**3GPP TSG-SA3 Meeting #115 *draft\_S3-240890-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1964** | **rev** | **-** | **Current version:** | **18.4.0** |  |
|  | | | | | | | | |
| *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:*** | Alignments on terminology for roaming intermediaries | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Roaming5G | | | | |  | ***Date:*** | | | 2024-03-01 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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 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:*** | | Roaming intermediaries were introduced in general, but text oftten refers to IPX only. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Updating to examplary IPX where apprpriate and using consistently RI throughout the spec. & Some format typos. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Roaming Hub and IPX provider ambiguity | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.2, 5.9.3.1, 5.9.3.2, 5.9.3.2a, 13.1.2, 13.2.1, 13.2.2.1, 13.2.2.2, 13.2.2.4.2, 13.2.2.4.3, 13.2.3.1, 13.2.3.2, 13.2.3.3, 13.2.3.4, 13.2.3.5, 13.2.4.1, 13.2.4.3.1.2, 13.2.4.5, 13.2.4.5.1, 13.2.4.5.2, 13.2.4.6, 13.2.4.7, 13.2.4.8, 13.5 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

**IPX provider**: Roaming Intermediary.

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

**IPX provider entity**: A type of Roaming 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.

<cut>

**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.

<cut>

**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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

## 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

CPA Conditional PSCell Addition

CPC Conditional PSCell Change

cPLMN consumer's PLMN

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

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

pPLMN producer's PLMN

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

NOTE: Void. Security Gateway

SEPP Security Edge Protection Proxy

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 5.9.3.1 General

The present sub-clause contains requirements common to sub-clauses 5.9.2 and 5.9.3.

A solution for e2e core network interconnection security shall satisfy the following requirements.

The solution shall support application layer mechanisms for addition, deletion and modification of message elements by intermediate nodes except for specific message elements described in the present document.

NOTE 1: Typical example for such a case is IPX providers modifying messages for routing purposes.

The solution shall support application layer mechanisms for generating error message elements by intermediate nodes.

NOTE 2: Typical example for such a case is a RH provider that needs to generate error messages due to operational aspects per contracts to the PLMN, which the RH provides its roaming services.

The solution shall provide confidentiality and/or integrity end-to-end between source and destination network for specific message elements identified in the present document. For this requirement to be fulfilled, the SEPP – cf [2], clause 6.2.17 shall be present at the edge of the source and destination networks dedicated to handling e2e Core Network Interconnection Security. The confidentiality and/or integrity for the message elements is provided between two SEPPs of the source and destination PLMN.

The destination network shall be able to determine the authenticity of the source network that sent the specific message elements protected according to the preceding bullet. For this requirement to be fulfilled, it shall suffice that a SEPP in the destination network that is dedicated to handling e2e Core Network Interconnection Security can determine the authenticity of the source network.

The solution should have minimal impact and additions to 3GPP-defined network elements.

The solution should be using standard security protocols.

The solution shall cover interfaces used for roaming purposes.

The solution should take into account considerations on performance and overhead.

The solution shall cover prevention of replay attacks.

The solution shall cover algorithm negotiation and prevention of bidding down attacks.

The solution should take into account operational aspects of key management.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT 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) representing the same PLMN. 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 PLMN's PLMN IDs (or SNPN IDs), with each of the PLMN’s (or SNPN’s) remote partners. If different PLMNs (or SNPNs) are represented by 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 3: If a given PLMN uses a Roaming Hub (RH) for the purposes of roaming with multiple other PLMNs, then a single TLS connection between the PLMN’s SEPP and the RH can be used for carrying the N32-f PRINS signalling for some or all the other PLMNs.

NOTE 4: void

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.

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

- 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 or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header in the received signaling message with the PLMN ID(s) or SNPN ID(s) that the sending SEPP represents by its certificate.

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

- If the sending SEPP represents multiple PLMN IDs or SNPN IDs, it is up to configuration and deployment to determine which PLMN ID or SNPN 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 or SNPN. 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) or SNPN ID(s) either in the N32-f context, the sending SEPP's certificate, or a locally configured list of PLMN IDs or SNPN-IDs that the sending SEPP represents.

- If the 3gpp-Sbi-Originating-Network-Id header does not match with any of the PLMN IDs or SNPN 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 PLMN ID of the PLMN or SNPN 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.

NOTE 5: Details on SEPP behaviour are specified in TS 29.500 [74].

