUSF} if available as specified in 3GPP TS 33.535 [24A], shall further derive the A-KID from the A-TID as specified in 3GPP TS 33.535 [24A] and shall provide K_{AKMA} and A-KID to the upper layers.

The UE supporting AKMA shall notify the upper layers whenever there is a change of the K_{AUSF} upon reception of an EAP-success message in subclauses 5.4.1.2.2.8, 5.4.1.2.3.1 and 5.4.1.2.3A.1 or upon reception of SECURITY MODE COMMAND message in subclauses 5.4.2.3.

During an ongoing primary authentication and key agreement procedure (see subclause 5.4.1), if the UE receives a request from upper layers to obtain K_{AKMA} and A-KID, the UE shall derive the K_{AKMA} and A-TID after the completion of the ongoing primary authentication and key agreement procedure, shall further derive the A-KID from the A-TID as specified in 3GPP TS 33.535 [24A] and shall provide K_{AKMA} and A-KID to the upper layers.

NOTE 1: The upper layers derive the AKMA Application Key (K_{AF}) from K_{AKMA} as specified in 3GPP TS 33.535 [24A].

NOTE 2: The knowledge of whether a certain application needs to use AKMA or not is application specific and is out of the scope of 3GPP.

NOTE 3: The exact method of securing the data exchange at the upper layers using K_{AF} is application specific and is out of the scope of 3GPP.

NOTE 4: The upper layers request the UE NAS layer to provide K_{AKMA} and A-KID before the upper layers initiate communication with an AKMA application function.

NOTE 5: Upon receiving a request from the upper layers to obtain K_{AKMA} and A-KID, if there is no K_{AUSF} available, the UE NAS layer cannot derive the K_{AKMA} and A-KID and provides an indication to the upper layers that K_{AKMA} and A-KID cannot be generated.

4.22 Uncrewed aerial vehicle identification, authentication, and authorization

4.22.1 General

A 5GS can support UAV identification, authentication, and authorization (see 3GPP TS 23.256 [6AB]). This subclause describes NAS-specific aspects of the 5GS features to support UAV identification, authentication, authorization and C2 communication authorization.

Before accessing 5GS for UAS services, the UE supporting UAS services must have an assigned CAA-level UAV ID. The UE can be registered to 5GS for UAS services if there is a valid aerial subscription in the UE's subscription.

4.22.2 Authentication and authorization of UAV

The 5GS supports the USS UAV Authorization and Authentication (UUAA) procedure for a UE supporting UAS services. Depending on operator policy or regulatory requirements, the UUAA-MM procedure can be performed by the UE and the AMF at a registration procedure as specified in subclause 5.5.1.2, the UUAA-SM procedure can be performed by the UE and the SMF at a PDU session establishment procedure as specified in subclause 6.4.1.2, or both can be performed. The UE shall support UUAA-MM and UUAA-SM, and the network shall support UUAA-SM and may optionally support UUAA-MM. The UUAA procedure needs to be performed by 5GS with USS successfully before the connectivity for UAS services is established.

During the registration procedure as described in subclause 5.5.1.2, the UE supporting UAS services provides CAA-level UAV ID to the AMF, and the AMF may trigger the UUAA-MM procedure. If the UE supporting UAS services does not provide CAA-level UAV ID to the AMF and the network is configured to perform UUAA-MM at registration procedure, the AMF may accept the registration request and shall mark in the UE's 5GMM context that the UE is not allowed to request UAS services. If the UE wants to use the UAS services by providing the CAA-Level UAV ID later on, the UE shall perform the registration procedure for mobility and periodic registration update.

When a UE supporting UAS services requests to establish a PDU session as described in subclause 6.4.1.2 for USS communication, the UE provides CAA-level UAV ID to the network, and the SMF may trigger the UUAA-SM procedure based on the DNN and S-NSSAI combination for aerial services according to the user's subscription data and the CAA-level UAV ID provided by the UE.

If the UE does not provide CAA-level UAV ID and the user’s subscription data for the UE requires the UUAA-SM, the network rejects the UE-requested PDU session establishment procedure for the UAS services.

The UE supporting UAS services shall not provide CAA-level UAV ID to the network over non-3GPP access, and the network shall not perform UUAA procedure for non-3GPP access and shall ensure that the UE is not allowed to access any aerial services in non-3GPP access.

