**3GPP TSG-SA3 Meeting #115 *draft\_S3-240884-r1***

Athens, Greece, 26th February - 1st March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1968** | **rev** | **-** | **Current version:** | **16.17.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living document for backtracking 5G Roaming changes - Modification of PRINS to enable Roaming Hubs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, Vodafone | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16 | | | | |  | ***Date:*** | | | 2024-02-26 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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 can be 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:*** | | Backtracking the changes in scope of the 5G Roaming WID to earlier releases based on the endorsed wayforward from [S3-240313](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_115_Athens/Docs/S3-240313.zip). The changes introduce the necessary requirements to enable the support of Roaming Hubs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The proposed changes correspond to the ones from the agreed previous CRs: [SP-231202](https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGs_101_Bangalore_2023-09/Docs/SP-231202.zip), [S3-234764](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_113_Chicago/docs/S3-234764.zip) and [S3-235069](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_113_Chicago/docs/S3-235069.zip) | | | | | | | | |
|  | |  | | | | | | | | |
| ***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, 5.9.3.2a (new), 13.1.2, 13.2.1, 13.2.3.1, 13.2.2.3, 13.2.4.5.2, 13.2.4.5.2a (new), 13.2.4.7, 13.2.4.8, G1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Changes\*\*\*\*

## 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.

**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.

**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 of Roaming 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.

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

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

**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.

\*\*\*\* Next Changes\*\*\*\*

#### 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 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 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, the message is discarded.

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

NOTE X: If a given PLMN uses a Roaming Hub for the purposes of roaming with multiple other PLMNs, then a single TLS connection between the PLMN’s SEPP and the roaming hub can be used for carrying the N32-f PRINS signalling for some or all the other PLMNs.

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

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

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').

\*\*\*\* Next Changes\*\*\*\*

#### 5.9.3.2a Support for Messages generated by Roaming Intermediaries

A PLMN SEPP that makes use of Roaming Intermediaries shall be able to handle error messages generated by Roaming Intermediaries, delivered over the N32 connection.

The following error messages relevant to Roaming Hub shall be supported,

- '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'.

The mechanism used by the SEPP for setting up N32-c via a chain of Roaming Intermediaries shall contain sufficient information such that the target PLMN and the Roaming Intermediaries can determine the identities of the initiating PLMN and the target PLMN.

NOTE: The Roaming Intermediary can reject the N32-c connection if no roaming relation exists. In this case, the expected error is "the N32 connection cannot be setup due to contractual reasons".

Additionally, it shall be possible for the Roaming Hubs to generate application layer control plane messages in order to reject traffic. Application layer control plane messages may be generated by the Roaming Hubs in order to reject registration attempts (refer to TS 23.502 [8] clause 4.2.2.2), to terminate sessions (see TS 23.502 [8] clause 4.3.4.3) and/or deregister the UE (refer to TS 23.502 [8] clause 4.2.2.3.3) and shall be sent using the corresponding NF Service operation to the NF, when relevant decisions are enforced by the Roaming Hub.

In this case, such messages are transparent to the SEPP and the SEPP shall act on them as any other message on the N32-f interface not making use of Roaming Intermediaries. How the SEPP authorizes such messages is left to implementation.

\*\*\*\* Next Changes\*\*\*\*

### 13.1.2 Protection between SEPPs

TLS shall be used for N32-c connections between the SEPPs.

The SEPP shall maintain a set of trust anchors, each consisting of a list of trusted root certificates and a list of corresponding PLMN-IDs. Any given PLMN-ID shall appear in at most one trust anchor. During N32-c connection setup, the SEPP shall map the PLMN-ID of the remote SEPP leaf (server or client) certificate to the associated trust anchor for the purposes of certificate chain verification. Only the root certificates in the associated list shall be treated as trusted during certificate chain verification. If the remote SEPP certificate contains multiple PLMN-IDs that are mapped to different trust anchors, then that certificate shall be rejected.

If there are no IPX providers between the SEPPs, TLS shall be used for N32-f connections between the SEPPs. Different TLS connections are used for N32-c and N32-f. .If there are IPX providers which only offer IP routing service between SEPPs, either TLS or PRINS (application layer security) shall be used for protection of N32-f connections between the SEPPs. PRINS is specified in clause 5.9.3 (requirements) and clause 13.2 (procedures).