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 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 1: 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 CHANGE

### 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.

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 no Roaming Intermediaries 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 Roaming Intermediarieswhich 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. If the peer network is a PLMN, the SEPP compares 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. If the peer network is an SNPN, the SEPP compares the SNPN-ID contained in the SEPP TLS certificates used to establish the N32-c and N32-f connections.

If there are Roaming Intermediarieswhich, 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 Roaming Intermediary or between two Roaming Intermediaries 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 9113 [47].

NOTE 1: Void

NOTE 2: Void.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

### 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.

NOTE: In the following the descriptions are provided for IPXs as Roaming Intermediaries, but equally apply to Roaming Hubs as Roaming Intermediaries. The domain ipxnetwok.org is used for both.

It is assumed that there are interconnect providers (Roaming Intermediaries, RIs) 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 CHANGE

### 13.2.2 N32-c connection between SEPPs

#### 13.2.2.1 General

When the negotiated security mechanism to use over N32, according to the procedure in clause 13.5, is PRINS (described in clause 13.2), the SEPPs use the established TLS connection (henceforth referred to as N32-c connection) to negotiate the N32-f specific associated security configuration parameters required to enforce application layer security on HTTP messages exchanged between the SEPPs. A second N32-c connection is established by the receiving SEPP to enable it to not only receive but also send HTTP Requests.

The N32-c connection is used for the following purposes:

- Key agreement: The SEPPs independently export keying material associated with the first N32-c connection between them and use it as the pre-shared key for generating the shared session key required.

- Parameter exchange: The SEPPs exchange security related configuration parameters that they need to protect HTTP messages exchanged between the two Network Functions (NF) in their respective networks.

- Error handling: The receiving SEPP sends an error signalling message to the peer SEPP when it detects an error on the N32-f interface.

The following security related configuration parameters may be exchanged between the two SEPPs:

a. Modification policy. A modification policy, as specified in clause 13.2.3.4, indicates which IEs can be modified by a Roaming Intermediary (RI) of the sending SEPP.

b. Data-type encryption policy. A data-type encryption policy, as specified in 13.2.3.2, indicates which types of data will be encrypted by the sending SEPP.

c. Cipher suites for confidentiality and integrity protection, when application layer security is used to protect HTTP messages between them.

d. N32-f context ID. As specified in clause 13.2.2.4.1, N32-f context ID identifies the set of security related configuration parameters applicable to a protected message received from a SEPP in a different PLMN.

#### 13.2.2.2 Procedure for Key agreement and Parameter exchange

1. The two SEPPs shall perform the following cipher suite negotiation to agree on a cipher suite to use for protecting NF service related signalling over N32-f.

1a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP’s supported cipher suites. The cipher suites shall be ordered in initiating SEPP’s priority order. The SEPP shall provide an initiating SEPP’s N32-f context ID for the responding SEPP.

1b. The responding SEPP shall compare the received cipher suites to its own supported cipher suites and shall select, based on its local policy, a cipher suite, which is supported by both initiating SEPP and responding SEPP.

1c. The responding SEPP shall send a Security Parameter Exchange Response message to the initiating SEPP including the selected cipher suite for protecting the NF service related signalling over N32. The responding SEPP shall provide a responding SEPP’s N32-f context ID for the initiating SEPP.

2. The two SEPPs may perform the following exchange of Data-type encryption policies and Modification policies. Both SEPPs shall store protection policies sent by the peer SEPP:

2a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP’s Data-type encryption policies, as described in clause 13.2.3.2, and Modification policies, as described in clause 13.2.3.4.

2b. The responding SEPP shall store the policies if sent by the initiating SEPP.

2c. The responding SEPP shall send a Security Parameter Negotiation Response message to the initiating SEPP with the responding SEPP’s suite of protection policies.

2d. The initiating SEPP shall store the protection policy information if sent by the responding SEPP.

3. The two SEPPs shall exchange Roaming Intermediary (RI) security information lists that contain information on RI public keys or certificates that are needed to verify RI modifications at the receiving SEPP.

4. The two SEPPs shall export keying material from the TLS session established between them using the TLS export function. For TLS 1.2, the exporter specified in RFC 5705 [61] shall be used. For TLS 1.3, the exporter described in section 7.5 of RFC 8446 [60] shall be used. The exported key shall be used as the master key to derive session keys and IVs for the N32-f context as specified in clause 13.2.4.4.1.