If provided by the upper layers, the UE supporting UAS services provides to the network the USS address during the registration procedure or PDU session establishment procedure so that the network uses the information to discover the USS.

NOTE: The parameters (e.g., CAA-level UAV ID or USS address) sent by a UE supporting UAS services to the network for UAS services are included in the Service-level-AA container IE which is a non-cleartext IE.

After successful UUAA procedure, either the AMF or the SMF may initiate re-authentication of the UAV when required by the USS. If UUAA-MM fails during a re-authentication and there are PDU sessions established using UAS services, the AMF shall request the SMF to perform the release of these PDU sessions and may trigger a network-initiated de-registration procedure based on operator policy. If UUAA-SM fails during a re-authentication, the SMF shall release the PDU session related to re-authentication.

If the UUAA is revoked, the PDU session related to the UAS services shall be released by the SMF. Based on operator policy, the AMF may decide to keep the UE registered or trigger a de-registration procedure.

4.22.3 Authorization of C2 communication

The 5GS supports USS authorization of C2 communication for pairing of UAV and UAV-C. The pairing of UAV and UAV-C needs to be authorized by USS successfully before the user plane connectivity for C2 communication (over Uu or over NR-PC5) is enabled. For C2 authorization procedure, the UE supporting UAS services provides to the network with CAA-level UAV ID.

The USS authorization of UAV flight can also be performed during the C2 authorization procedure. The UE supporting UAS services provides the UAV flight authorization information to the network if provided by upper layers.

NOTE 1: The C2 authorization payload in the service-level-AA payload can include one, some or all of the pairing information for C2 communication, an indication of the request for direct C2 communication, pairing information for direct C2 communication, and the UAV flight authorization information (see subclauses 6.4.1.2 and 6.4.2.2).

The UE supporting UAS services can establish a PDU session for the C2 communication by providing the CAA-level UAV ID and the C2 authorization payload. The SMF upon reception of the UE's request for the PDU session establishment, determines that authorization is required based on the DNN and S-NSSAI combination of the PDU session is for aerial services according to user's subscription data and the CAA-level UAV ID included in the request.

If a UE supporting UAS services uses a common PDU session for both USS communication and C2 communication, the C2 communication can be authorized using UUAA-SM procedure during the PDU session establishment procedure or during the PDU session modification procedure. If the pairing of UAV and UAV-C is revoked, the network shall disable C2 communication for the PDU session. The SMF upon reception of the UE's request for the PDU session establishment, determines that authorization is required based on the DNN and S-NSSAI combination of the PDU session is for aerial services according to user's subscription data and the CAA-level UAV ID included in the request.

NOTE 2: The network can disable C2 communication for the PDU session e.g., by removing the QoS flow for C2 communication during PDU session modification procedure as decribed in subclauses 6.3.2.2.

If a UE supporting UAS services uses separate PDU sessions for, respectively, USS communication and C2 communication, the C2 communication is authorized using UUAA-SM during the PDU session establishment procedure. If the pairing of UAV and UAV-C is revoked, the PDU session for C2 communication shall be released by the SMF.

During the registration procedure for UAS services, direct C2 communication can be authorized as described in subclause 5.5.1.2. A UE supporting A2X over NR-PC5 can perform registration procedure for UAS services including a request for authorization of direct C2 communication by providing CAA-level UAV ID and C2 authorization payload.

4.22.4 Void

4.23 NAS over Non-Terrestrial Network

4.23.1 General

A 5GS can support 3GPP satellite NG-RAN access technology (see 3GPP TS 23.501 [8]). This subclause describes NAS-specific aspects of the 5GS features to support 3GPP satellite NG-RAN access technology.

4.23.2 List of "PLMNs not allowed to operate at the present UE location"

For 3GPP satellite NG-RAN the UE shall store a list of "PLMNs not allowed to operate at the present UE location". Each entry consists of:

a) the PLMN identity of the PLMN which sent a message including 5GMM cause value #78 "PLMN not allowed to operate at the present UE location" via satellite NG-RAN access technology; and

b) the geographical location, if known by the UE, where 5GMM cause value #78 was received on satellite NG-RAN access technology; and

c) if the geographical location exists, a UE implementation specific distance value.

