**3GPP TSG-SA Meeting #101 *SP-231175***

**, , - was SP-231076**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1789** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  |
| *For* [***HELP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Modification of PRINS to enable Roaming Hubs |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | Vodafone, DoCoMo, Verizon, Deutsche Telekom, KPN, KDDI, Spark NZ Ltd, DISH Network, T-Mobile USA, Telefónica,  |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 2023-09-06 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The currently specified N32 interface security prevents the proper working of Roaming Hubs |
|  |  |
| ***Summary of change:*** | In clause 3.1 add definitions for roaming hub, IPX provider, Roaming Intermediaries and IPX provider entities.In clause 5.9.3.2 – add requirements for Roaming HubsIn clause 5.9.3.2 – add requirements for all error messages on the N32-c interface to be visable at the roaming hub.In clause 5.9.3.2 – Add requirement for PLMNID aggrigation when originating from a roaming hub In clauses 5.9.3.2, 13.2.4.7 and 13.2.4.8, update Intermediaries to Roaming IntermediariesIn clause 13.2.4.5.2 – add means for the roaming hub to originate N32 messages within PRINS.In Clause 13.2.4.7 – add the abitlity for a SEPP to validate messages originated by a Roaming Hub |
|  |  |
| ***Consequences if not approved:*** | Roaming Hubs will not work to 3GPP specifications leading to potential market issues. |
|  |  |
| ***Clauses affected:*** | 3.1, 5.9.3.2, 13.2.4.5.2, 13.2.4.7, 13.2.4.8 |
|  |  |
|  | **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:*** |  |

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[12] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[25] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"

[26] Void

[27] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available <http://www.secg.org/sec1-v2.pdf>

[30] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

[38] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[39] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[40] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] Void.

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[44] IETF RFC 7519: "JSON Web Token (JWT)".

[45] IETF RFC 7515: "JSON Web Signature (JWS)".

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[48] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[49] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] Void

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

[60] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[61] IETF RFC 5705,"Keying Material Exporters for Transport Layer Security (TLS)".

[62] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] IETF RFC 9048: "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

[76] Internet draft draft-ietf-emu-eap-tls13: "Using EAP-TLS with TLS 1.3"

[77] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] Void

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

[90] RFC 2818: "HTTP Over TLS".

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[94] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition".

[95] 3GPP TS 29.502: "5G System; Session Management Services".

[96] 3GPP TS 29.526: "5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services".

[97] 3GPP TS 23.402: "Authentication enhancements for non-3GPP accesses".

[98] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[99] RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[100] RFC 6678: "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method".

[101] General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>.

[102] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

[103] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services".

[104] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[105] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

[106] 3GPP TS 23.554 Application architecture for MSGin5G Service; Stage 2.

[107] 3GPP TS 22.262 Message service with the 5G System (5GS); Stage 1.

[108] 3GPP TS 26.502: "5G multicast–broadcast services; User Service architecture".

[109] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

# 3 Definitions and abbreviations

## 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\_Authentication\_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 IPX (cIPX):** IPX provider entity 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:** For historical reasons this term in this specification is equivalent toRoaming Intermediary.

**IPX provider entity:** A type ofRoaming Intermediary defined by GSMA as IPX provider.

Editor's Note: GSMA does not use the term "IPX provider entity". Reference to GSMA PRD that defines the IPX provider will be added when GSMA determines the PRD in which it will be defined.

**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 IPX providers 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".

**producer's IPX (pIPX)**: IPX provider entity 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; as defined by GSMA.

Editor's Note: Reference to GSMA PRD that defines the IPX provider entity will be added when GSMA determines the PRD in which it will be defined.

**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].

**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.

\*\*\* Change \*\*\*

#### 5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)

The SEPP shall act as a non-transparent proxy node.

The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs or SNPNs that use the N32 interface to communicate with each other.

The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network.

The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.

The SEPP shall perform topology hiding by limiting the internal topology information visible to external parties.

As a reverse proxy the SEPP shall provide a single point of access and control to internal NFs.

The receiving SEPP shall be able to verify whether the sending SEPP is authorized to use the PLMN ID or SNPN ID in the received N32 message.

The SEPP to SEPP communication may go via up to two Roaming Intermediaries. The changes made by Roaming Intermediaries to messages originated by a SEPP, based on the originating PLMNs policy, shall be identifiable by the receiving SEPP.

The SEPP shall be able to clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of Roaming Intermediaries performing message modifications. The SEPP shall support multiple trust anchors.

NOTE 1: Such a differentiation and support of multiple trust anchors could be done e.g. by implementing separate certificate storages.

The SEPP shall discard malformed N32 signaling messages.