5. When the responding SEPP needs to initiate traffic, e.g., error reporting, in the reverse direction to the sending SEPP, the responding SEPP in the first N32-c connection shall now setup a second N32-c connection by establishing a mutually authenticated TLS connection with the peer SEPP.

NOTE: The second N32-c connection setup by the responding SEPP does not perform the negotiation of steps 1-4.

6. The two SEPPs start exchanging NF to NF service related signalling over N32-f and tear down the N32-c connection. The SEPPs may initiate new N32-c TLS sessions for any further N32-c communication that may occur over time while application layer security is applied to N32-f.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

##### 13.2.2.4.2 N32-f peer information

The N32-f connection between SEPPs is bidirectional and consists of the two SEPP endpoints and possibly up to two Roaming Intermediaries. The SEPPs are identified by the PLMN ID and additionally a SEPP ID to distinguish between several SEPPs in the same PLMN. The remote SEPP address is necessary for routing the messages to the correct destination.

The N32-f peer information shall consist of the following parameters:

- Remote PLMN ID;

- Remote SEPP ID;

- Remote SEPP address.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

##### 13.2.2.4.3 N32-f security context

The N32-c initial handshake described in clause 13.2.2.2 establishes session keys, Ivs and negotiated cipher suites. Counters are used for replay protection. Modification policies are identified by modification policy IDs, to be able to verify received messages that have undergone RI modifications.

The N32-f security context shall consist of the following parameters:

- Session keys

- Negotiated cipher suites

- Data type encryption policy IDs

- Modification policy list (if RIs are used)

- Modification policy IDs

- RI provider identifier

- Counters

- Ivs

- List of security information of the Roaming Intermediaries connected to the SEPPs (RI security information list)

- RI provider identifier

- List of raw public keys or certificates for that Roaming Intermediary

#### 

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 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 Roaming Intermediaries. 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 CHANGE

#### 13.2.3.2 Data-type encryption policy

The SEPP shall contain an operator-controlled protection policy that specifies which types of data shall be encrypted. The data-types defined are the following:

- Data of the type ‘SUPI’;

- Data of the type ‘authentication vector’;

- Data of the type ‘location data’;

- Data of the type ‘cryptographic material’;

- Data of the type ‘authorization token’.

The policy shall be specific per roaming partner. The policy shall contain a policy identifier and a release number referring to the release it is applicable for.

The data-type encryption policies in the two partner SEPPs shall be equal to enforce a consistent ciphering of Ies on N32-f.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 13.2.3.3 NF API data-type placement mapping

Each NF API data-type placement mapping shall contain the following:

- Which Ies contain data of the type ‘SUPI’ or type ‘NAI’.

- Which Ies contain data of the type ‘authentication vector’.

- Which Ies contain data of the type ‘location data’.

- Which Ies contain data of the type ‘cryptographic material’.

- Which Ies contain data of the type ‘authorization token’.

The location of the Ies refers to the location of the Ies after the SEPP has rewritten the message for transmission over N32-f.

An NF API data-type placement mapping shall furthermore contain data that identifies the NF API, namely

- The name of the NF;

- The API version;

- An identifier for the NF API data-type placement mapping;

- The NF’s 3GPP Release version.

NOTE: Larger networks can contain multiple NFs with the same API, e.g. three AMFs. The NF API policy applies to all NFs with the same API.

The NF API data-type placement mapping shall reside in the SEPP.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 13.2.3.4 Modification policy

The SEPP shall contain an operator-controlled policy that specifies which Ies can be modified by the RI provider directly related to this particular SEPP. These Ies refer to the Ies after the sending SEPP has rewritten the message.

Each PLMN-operator shall agree the modification policy with the RI provider it has a business relationship with prior to establishment of an N32 connection. Each modification policy applies to one individual relation between PLMN-operator and RI provider. To cover the whole N32 connection, both involved roaming partners shall exchange their modification policies.

NOTE 1: In order to validate modifications for messages received on the N32-f interface, the operator’s roaming partners will have to know the overall modification policy.

NOTE 2: Modification includes removal and addition of new IE. Ies therefore may not be present in the rewritten message.

The Ies that the RI is allowed to modify shall be specified in a list giving an enumeration of JSON paths within the JSON object created by the SEPP. Wildcards may be used to specify paths.

This policy shall be specific per roaming partner and per RI provider that is used for the specific roaming partner.