Before storing a new entry in the list, the UE shall delete any existing entry with the same PLMN identity. Upon storing a new entry, the UE starts a timer instance associated with the entry with an implementation specific value that shall not be set to a value smaller than the timer value indicated by the network in the Lower bound timer value IE, if any. If the Lower bound timer value IE was not provided by the network, the value of the timer shall be set based on the UE implementation.

The UE is allowed to attempt to access a PLMN via satellite NG-RAN access technology which is part of the list of "PLMNs not allowed to operate at the present UE location" only if:

a) the current UE location is known, a geographical location is stored for the entry of this PLMN, and the distance to the current UE location is larger than a UE implementation specific value; or

b) the access is for emergency services (see 3GPP TS 23.122 [5] for further details).

NOTE 1: When the UE is accessing network for emergency services, it is up to operator and regulatory policies whether the network needs to determine if the UE is in a location where network is not allowed to operate.

NOTE 2: While location determination is ongoing to ensure that operator and regulatory policies are met, the AMF can perform DNN-based or S-NSSAI based congestion control as specified in subclauses 5.3.10 and 5.3.11 to prevent the UE from accessing network.

The list shall accommodate three or more entries. The maximum number of entries is an implementation decision. When the list is full and a new entry has to be inserted, the oldest entry shall be deleted.

Each entry shall be removed if for the entry:

a) the UE successfully registers via satellite NG-RAN access technology to the PLMN stored in the entry except when the UE registers for emergency services; or

b) the timer instance associated with the entry expires.

The UE may delete the entry in the list, if the current UE location is known, a geographical location is stored for the entry of this PLMN, and the distance to the current UE location is larger than a UE implementation specific value.

If the UE is in 5GMM-DEREGISTERED.LIMITED-SERVICE state and an entry from the list of "PLMNs not allowed to operate at the present UE location" is removed, the UE shall perform PLMN selection according to 3GPP TS 23.122 [5].

When the UE is switched off, the UE shall keep the list of "PLMNs not allowed to operate at the present UE location" in its non-volatile memory. The UE shall delete the list of "PLMNs not allowed to operate at the present UE location" if the USIM is removed.

If the UE is switched off when the timer instance associated with the entry in the list is running, the UE shall behave as follows when the UE is switched on and the USIM in the UE remains the same:

let t1 be the time remaining for timer instance associated with the entry in the list to timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted and considered expired. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

4.23.3 5GS mobility management via a satellite NG-RAN cell

For 5GS mobility management via a satellite NG-RAN cell the UE shall apply the value of the applicable NAS timer indicated in table 10.2.1 for access via a satellite NG-RAN cell.

NOTE 1: The applied NAS timer values are based on the current satellite NG-RAN access RAT type determined based on information from lower layers.

The NAS timer value obtained by the UE is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure, and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

The access via a satellite NG-RAN cell by a UE is indicated to the AMF by lower layers and shall be stored by the AMF. When an AMF that supports access via satellite NG-RAN cells performs NAS signalling with a UE via satellite

NG-RAN cells, the AMF shall calculate the value of the applicable NAS timer indicated in table 10.2.2 for access via a satellite NG-RAN cell.

NOTE 2: The applied NAS timer values are based on the current satellite NG-RAN access RAT type determined based on information from lower layers.

The NAS timer value obtained by the network is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

4.23.4 5GS session management via a satellite NG-RAN cell

For 5GS session management via a satellite NG-RAN cell the UE shall apply the value of the applicable NAS timer indicated in table 10.3.1 for access via a satellite NG-RAN cell.

NOTE 1: The applied NAS timer values are based on the current satellite NG-RAN access RAT type determined based on information from lower layers.

The NAS timer value obtained by the UE is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure, and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

If the use of extended NAS timer for access via a satellite NG-RAN cell is indicated by the AMF (see 3GPP TS 23.501 [8] and 3GPP TS 23.502 [9]), the SMF shall calculate the value of the applicable NAS timer indicated in table 10.3.2 for access via a satellite NG-RAN cell.

The NAS timer value obtained by the network is used as described in the appropriate procedure subclause of this specification. The NAS timer value shall be calculated at start of a NAS procedure and shall not be re-calculated until the NAS procedure is completed, restarted or aborted.

