**3GPP TSG-SA3 Meeting #121 S3-251741**

Goteborg, Sweden, 7 – 11 April 2025

|  |
| --- |
| *CR-Form-v12.1* |
| **Draft CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **draft-CR** | **rev** | **-** | **Current version:** | **19.2.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Living CR for security for PLMN hosting a NPN  |
|  |  |
| ***Source to WG:*** | China Telecom, ZTE |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | PLMNNPN |  | ***Date:*** | 2025-02-17 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | The feature of security for PLMN hosting a NPN needs to be added. |
|  |  |
| ***Summary of change:*** | Living CR for how the work on the security for PLMN hosting a NPN study can be implemented in TS 33.501. This draft CR is intended to compile a list of recommendations, based on the conclusions in TR 33.757, on how to secure the border between PLMN and hosted NPN when dedicated NFs interacting with PLMN through SBA interface. |
|  |  |
| ***Consequences if not approved:*** | The work item is incomplete. |
|  |  |
| ***Clauses affected:*** | 3.1, 3.2, I.1, Annex xx(new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** | SA3#120: S3-251168SA3#121: S3-251741 was implementation of S3-251359, S3-251738, S3-251739 and S3-251740. |

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

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**5G security context:** The state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network.

NOTE 1: The "5G security context data" consists of the 5G NAS security context, and the 5G AS security context for 3GPP access and/or the 5G AS security context for non-3GPP access.

NOTE 2: A 5G security context has type "mapped", "full native" or "partial native". Its state can either be "current" or "non-current". A context can be of one type only and be in one state at a time. The state of a particular context type can change over time. A partial native context can be transformed into a full native. No other type transformations are possible.

**5G AS security context for 3GPP access:** The cryptographic keys at AS level with their identifiers, the Next Hop parameter (NH), the Next Hop Chaining Counter parameter (NCC) used for next hop access key derivation, the identifiers of the selected AS level cryptographic algorithms, the UE security capabilities, and the UP Security Policy at the network side, UP security activation status and the counters used for replay protection.

NOTE 3: NH and NCC need to be stored also at the AMF during connected mode.

NOTE 4: UP security activation status is sent from gNB/ng-eNB in step 1b in clause 6.6.2 corresponding to the active PDU session(s).

**5G AS security context for non-3GPP access:** The key KN3IWF, the cryptographic keys, cryptographic algorithms and tunnel security association parameters used at IPsec layer for the protection of IPsec SA.

**5G AS Secondary Cell security context**: The cryptographic keys at AS level for secondary cell with their identifiers, the identifier of the selected AS level cryptographic algorithms for secondary cell, the UP Security Policy at the network side, and counters used for replay protection.

**5G** **Home Environment Authentication Vector:** authentication data consisting of RAND, AUTN, XRES\*, and KAUSF for the purpose of authenticating the UE using 5G AKA.

NOTE 3a: This vector is received by the AUSF from the UDM/ARPF in the Nudm\_UEAuthentication\_Get Response.

**5G Authentication Vector:** authentication data consisting of RAND, AUTN, HXRES\*, and KSEAF.

NOTE 3b: This vector is received by the SEAF from the AUSF in the Nausf\_Authentication\_Authenticate Response.

**5G NAS security context:** The key KAMF with the associated key set identifier, the UE security capabilities, the uplink and downlink NAS COUNT values.

NOTE 4: The distinction between native 5G security context and mapped 5G security context also applies to 5G NAS security contexts. The 5G NAS security context is called "full" if it additionally contains the integrity and encryption keys and the associated identifiers of the selected NAS integrity and encryption algorithms.

**5G Serving Environment Authentication Vector:** a vector consisting of RAND, AUTN and HXRES\*.

**ABBA parameter:** Parameter that provides antibidding down protection of security features against security features introduced in higher release to a lower release and indicates the security features that are enabled in the current network.

**activation of security context:** The process of taking a security context into use.

**anchor key:** The security key KSEAF provided during authentication and used for derivation of subsequent security keys.

**application Layer Security:** mechanism by which HTTP messages, exchanged between a Network Function in one PLMN and a Network Function in another PLMN, are protected on the N32-f interface between the two SEPPs in the two PLMNs.