The sending SEPP shall reject messages received from the NF (directly or via SCP) with JSON including "encBlockIndex" (regardless of the encoding used for that JSON request).

The receiving SEPP shall reject any message in which a Roaming Intermediary has inserted or relocated references to encBlockIndex.

The SEPP shall implement rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling. This includes SEPP-to-SEPP signaling messages.

The SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).

NOTE 2: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the SEPP’s own PLMN (or SNPN), the message is discarded.

The SEPP shall be able to use one or more PLMN IDs (or SNPN IDs). In the situation that a PLMN (or SNPN)is using more than one PLMN ID (or SNPN ID), this PLMN's SEPP (or SNPN's SEPP) may use the same N32-connection for all of the networks PLMN IDs (or SNPN IDs), with each of the PLMN's (or SNPN's) remote partners. If different PLMNs (or SNPNs) are represented by the PLMN IDs (or SNPN IDs) supported by a SEPP, the SEPP shall use separate N32-connections for each pair of home and visited PLMN (or SNPN).

Note: If PRINS is used by a roaming hub, the roaming hub can use the same N32-f connection between the roaming hub and the adjecent PLMNs for the PLMNs accessed via the roaming hub

NOTE: in this case PRINS provides origin authentication and the originatining PLMN\_ID.

Error messages may be originated from either PLMN SEPPs to adjacent Roaming Hubs or Roaming Hubs to adjacent PLMN SEPPs, in an identifiable way.

Editor's Note: Whether the error messages are on N32 layer or on SBA signalling layer or both is ffs.

If allowed by the PLMN policy, the SEPP shall be able to send error messages on the N32 interface to a roaming hub via the N32-f.

Specific error messages relevant to Roaming Hubs shall be supported (such as 'an IE is encrypted while it was expected to be available in the clear', 'an IE is not encrypted while its availability in the clear is not required', 'the N32 connection cannot be setup due to contractual reasons', 'the N32 connection cannot be setup due to a connectivity issue' and 'the message was not delivered due to contractual reasons').

Sending SEPP behavior for the 3gpp-Sbi-Originating-Network-Id header specified in TS 29.500 [74]:

- If the sending NF or the SCP has inserted the 3gpp-Sbi-Originating-Network-Id header in the signaling message (service/subscription request or notification message), the sending SEPP shall compare the PLMN ID in the 3gpp-Sbi-Originating-Network-Id header in the received signaling message with the PLMN ID(s) that the sending SEPP represents by its certificate.

- If the PLMN ID does not match with any of the PLMN IDs that the sending SEPP represents, the sending SEPP shall discard the received signaling message.

- If the PLMN ID matches with any of the PLMN IDs that the sending SEPP represents, the sending SEPP shall forward the signaling message to the receiving SEPP.

- If the sending NF and the SCP have not included the 3gpp-Sbi-Originating-Network-Id header in the signalling message, the sending SEPP shall include the 3gpp-Sbi-Originating-Network-Id header and send the updated signaling message to the receiving SEPP.

- If the sending SEPP only represents one PLMN-ID, the sending SEPP shall insert the 3gpp-Sbi-Originating-Network-Id header with this ID.

- If the sending SEPP represents multiple PLMN-IDs, it is up to configuration and deployment to determine which PLMN-ID value should be included in the header.

Receiving SEPP behavior for the 3gpp-Sbi-Originating-Network-Id header:

- The receiving SEPP shall check whether the 3gpp-Sbi-Originating-Network-Id header included in the signalling message belongs to the sending SEPP’s own PLMN. It does this by verifying that the asserted PLMN ID in the 3gpp-Sbi-Originating-Network-Id header matches one of the sending SEPP's own PLMN ID(s) either in the N32-f context, the sending SEPP's certificate, or a locally configured list of PLMN-IDs that the sending SEPP represents.

- If the 3gpp-Sbi-Originating-Network-Id header does not match with any of the PLMN IDs belonging to the peer sending SEPP, the receving SEPP shall discard the received signaling message.

- If the 3gpp-Sbi-Originating-Network-Id header matches with any of the PLMN IDs IDs belonging to the peer sending SEPP, the header is successfully verified, and the receiving SEPP shall forward the received signaling message to the target NF.

\*\*\* Change \*\*\*

##### 13.2.4.5.2 Modifications by IPX

NOTE 1: It is assumed that operators act as a certification authority for IPX providers they have a direct business relationship with. In order to authorize N32-f message modifications, operators sign a digital certificate for each of these IPX providers and provide it to both the IPX provider itself as well as their roaming partners to enable them to validate any modifications by this IPX provider.