4.23.5 Handling multiple tracking area codes from the lower layers

When a UE camps on a satellite NG-RAN cell, the UE may receive multiple TACs from the lower layers. The UE shall construct TAIs from the multiple TACs (i.e. concatenate the identity of the current PLMN and each of the TACs) and select a TAI as follows:

a) if at least one TAI belongs to the current registration area of the UE, the UE shall select a TAI which belongs to the current registration area of the UE according to the followings.

   If there are multiple TAIs which belong to the current registration area of the UE, the UE shall select a TAI as follows:

   1) if there is a TAI which belongs to the list of "allowed tracking area" (if any) and does not belong to the list of "non-allowed tracking areas" (if any), the UE shall select a TAI which belongs to the list of "allowed tracking area" (if any) and does not belong to the list of "non-allowed tracking areas" (if any). In this case, if there are multiple TAIs which belong to the list of "allowed tracking area" (if any) and does not belong to the list of "non-allowed tracking areas" (if any), then the UE shall consider each of these TAIs equal and select a TAI in an implementation-specific way (e.g. taking into account LADN service area information). If these multiple TAIs contain the previous current TAI, the current TAI can be left unchanged.

   2) if there is no TAI which belongs to the list of "allowed tracking area" (if any) and does not belong to the list of "non-allowed tracking areas" (if any) or neither the list of "allowed tracking area" nor the list of "non-allowed tracking areas" is available, then the UE shall consider each of these TAIs equal and select a TAI in an implementation-specific way (e.g. taking into account LADN service area information). If these multiple TAIs contain the previous current TAI, the current TAI can be left unchanged.

b) if the current registration area is not available in the UE or no TAI belongs to the current registration area of the UE and:

   1) there is a TAI which belongs to neither the list of "5GS forbidden tracking areas for roaming" nor the list of "5GS forbidden tracking areas for regional provision of service", the UE shall select a TAI which belongs to neither the list of "5GS forbidden tracking areas for roaming" nor the list of "5GS forbidden tracking areas for regional provision of service". In this case, if there are multiple TAIs which belong to neither the list of

"5GS forbidden tracking areas for roaming" nor the list of "5GS forbidden tracking areas for regional provision of service", then the UE shall consider each of these TAIs equal and select a TAI in an implementation-specific way.

2) all TAIs belong to the list of "5GS forbidden tracking areas for roaming" or the list of "5GS forbidden tracking areas for regional provision of service", then the UE shall consider each of these TAIs equal and select a TAI in an implementation-specific way.

The UE shall consider the selected TAI as the current TAI. The UE shall select a TAI when:

a) the UE receives multiple TACs from the lower layers; or

b) the UE has received multiple TACs from the lower layers upon starting to camping on the current cell and the registration area, the list of "allowed tracking areas", the list of "non-allowed tracking areas", the list of "5GS forbidden tracking areas for roaming", or the list of "5GS forbidden tracking areas for regional provision of service" is updated.

Handling of the list of "5GS forbidden tracking areas for roaming" and the list of "5GS forbidden tracking areas for regional provision of service" is specified in subclause 5.3.13.

4.24 Minimization of service interruption

The UE and the network may support Minimization of service interruption (MINT). MINT aims to enable a UE to obtain service from a PLMN offering disaster roaming services when a disaster condition applies to the UE determined PLMN with disaster condition.

If the UE supports MINT, the indication of whether disaster roaming is enabled in the UE, the indication of 'applicability of "lists of PLMN(s) to be used in disaster condition" provided by a VPLMN', the one or more "list of PLMN(s) to be used in disaster condition", disaster roaming wait range and disaster return wait range provisioned by the network, if available, are stored in the non-volatile memory in the ME as specified in annex C and are kept when the UE enters 5GMM-DEREGISTERED state. Annex C specifies condition under which the indication of whether disaster roaming is enabled in the UE, the indication of 'applicability of "lists of PLMN(s) to be used in disaster condition" provided by a VPLMN', the one or more "lists of PLMN(s) to be used in disaster condition", disaster roaming wait range and disaster return wait range stored in the ME are deleted.