**authentication data:** An authentication vectoror transformed authentication vector.

**authentication vector:** A vector consisting of CK, IK, RAND, AUTN, and XRES.

**backward security**: The property that for an entity with knowledge of Kn, it is computationally infeasible to compute any previous Kn-m (m>0) from which Kn is derived.

NOTE 5: In the context of KgNB key derivation, backward security refers to the property that, for a gNB with knowledge of a KgNB, shared with a UE, it is computationally infeasible to compute any previous KgNB that has been used between the same UE and a previous gNB.

**CM-CONNECTED state:** This is as defined in TS 23.501 [2].

NOTE5a: The term CM-CONNECTED state corresponds to the term 5GMM-CONNECTED mode used in TS 24.501 [35].

**CM-IDLE state:** As defined in TS 23.501 [2].

NOTE5b: The term CM-IDLE state corresponds to the term 5GMM-IDLE mode used in TS 24.501 [35].

**consumer's RI (cRI): RI** with a business relationship with the cSEPP operator.

**consumer's NRF (cNRF):** The NRF that authenticates the service consumer NF and resides in the PLMN where the service consumer NF is located.

**consumer's PLMN (cPLMN):** The PLMN where the service consumer NF is located**.**

**consumer's SEPP (cSEPP):** The SEPP residing in the PLMN where the service consumer NF is located.

**Credentials Holder:** As defined in TS 23.501 [2].

**current 5G security context:** The security context which has been activated most recently.

NOTE5c: A current 5G security context originating from either a mapped or native 5G security context can exist simultaneously with a native non-current 5G security context.

**Default Credentials Server:** As defined in TS 23.501[2].

**Default UE credentials:** As defined in TS 23.501[2].

**forward security**: The fulfilment of the property that for an entity with knowledge of Km that is used between that entity and a second entity, it is computationally infeasible to predict any future Km+n (n>0) used between a third entity and the second entity.

NOTE 6: In the context of KgNB key derivation, forward security refers to the property that, for a gNB with knowledge of a KgNB, shared with a UE, it is computationally infeasible to predict any future KgNB that will be used between the same UE and another gNB. More specifically, n hop forward security refers to the property that a gNB is unable to compute keys that will be used between a UE and another gNB to which the UE is connected after n or more handovers (n=1 or more).

**full native 5G security context:** A native 5G security context for which the 5G NAS security context is full according to the above definition.

NOTE6a: A full native 5G security context is either in state "current" or state "non-current".

**Home Network Identifier:** An identifier identifying the home network of the subscriber.

NOTE6b: Described in detail in TS 23.003 [19].

**Home Network Public Key Identifier:** An identifier used to indicate which public/private key pair is used for SUPI protection and de-concealment of the SUCI.

NOTE6c: Described in this document and detailed in TS 23.003 [19].

**IAB-donor-CU**: As defined in TS 38.401 [78] .

**IAB-donor-DU**: As defined in TS 38.401 [78].

**IAB-node**: As defined in TS 38.300 [52].

**IAB-donor gNB**:As defined in TS 38.300 [52].

**IAB-UE**: The function within an IAB node, which behaves as a UE.

**IPX provider**: Roaming Intermediary.

NOTE 6ca: For historical reasons this term in the present document is equivalent to Roaming Intermediary.

**mapped 5G security context**: An 5G security context, whose KAMF was derived from EPS keys during interworking and which is identified by mapped ngKSI.

**Master node**: As defined in TS 37.340 [51].

**N32-c connection:** A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN.

NOTE 6d: This is a short-lived connection that is used between the SEPPs for negotiation of the N32-f protection mechanism, cipher suite and protection policy exchange, and error notifications. Every N32-f connection requires an N32-c connection that was established before establishing N32-f.

**N32-f connection:** Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN for exchange of protected HTTP messages.

NOTE 6e: When Roaming Intermediaries are present in the path between the two SEPPs, an N32-f HTTP connection is setup on each hop towards the other SEPP.

**native 5G security context:** An 5G security context, whose KAMF was created by a run of primary authentication and which is identified by native ngKSI.

**ng-eNB**: As defined in TS 38.300 [52].

**NG-RAN node**: gNB or ng-eNB (as defined in TS 38.300 [52]).

**non-current 5G security context:** A native 5G security context that is not the current one.

NOTE 7: A non-current 5G security context may be stored along with a current 5G security context in the UE and the AMF. A non-current 5G security context does not contain 5G AS security context. A non-current 5G security context is either of type "full native" or of type "partial native".