If TLS is selected, the SEPP shall correlate the N32-f TLS connection with the N32-c connection by comparing the PLMN-IDs contained in the SEPP TLS certificates used to establish the N32-c and N32-f connections. Specifically, if the certificate used for N32-f contains one or more PLMN-IDs that are not contained in the TLS certificate used for the corresponding N32-c, the N32-f certificate shall be rejected.

Operator Group Roaming Hubs SEPPs are equivalent to a network operator SEPP when they are in the same security domain and are not considered IPX providers as detailed in this clause. The communication between a group network operator's SBA network border element and the Operator Group Roaming Hub SEPP is out of scope of the present document.

If there are IPX providers which, in addition to IP routing, offer other services that require modification or observation of the information and/or additions to the information sent between the SEPPs, PRINS shall be used for protection of N32-f connections between the SEPPs.

NOTE 1a: The procedure specified in clause 13.5 for security mechanism selection between SEPPs allows SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32, and provides robustness and future-proofness, e.g. in case new algorithms are introduced in the future.

If PRINS is used on the N32-f interface, one of the following additional transport protection methods should be applied between SEPP and IPX provider for confidentiality and integrity protection:

- NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5], or

- TLS VPN with mutual authentication following the profile given in clause 6.2 of TS 33.210 [3] and clause clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks, with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

NOTE 1: Void

NOTE 2: Void.

\*\*\*\* Next Changes\*\*\*\*

### 13.2.1 General

The internetwork interconnect allows secure communication between service-consuming and a service-producing NFs in different PLMNs. Security is enabled by the Security Edge Protection Proxies of both networks, henceforth called cSEPP and pSEPP respectively. The SEPPs enforce protection policies regarding application layer security thereby ensuring integrity and confidentiality protection for those elements to be protected.

It is assumed that there are interconnect providers between cSEPP and pSEPP. The interconnect provider the cSEPP's operator has a business relationship with is called cIPX, while the interconnect provider the pSEPP's operator has a business relationship with is called pIPX. There could be further interconnect providers in between cIPX and pIPX, but they are assumed to be transparent and simply forward the communication.

The SEPPs use JSON Web Encryption (JWE, specified in RFC 7516 [59]) for protecting messages on the N32-f interface, and the IPX providers use JSON Web Signatures (JWS, specified in RFC 7515 [45]) for signing their modifications needed for their mediation services.

For illustration, consider the case where a service-consuming NF sends a message to a service-producing NF. If this communication is across PLMN operators over the N32-f interface, as shown in Figure 13.2.1-1 below, the cSEPP receives the message and applies symmetric key based application layer protection, as defined in clause 13.2 of the present document. The resulting JWE object is forwarded to Roaming Intermediaries. The pIPX and cIPX can offer services that require modifications of the messages transported over the interconnect (N32) interface. These modifications are appended to the message as digitally signed JWS objects which contain the desired changes. The pSEPP, which receives the message from pIPX, validates the JWE object, extracts the original message sent by the NF, validates the signature in the JWS object and applies patches corresponding to the modifications by Roaming Intermediaries. The pSEPP then forwards the message to the destination NF.

The N32 interface consists of:

- N32-c connection, for management of the N32 interface, and

- N32-f connection, for sending of JWE and JWS protected messages between the SEPPs.

The application layer security protocol for the N32 interface described in clause 13.2 of the present document is called PRINS.



Figure 13.2.1-1: Overview of PRINS

\*\*\*\* Next Changes\*\*\*\*

#### 13.2.3.1 Overview of protection policies

The protection policy suite is comprised of a data-type encryption policy and a modification policy. Together, these policies determine which part of a certain message shall be confidentiality protected and which part of a certain message shall be modifiable by IPX providers. The SEPP shall apply the protection policies for application layer protection of messages on the N32-f interface.

There are two types of protection policies, namely:

- Data-type encryption policy: specifies which data types need to be confidentiality protected;

- Modification policy: specifies which IEs are modifiable by Roaming Intermediaries.

In addition, there is a mapping between the data-types in the data-type encryption policy and the IEs in NF API descriptions which is given in a NF-API data-type placement mapping.

\*\*\*\* Next Changes\*\*\*\*

#### 13.2.2.3 Procedure for error detection and handling in SEPP

Errors can occur on an active N32-c connection or on one or more N32-f connections between two SEPPs.

When an error is detected, the SEPP shall map the error to an appropriate cause code. The SEPP shall create a signalling message to inform the peer SEPP, with cause code as one of its parameters.