Upon selecting a PLMN for disaster roaming as specified in 3GPP TS 23.122 [5]:

a) if the UE does not have a stored disaster roaming wait range, the UE shall perform a registration procedure for disaster roaming services on the selected PLMN as described in subclause 5.5.1; and

b) if the UE has a stored disaster roaming wait range, the UE shall generate a random number within the disaster roaming wait range and start a timer with the generated random number. While the timer is running, the UE shall not initiate registration on the selected PLMN except if the UE needs to request an emergency PDU session, in which case the UE shall initiate the registration procedure, set the 5GS registration type IE to "emergency registration" in the REGISTRATION REQUEST message and keep the timer running. Upon expiration of the timer, if the UE does not have an emergency PDU session, the UE shall perform a registration procedure for disaster roaming services as described in subclause 5.5.1 if still camped on the selected PLMN. If the UE has an emergency PDU session when the timer expires, the registration procedure for disaster roaming services as described in subclause 5.5.1 shall be performed after the release of the emergency PDU session, if the UE is still camped on the selected PLMN.

If the UE is switched off when the timer for disaster roaming wait range is running, the UE shall behave as follows when the UE is switched on, the USIM in the UE remains the same and the UE selects the PLMN for disaster roaming:

- let t1 be the time remaining for the timer for disaster roaming wait range timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

Upon determining that a disaster condition has ended as specified in 3GPP TS 23.122 [6]:

a) the UE shall stop the timer started with a generated random number within the disaster roaming wait range, if running;

b) the UE shall perform PLMN selection as specified in 3GPP TS 23.122 [5], except if the UE already selected an allowable PLMN as specified in 3GPP TS 23.122 [6]; and

c) if the UE selects the UE determined PLMN with disaster condition and has a stored disaster return wait range, which is

   1) provided by the PLMN providing disaster roaming services; or

   2) provided by the selected PLMN,

   the UE shall generate a random number within the disaster return wait range, start a timer with the generated random number value and enter 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION state or 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE state, if registered. While the timer is running, the UE shall not initiate registration on the selected PLMN except if the UE needs to request an emergency PDU session, in which case the UE shall initiate the registration procedure, set the 5GS registration type IE to "emergency registration" in the REGISTRATION REQUEST message and keep the timer running. Upon expiration of the timer, if the UE does not have an emergency PDU session, the UE shall perform a registration procedure if still camped on the selected PLMN. If the UE has an emergency PDU session when the timer expires, the registration procedure as described in subclause 5.5.1 shall be performed after the release of the emergency PDU session, if the UE is still camped on the selected PLMN.

   Otherwise, the UE shall perform registration procedure in the selected PLMN.

If the UE is switched off when the timer for disaster return wait range is running, the UE shall behave as follows when the UE is switched on, the USIM in the UE remains the same and the UE selects the UE determined PLMN with disaster condition:

- let t1 be the time remaining for the timer for disaster return wait range timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

When the AMF assigns a registration area to the UE registered for disaster roaming services, the AMF shall only include TAIs covering the area with the disaster condition.

When the AMF determines that the disaster condition has ended and the UE which is registered for disaster roaming services has an emergency PDU session, the AMF shall initiate the generic UE configuration update procedure to indicate that the UE is registered for emergency services as described in subclause 5.4.4.2.

Interworking with EPS is not supported for UEs that are registered for disaster roaming services. When registering for disaster roaming services, the UE indicates to the network that S1 mode is not supported as described in subclause 5.5.1.2.2. While registered for disaster roaming services and upon a need to establish an emergency PDU session or perform emergency services fallback, the UE initiates the registration procedure for mobility and periodic registration update and indicates that S1 mode is supported as described in subclause 5.5.1.3.2.

If the UE is registered for disaster roaming services and the registered PLMN is removed from forbidden PLMN lists due to reasons specified in 3GPP TS 23.122 [5] subclause 4.4.6 or in 3GPP TS 23.122 [5] Annex C, then UE shall initiate the de-registration procedure and perform PLMN selection as specified in 3GPP TS 23.122 [5].

4.25 Support of MUSIM features

A network and a MUSIM UE may support one or more of the MUSIM features (i.e. the N1 NAS signalling connection release, the paging indication for voice services, the reject paging request, the paging restriction and the paging timing collision control).