**Operator Group Roaming Hub:** Roaming hub used by a group of network operators that reside in the same security domain to consolidate and secure operator group roaming.

**partial native 5G security context:** A partial native 5G security context consists of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values, which are initially set to zero before the first NAS SMC procedure for this security context.

NOTE 8: A partial native 5G security context is created by primary authentication, for which no corresponding successful NAS SMC has been run. A partial native context is always in state "non-current".

**PLMN Operational domain:** Network entities of NPN that can be deployed in PLMN operator premises are under the control of the PLMN operator.

**PNI-NPN Operational domain:** Dedicated network entities of a NPN that are outside of the PLMN operator's security domain and are deployed with the support of a PLMN operator as defined in TS 22.261 [7].

**producer's RI (pRI)**: RI with a business relationship with the pSEPP operator.

**producer's NRF (pNRF):** The NRF where the service producer NF is registered in the PLMN where the service producer NF is located.

**producer's PLMN (pPLMN):** The PLMN where the service producer NF is located.

**producer's SEPP (pSEPP):** The SEPP residing in the PLMN where the service producer NF is located.

**Protection Scheme Identifier:** An identifier identifying a protection scheme that is used for concealing the SUPI.

**RM-DEREGISTERED state:** This is as defined in TS 23.501 [2].

NOTE8a: The term RM-DEREGISTERED state corresponds to the term 5GMM-DEREGISTERED mode used in TS 24.501 [35].

**RM-REGISTERED state:** As defined in TS 23.501 [2].

NOTE8b: The term RM-REGISTERED state corresponds to the term 5GMM-REGISTERED mode used in TS 24.501 [35].

**Roaming Hub:** A type ofRoaming Intermediary that provides a set of services to client PLMNs to facilitate the deployment and the operation of roaming and interworking services; as defined by GSMA.

**Roaming Intermediary**: an entity that provides roaming related services.

**Routing Indicator:** An indicator defined in TS 23.003 [19] that can be used for AUSF or UDM selection.

**Scheme Output**: the output of a public key protection scheme used for SUPI protection.

**security anchor function:** The function SEAF that serves in the serving network as the anchor for security in 5G.

**Secondary node**: As defined in TS 37.340 [51].

**STM Data Consumer**: This term is defined in TS 28.560 [121].

**STM Data Producer**: This term is defined in TS 28.560 [121].

**STM Management Consumer**: This term is defined in TS 28.560 [121].

**STM Management Producer**: This term is defined in TS 28.560 [121].

NOTE: The STM Management/Data Producers and the STM Management/Data Consumers are left for implementation, with the consideration of being the end-point of the Signalling monitoring interfaces for which security requirements are specified in 5.9.4.

**subscription credential(s):** The set of values in the USIM and in the home operator's network, consisting of at least the long-term key(s) and the subscription identifier SUPI, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.

**subscription identifier:** The SUbscription Permanent Identifier (SUPI).

NOTE8c: As defined in TS 23.501 [2] and detailed in 23.003 [19].

**subscription concealed identifier:** A one-time use subscription identifier, called the SUbscription Concealed Identifier (SUCI), which contains the Scheme-Output, and additional non-concealed information needed for home network routing and protection scheme usage.

NOTE8d: Defined in the present document; detailed in TS 23.003 [19].

**subscription identifier de-concealing function:** The Subscription Identifier De-concealing Function (SIDF) service offered by the network function UDM in the home network of the subscriber responsible for de-concealing the SUPI from the SUCI.

**transformed authentication vector:** an authentication vector where CK and IK have been replaced with CK' and IK'.

**UE 5G security capability:** The UE security capabilities for 5G AS and 5G NAS.

**UE security capabilities:** The set of identifiers corresponding to the ciphering and integrity algorithms implemented in the UE.