The SEPP shall use the N32-c connection to send the signalling message to the peer SEPP. If the old N32-c connection has been terminated, it uses a new N32-c connection instead. If errors are relevant for the Roaming intermediaries, the error message shall be sent over N32-f to the peer SEPP, and shall be sent over N32-c if delivery over N32-f failed

If the error occurred in the processing of the one or more N32-f message(s), the SEPP shall include the corresponding message ID (s), obtained from the metadata section of the N32-f message, as a parameter in the signalling message. This allows the peer SEPP to identify the source message(s) (HTTP Request or Response) on which the other SEPP found the error.

NOTE: Local action taken by either SEPP is out of 3GPP scope.

\*\*\*\* Next Changes\*\*\*\*

##### 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 Roaming Intermediary, while the pIPX is the second Roaming Intermediary. In cases of messages from pSEPP to cSEPP the pIPX is the first Roaming Intermediary, while the cIPX is the second Roaming Intermediary.

The first Roaming Intermediary shall parse the encapsulated request (i.e. the clearTextEncapsulationMsg in the dataToIntegrityProtect block) and determine which changes are required. The first Roaming 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 Roaming Intermediary shall create a modifiedDataToIntegrityProtect JSON object as described in clause 13.2.4.5.1. The JSON object shall include the Roaming Intermediary's identity and the JWE authentication tag, which associates this update by the Roaming Intermediary with the JWE object created by the sending SEPP.

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

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

The second Roaming 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 Roaming Intermediary with the JWE object created by the sending SEPP.

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

\*\*\*\* Next Changes\*\*\*\*

##### 13.2.4.5.2a Error messages originated 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 a reformattedData JSON element including only the metadata IE as defined in TS 29.573 [73], Table 6.2.5.2.2 for the Request, and Table 6.2.5.2.3 for the response, and the patches shall be based on a reformattedData JSON element including only the metadata.

The reformattedData JSON element shall only contain metadata with N32-f message ID and N32-f context ID.

\*\*\*\* Next Changes\*\*\*\*

#### 13.2.4.7 Message verification by the receiving SEPP

The receiving SEPP determines that the received message is generated by the Roaming Hub based on the reformattedData IE.

If the received messages is not generated by a roaming hub:

- The receiving 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").

- 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.

- 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.

- The receiving SEPP shall check whether the modifications performed by the 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.

If the received message is generated by a Roaming Hub:

- The receiving SEPP shall check that the raw public key or certificate of the JWS signature IPX's identity in the modifiedDataToIntegrityProtect block matches the adjacent Roaming Hub identity.

- If the receiving SEPP determines from the error message that the Roaming Hub requires a modified request message, it can modify if allowed by the MNO's policy, and can resend the modified request message.

\*\*\*\* Next Changes\*\*\*\*

#### 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 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 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.

\*\*\*\* Next Changes\*\*\*\*

# G.1 Introduction

The SEPP as described in clause 4.X is the entity that sits at the perimeter of the network and performs application layer security on the HTTP message before it is sent externally over the roaming interface.

The application layer traffic comprises all the IEs in the HTTP message payload, sensitive information in HTTP message header and Request URI. Not all the IEs get the same security treatment in SEPP. Some IEs require e2e encryption, some only require e2e integrity protection, while other IEs may require e2e integrity protection but modifiable by intermediate IPX provider while in-transit.



Figure G.1-1: Signaling message from AMF (vPLMN) to AUSF (hPLMN) traversing the respective SEPPs

In the above figure, an example is shown where the AMF NF in the visited PLM network (vPLMN) invokes an API request on the AUSF NF in the home PLM network (hPLMN) using the following message flow:

- The AMF NF first sends the HTTP Request message to its local SEPP (i.e. vSEPP).

- The vSEPP applies application layer security (PRINS) and sends the secure message on the N32 interface to AUSF NF of the hPLMN.

- The hSEPP at the edge of the hPLMN, receives all incoming HTTP messages from its roaming partners. It verifies the message, removes the protection mechanism applied at the application layer, and forwards the resulting HTTP message to the corresponding AUSF NF.

To allow for the trusted Roaming Intermediary IPX nodes to see and possibly modify specific IEs in the HTTP message, while completely protecting all sensitive information end to end between SEPPs, the SEPP implements application layer security in such a way that:

- Sensitive information such as authentication vectors are fully e2e confidentiality protected between two SEPPs. This ensures that no node in the IPX network shall be able to view such information while in-transit.

- IEs that are subject to modification by Roaming Intermediary IPX nodes are integrity protected and can only be modified in a verifiable way by authorized IPX nodes.

- Receiving SEPP can detect modification by unauthorized IPX nodes.

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