Only cIPX and pIPX shall be able to modify messages between cSEPP and pSEPP. In cases of messages from cSEPP to pSEPP, the cIPX is the first intermediary, while the pIPX is the second intermediary. In cases of messages from pSEPP to cSEPP the pIPX is the first intermediary, while the cIPX is the second intermediary.

The first intermediary shall parse the encapsulated request (i.e. the clearTextEncapsulationMsg in the dataToIntegrityProtect block) and determine which changes are required. The first intermediary creates an Operations JSON patch document to describe the differences between received and desired message, using the syntax and semantic from RFC 6902 [64], such that, when applying the JSON patch to the encapsulated request the result will be the desired request. If no patch is required, the operations element is null.

NOTE 2: It is necessary to create a JWS object even if no patch is required to prevent deletion of modifications.

The first intermediary shall create a modifiedDataToIntegrityProtect JSON object as described in clause 13.2.4.5.1. The JSON object shall include the intermediary’s identity and the JWE authentication tag, which associates this update by the intermediary with the JWE object created by the sending SEPP.

The first intermediary shall use the modifiedDataToIntegrityProtect JSON object as input to JWS to create a JWS object. The first intermediary shall append the generated JWS object to the payload in the HTTP message and then send the messageto the next hop.

The second intermediary shall parse the encapsulated request, apply the modifications described in the JSON patch appended by the first intermediary and determine further modifications required for obtaining the desired request. The second intermediary shall record these modifications in an additional JSON patch against the JSON object resulting from application of the first intermediary's JSON patch. If no patch is required, the operations element for the second JSON patch is null.

The second intermediary shall create a modifiedDataToIntegrityProtect JSON object as described in clause 13.2.4.5.1. It shall include its identity and the JWE authentication tag, which associates this update by the second intermediary with the JWE object created by the sending SEPP.

The second intermediary shall use the modifiedDataToIntegrityProtect JSON object as input to JWS to create a JWS object. The second intermediary shall append the generated JWS object to the payload in the HTTP message and then send the message to the receiving SEPP.

13.2.4.5.2a Modifications by Roaming Hub

In case a roaming hub needs to originate an error message, then clause 13.2.4.5.2 shall also apply with the following addition: If an error message needs to be sent, the originating roaming hub shall insert an empty reformattedData IE as defined in 29.573, Table 6.2.5.2.2-1 for the Request, and Table 6.2.5.2.3-1 for the response, and the patches shall be based on an empty reformattedData JSON element.

Editor's Note: Whether it is an empty reformattedData JSON element or an empty DataToIntegrityProtectBlock that is inserted by the Roaming Hub and that the Roaming Hub bases its patches on is ffs.

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

#### 13.2.4.7 Message verification by the receiving SEPP

The receiving SEPP shall decrypt the JWE ciphertext using the shared session key and the following parameters obtained from the JWE object – Initialization Vector, Additional Authenticated Data value (clearTextEncapsulatedMessage in "aad") and JWE Authentication Tag ( "tag").

If the reformattedData IE is not empty, the receiving SEPP shall check the integrity and authenticity of the clearTextEncapsulatedMessage and the encrypted text by verifying the JWE Authentication Tag in the JWE object with the JWE AAD algorithm. The algorithm returns the decrypted plaintext (dataToIntegrityProtectAndCipher) only if the JWE Authentication Tag is correct.

The receiving SEPP refers to the NF API data-type placement mapping table to re-construct the original reformatted message by updating corresponding entries in clearTextEncapsulatedMessage with values in the dataToIntegrityProtectAndCipher array.

The receiving SEPP shall next verify IPX provider updates, if included, by verifying the JWS signatures added by the Roaming Intermediaries. The SEPP shall verify the JWS signature, using the corresponding raw public key or certificate that is contained in the IPX provider’s security information list obtained during parameter exchange in the related N32-c connection setup or, alternatively, has been configured for the particular peer SEPP. If the reformattedData IE is not empty, the receiving SEPP shall then check that the raw public key or certificate of the JWS signature IPX's Identity in the modifiedDataToIntegrity block matches to the IPX provider referred to in the "authorizedIPX ID" field added by the sending SEPP, based on the information given in the IPX provider security information list. If the reformattedData IE is empty, the receiving SEPP shall check that the raw public key or certificate of the JWS signature IPX's identity in the modifiedDataToIntegrityProtect block matches to the adjacent roaming hub in the N32-f security context extracted from the modifiedDataToIntegrityProtect block, which is defined in clause 13.2.4.5.1, of the first roaming hub.

Editor's Note: Whether an N32-f security context of the roaming hub can be extracted from the modifiedDataToIntegrityProtect is ffs.