NOTE 9: This includes capabilities for NG-RAN and 5G NAS, and includes capabilities for EPS, UTRAN and GERAN if these access types are supported by the UE.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC 5G Core Network

5G-AN 5G Access Network

5G-RG 5G Residential Gateway

NG-RAN 5G Radio Access Network

5G AV 5G Authentication Vector

5G HE AV 5G Home Environment Authentication Vector

5G NSWO 5G Non-Seamless WLAN Offload

5G SE AV 5G Serving Environment Authentication Vector

ABBAAnti-Bidding down Between Architectures

AEAD Authenticated Encryption with Associated Data

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

AMF Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF Authentication credential Repository and Processing Function

AUN3 Authenticable Non-3GPP devices

AUSF Authentication Server Function

AUTN AUthentication TokeN

AV Authentication Vector

AV' transformed Authentication Vector

BAP Backhaul Adaptation Protocol

BH Backhaul

CCA Client Credentials Assertion

Cell-ID Cell Identity as used in TS 38.331 [22]

CH Credentials Holder

CHO Conditional Handover

CIoT Cellular Internet of Things

cIPX consumer's IPX

CKSRVCC Cipher Key for Single Radio Voice Continuity

cNRF consumer's NRF

CP Control Plane

CPAC Conditional PSCell Addition or Change

CPA Conditional PSCell Addition

CPC Conditional PSCell Change

cPLMN consumer's PLMN

cRI consumer's RI

cSEPP consumer's SEPP

CTR Counter (mode)

CU Central Unit

DCS Default Credentials Server

DN Data Network

DNN Data Network Name

DU Distributed Unit

EAP Extensible Authentication Protocol

EDT Early Data Transmission

EMSK Extended Master Session Key

EN-DC E-UTRA-NR Dual Connectivity

ENSI External Network Slice Information

EPS Evolved Packet System

FN-RG Fixed Network RG

gNB NR Node B

GUTI Globally Unique Temporary UE Identity

HRES Hash RESponse

HXRES Hash eXpected RESponse

IAB Integrated Access and Backhaul

IKE Internet Key Exchange

IKSRVCC Integrity Key for Single Radio Voice Continuity

IPUPS Inter-PLMN UP Security

IPX IP exchange service

KSI Key Set Identifier

KSISRVCC Key Set Identifier for Single Radio Voice Continuity

LI Lawful Intercept

MBSF Multicast/Broadcast Service Function

MBSSF Multicast/Broadcast Service Security Function

MBSTF Multicast/Broadcast Service Transport Function

MeNB Master eNB

MN Master Node

MO-EDT Mobile Originated Early Data Transmission

MT-EDT Mobile Terminated Early Data Transmission

MR-DC Multi-Radio Dual Connectivity

MSK Master Session Key

N3IWF Non-3GPP access InterWorking Function

NAI Network Access Identifier

NAS Non Access Stratum

NDS Network Domain Security

NEA Encryption Algorithm for 5G

NF Network Function

NG Next Generation

ng-eNB Next Generation Evolved Node-B

ngKSI Key Set Identifier in 5G

N5CW Non-5G-Capable over WLAN

N5GC Non-5G-Capable

NIA Integrity Algorithm for 5G

NPN Non-Public Network

NR New Radio

NR-DC NR-NR Dual Connectivity

NSSAI Network Slice Selection Assistance Information

NSSAA Network Slice Specific Authentication and Authorization

NSWO Non-Seamless WLAN Offload

NSWOF Non-Seamless WLAN Offload Function

PDN Packet Data Network

PEI Permanent Equipment Identifier

pIPX producer's IPX

pNRF producer's NRF

PNI-NPN Public Network Integrated NPN

pPLMN producer's PLMN

pRI producer's RI

PRINS PRotocol for N32 INterconnect Security

pSEPP producer's SEPP

PUR Preconfigured Uplink Resource

QoS Quality of Service

RES RESponse

RI Roaming Intermediary

RH Roaming Hub

SCG Secondary Cell Group

SEAF SEcurity Anchor Function

SCP Service Communication Proxy

SEPP Security Edge Protection Proxy

SCPAC Subsequent Conditional PSCell Addition or Change

SgNB Secondary gNB

SIDF Subscription Identifier De-concealing Function

SMC Security Mode Command

SMF Session Management Function

SN Secondary Node

SN Id Serving Network Identifier

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TLS Transport Layer Security

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TWAP Trusted WLAN Access Point

TWIF Trusted WLAN Interworking Function

TSC Time Sensitive Communication

UE User Equipment

UEA UMTS Encryption Algorithm

UDM Unified Data Management

UDR Unified Data Repository

UIA UMTS Integrity Algorithm

ULR Update Location Request

UP User Plane

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

USIM Universal Subscriber Identity Module

XRES eXpected RESponse

\* \* \* End of Change 1 \* \* \* \*

\* \* \* Second Change \* \* \* \*

# I.1 General

This Annex provides details on security for non-public networks. Most of the security procedures are the same as public networks so this annex only summarizes and specifies where there are exceptions to the normal procedures.