If MUSIM UE supports one or more MUSIM features, the UE indicates support of one or more MUSIM features (except for the paging timing collision control) during the registration procedure. If the UE has indicated support of the N1 NAS signalling connection release or the reject paging request or both and the UE supports the paging restriction, the UE indicates support of the paging restriction.

If the UE indicates support of one or more MUSIM features and the network decides to accept one or more MUSIM features, the network indicates the support of one or more MUSIM features during the registration procedure. The network only indicates the support of the paging restriction together with the support of either N1 NAS signalling connection release or the reject paging request.

The network does not indicate support for any MUSIM feature to the UE during the registration for emergency services.

If the UE is not currently registered for emergency service and the UE receives the CONFIGURATION UPDATE COMMAND message with the 5GS registration result IE value set to "Registered for emergency services", then UE shall behave as if the network did not indicate support for any MUSIM feature in the last registration procedure. If the network has sent CONFIGURATION UPDATE COMMAND message with the 5GS registration result IE value set to "Registered for emergency services", then network shall behave as if it did not indicate support for any MUSIM feature in the last registration procedure.

If a UE stops fulfilling the condition to be considered a MUSIM UE as defined in subclause 3.1, and the UE has negotiated support of one or more MUSIM features, then the UE shall initiate a registration procedure for mobility and periodic registration update to indicate that all the MUSIM features are not supported (except for the paging timing collision control) as specified in subclause 5.5.1.3.

A MUSIM UE operating in NB-N1 mode or in WB-N1 mode CE mode B does not indicate the support for paging indication for voice services during the registration procedure towards the network.

4.26 Support for Personal IoT Network service

The 5GS can support the personal IoT network (PIN) service (see 3GPP TS 23.501 [8]).

The PIN enables the personal IoT network elements (PINEs) to communicate with each other via PIN direct communication, PIN indirect communication or PIN-DN communication. For the PIN indirect communication and PIN-DN communication, a UE acting as a PIN element with gateway capability (PEGC) enables the PINEs behind the PEGC to connect to the network and to communicate with other PINEs within the PIN or with the DN via the PDU session established for PIN. A PEGC may serve one or more PINs. The PEGC establishes only one PDU session for each PIN. The PEGC establishes different PDU sessions for different PINs based on different DNNs and S-NSSAIs. The PEGC may establish only one PDU session for multiple PINs if traffic differentiation for multiple PINs is not required in 5GS.

NOTE 1: The PIN direct communication is out of the scope of 3GPP.

The PIN, PEGC, and PINEs are managed by PIN element with management capability (PEMC) and optionally the corresponding application function. Each PIN contains at least one PEGC and at least one PEMC. The PIN architecture is captured in 3GPP TS 23.501 [8].

The 5GS supports the delivery of URSP rules which include the PIN ID to a PEGC registered to 5GS (see 3GPP TS 23.501 [8] and 3GPP TS 23.503 [10]). The 5GS is enhanced to support the PDU session management for PIN to ensure the end-to-end QoS requirement.

The end-to-end QoS requirement for each PINE over PIN indirect communication and over PIN-DN communication includes:

a) the QoS requirement in the 3GPP access network; and

b) the QoS requirement in the non-3GPP access network.

The N3QAI is introduced to enable a PEGC to perform the QoS differentiation for the PINEs in the non-3GPP access network. If the UE supports receiving the N3QAI, the network may provide the N3QAI associated with the QoS flow during the PDU session establishment procedure as defined in subclause 6.4.1 or during the PDU session modification procedure as defined in subclause 6.4.2.

NOTE 2: How the PEGC applies N3QAI is outside the scope of the present document.

The non-3GPP delay budget refers to the delay budget between the PEGC and the PINE in the non-3GPP access network. If the UE supports providing the non-3GPP delay budget, the UE may provide the network with the non-3GPP delay budget for the one or more QoS flows associated with the PDU sessions for a PIN during the PDU session modification procedure as defined in subclause 6.4.2. The network takes into account the received non-3GPP delay budget to ensure the end-to-end QoS requirement of a PINE.

NOTE 3: The support of a 5G-RG or a FN-RG acting as a PEGC is not specified in this release of specification.

NOTE 4: The support of redundant PDU sessions does not apply for PIN.