The receiving SEPP shall check whether the modifications performed by the Roaming Intermediaries were permitted by the respective modification policies. The receiving SEPP shall use the modification policy of the cIPX obtained during parameter exchange in the related N32-c connection setup, and use the modification policy of pIPX configured within the receiving SEPP.

If this is the case, the receiving SEPP shall apply the patches in the Operations field in order, perform plausibility checks, and create a new HTTP request according to the "patched" clearTextEncapsulatedMessage.

The receiving SEPP shall verify that the PLMN-ID contained in the incoming N32-f message matches the PLMN-ID in the related N32-f context.

#### 13.2.4.8 Procedure

The following clause illustrates the message flow between the two SEPPs with modifications from cIPX and pIPX.



Figure 13.2.4.8-1 Message flow between two SEPPs

1. The cSEPP receives an HTTP request message from a network function. If the message contains a telescopic FQDN, the cSEPP removes its domain name from this FQDN to obtain the original FQDN as described in clause 13.1.

2. The cSEPP shall reformate the HTTP Request message as follows:

a. The cSEPP shall generate blocks (JSON objects) for integrity protected data and encrypted data, and protecting them:

The cSEPP shall encapsulate the HTTP request into a clearTextEncapsulatedMessage block containing the following child JSON objects:

- Pseudo\_Headers

- HTTP\_Headers with one element per header of the original request.

- Payload that contains the message body of the original request.

For each attribute that require end-to-end encryption between the two SEPPs, the attribute value is copied into a dataToIntegrityProtectAndCipher JSON object and the attribute's value in the clearTextEncapsulatedMessage is replaced by the index of attribute value in the dataToIntegrityProtectAndCipher block.

The cSEPP shall create a metadata block that contains the N32-f context ID, message ID generated by the cSEPP for this request/response transaction and next hop identity.

The cSEPP shall protect the dataToIntegrityProtect block and the dataToIntegrityProtectAndCipher block as per clause 13.2.4.4. This results in a single JWE object representing the protected HTTP Request message.

b. The cSEPP shall generate payload for the SEPP to SEPP HTTP message:

 The JWE object becomes the payload of the new HTTP message generated by cSEPP.

3. The cSEPP shall use HTTP POST to send the HTTP message to the first Roaming Intermediary.

4. The first Roaming Intermediary (e.g. visited network's IPX provider) shall create a new modifiedDataToIntegrityProtect JSON object with three elements:

a. The Operations JSON patch document contains modifications performed by the first Roaming Intermediary as per RFC 6902 [64].

b. The first Roaming Intermediary shall include its own identity in the Identity field of the modifiedDataToIntegrityProtect.

c. The first Roaming Intermediary shall copy the "tag" element, present in the JWE object generated by the cSEPP, into the modifiedDataToIntegrityProtect object. This acts as a replay protection for updates made by the first Roaming Intermediary.

The Roaming Intermediary shall execute JWS on the modifiedDataToIntegrityProtect JSON object and append the resulting JWS object to the message.

5. The first Roaming Intermediary shall send the modified HTTP message request to the second Roaming Intermediary (e.g. home network's IPX) as in step 3.

6. The second Roaming Intermediary shall perform further modifications as in step 4 if required. The second Roaming Intermediary shall further execute JWS on the modifiedDataToIntegrityProtect JSON object and shall append the resulting JWS object to the message.

7. The second Roaming Intermediary shall send the modified HTTP message to the pSEPP as in step 3.

 NOTE 1: The behaviour of the Roaming Intermediaries is not normative, but the pSEPP assumes that behaviour for processing the resulting request.

8. The pSEPP receives the message and shall perform the following actions:

- The pSEPP extracts the serialized values from the components of the JWE object.

- The pSEPP invokes the JWE AEAD algorithm to check the integrity of the message and decrypt the dataToIntegrityProtectAndCipher block. This results in entries in the encrypted block becoming visible in cleartext.

- The pSEPP updates the clearTextEncapsulationMessage block in the message by replacing the references to the dataToIntegrityProtectAndCipher block with the referenced decrypted values from the dataToIntegrityProtectAndCipher block.

- The pSEPP then verifies IPX provider updates of the attributes in the modificationsArray. It checks whether the modifications performed by the Roaming Intermediaries were permitted by policy.

 The pSEPP further verifies that the PLMN-ID contained in the message is equal to the "Remote PLMN-ID" in the related N32-f context.

- The pSEPP updates the modified values of the attributes in the clearTextEncapsulationMessage in order.

The pSEPP shall re-assemble the full HTTP Request from the contents of the clearTextEncapsulationMessage.

9. The pSEPP shall send the HTTP request resulting from step 8 to the home network's NF.

10.-18. These steps are analogous to steps 1.-9.