The feature for support of non-public networks (NPN) by 5GS is described in clause 5.30 of 23.501 [2].

NOTE X: The architecture of a PLMN hosting a NPN with dedicated NFs in the PNI-NPN operational domain is described in Annex XX.

\* \* \* End of Change 2 \* \* \* \*

\* \* \* Third Change \* \* \* \*

Annex XX (Informative): Security for PLMN hosting a NPN through SBA interface

# XX.1 General

This annex specifies the security aspects of PLMN hosting an NPN with dedicated NFs deployed in the PNI\_NPN operational domain. The annex describes how to secure the boundary between PLMN operational domain and PNI\_NPN operational domain when dedicated NFs interacting with PLMN operational domain through SBA interface and vice versa.

This annex is based on the following assumptions:

- Mutual trust between PLMN operational domain and the dedicated Network functions at the PNI\_NPN operational domain is not in place.

- Attacks may happen from PNI\_NPN operational domain to PLMN operational domain and PLMN operational domain to PNI\_NPN operational domain.

# XX.2 Architecture



Figure XX.2-1 Example of dedicated NFs deployed in the PNI-NPN operational domain

As depicted in Figure XX.2-1, dedicated UPF and part of CP functions are deployed in the PNI-NPN operational domain. The interface between the dedicated NFs in the PNI-NPN operational domain and the NFs in the PLMN operational domain is SBA interface.

NOTE: The choice of which of these CP functions (i.e., AMF or SMF, or both or none) are deployed in the PNI-NPN operational domain is a matter for deployment. Whether additional CP functions are deployed in the PNI-NPN operational domain and its associated additional security controls are not considered in the present document.

When the AMF is deployed in the PNI-NPN operational domain, there exists a privacy risk regarding SUPI exposure outside the PLMN operational domain. Appropriate measures to mitigate this risk may be considered when choosing this architecture for deployment.

# XX.3 Proxy entity at the border

It is recommended to deploy one or more proxy entities at the border between PLMN and PNI-NPN operational domains. The security capabilities of these proxy entities are listed below.

1. Transport layer protection solution (as defined in clause 13.3) is supported for mutual authentication between the proxy entities and between each proxy entity and the NFs they serve.
2. SBA authorization framework (as defined in clause 13.4) is reused for authorization between NFs in the PLMN and PNI-NPN operational domains.
3. Topology hiding to IP level (e.g., IP address or FQDN) and application level (e.g., target NFs in the discovery response, Callback URI in the payload of the messages) is supported.
4. Message inspection and filtering, malformed message handling are supported.

NOTE: Specific method for above security capabilities c) and d) is left to implementation.

Besides the security capabilities listed above, the part of the routing functionalities listed below also needs to be supported:

1. Indirect Communication (see TS 23.501[2] clause 7.1.1 for details).
2. Delegated Discovery (see TS 23.501[2] clauses 7.1.1 and 6.3.1 for details).
3. Message forwarding and routing to destination NF/NF service.
4. Message forwarding and routing to a next hop. (Required for bi-directional protection)

# XX.4 Policy Check

To control the information exchange between the PNI-NPN operational domain and the PLMN operational domain, policy checks can be performed by the proxy entity at the border that segregates the trust domain between these operational domains.

Policy check can be defined based on available controls from the present specification considering architectural requirements. Examples of such policy checks are:

1. Having transport layer protection based on clause 13.1 of the present document.
2. Having authorization based on clause 13.4 of the present document.

The selection and definition of the policies from the examples above or from the present specification is left to the choice of implementation considering the architectural needs.

# XX.5 Security for DNS messages crossing the border

DNS messages crossing the trust boundary can be protected. Security configuration and profiling of DNS servers is left to implementation. The dedicated NFs in the PNI-NPN operational domain are provisioned with the DNS security configuration, for example using one of the following methods:

- Pre-configuring the DNS security configuration in the dedicated NF.

- Updating the DNS security configuration in the dedicated NF during NF instantiation via the OAM.

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