The modification policy shall reside in the SEPP.

For each roaming parter, the SEPP shall be able to store a policy for receiving.

The following basic validation rules shall always be applied irrespective of the policy exchanged between two roaming partners:

- Ies requiring encryption shall not be inserted at a different location in the JSON object.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 13.2.3.5 Provisioning of the policies in the SEPP

The SEPP shall contain an interface that the operator can use to manually configure the protection policies in the SEPP.

The SEPP shall be able to store and process the following policies for outgoing messages:

- A generic data-type encryption policy;

- Roaming partner specific data-type encryption policies that will take precedence over a generic data-type encryption policy if present;

- NF API data-type placement mappings;

- Multiple modification policies, to handle modifications that are specific per RI provider and modification policies that are specific per RI provider and roaming partner.

The SEPP shall also be able to store and process the following policies for incoming messages during the initial connection establishment via N32-c:

- Roaming partner specific data-type encryption policies;

- Roaming partner specific modification policies that specify which fields can be modified by which of its RI providers.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 13.2.3.6 Precedence of policies in the SEPP

This clause specifies the order of precedence of data-type encryption policies and modification policies available in a SEPP.

In increasing order of precedence, the following policies apply for a message to be sent on N32:

1. The set of default rules specified in the present specification:

- For the data-type encryption policy, the rules on data-types that are mandatory to be encrypted according to clause 5.9.3.3.

- For the modification policy, the basic validation rules defined in clause 13.2.3.4.

2. Manually configured policies:

- For the data-type encryption policy: rules according to clause 13.2.3.2, on a per roaming partner basis.

- For the modification policy: rules according to clause 13.2.3.4, per roaming partner and per RI provider that is used for the specific roaming partner.

NOTE 1: It is assumed that operators agree both data-type encryption and modification policy in advance, for example as part of their bilateral roaming agreement. The protection policies exchanged via N32-c during the initial connection establishment only serve the purpose of detecting possible misconfigurations.

NOTE 2: It is assumed that the default rules and manually configured policies do not overlap or contradict each other. The manually configured policies are used to extend the protection by the default rules in the present document and are applied on top of them.

When a SEPP receives a data-type encryption or modification policy on N32-c as specified in clause 13.2.2.2, it shall compare it to the one that has been manually configured for this specific roaming partner and RI provider. If a mismatch occurs for one of the two policies, the SEPP shall perform one of the following actions, according to operator policy:

- Send the error message as specified in TS 29.573 [73], clause 6.1.4.3.2, to the peer SEPP.

- Create a local warning.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 13.2.4.1 General

The SEPP receives HTTP/2 request/response messages from the Network Function. It shall perform the following actions on these messages before they are sent on the N32-f interface to the SEPP in the other PLMN:

a) It parses the incoming message and, if present, rewrites the telescopic FQDN of the receiving NF to obtain the original FQDN as described in clause 13.1.

b) It reformats the message to produce the input to JSON Web Encryption (JWE) [59] as described in clause 13.2.4.3.

c) It applies JWE to the input created in b) to protect the reformatted message as described in clause 13.2.4.4.

d) It encapsulates the resulting JWE object into a HTTP/2 message (as the body of the message) and sends the HTTP/2 message to the SEPP in the other PLMN over the N32-f interface.

The message may be routed via the two Roaming Intermediaries, e.g., cIPX and pIPX nodes. These RI nodes may modify messages as follows:

a) The RI node recovers the cleartext part of the HTTP message from the JWE object, modifies it according to the modification policy, and calculates an "operations" JSON Patch object. It then creates a temporary JSON object with the "operators" JSON Patch object and some other parameters for replay protection etc. as described in clause 13.2.4.5.1.

b) The RI node uses the temporary JSON object as input into JSON Web Signature (JWS) [45] to create a JWS object, as described in clause 13.2.4.5.2.

c) The RI node appends the JWS object to the received message and sends it to the next hop.

The JWS objects generated by the two RI providers form an auditable chain of modifications that to the receiving SEPP shall apply to the parsed message after verifying that the patches conform to the modification policy.

Encryption of IEs shall take place end to end between cSEPP and pSEPP.

A SEPP shall not include IEs in the clear that are encrypted elsewhere in the JSON object.

A SEPP shall verify that an intermediate RI has not moved or copied an encrypted IE to a location that would be reflected from the producer NF in an IE without encryption.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

###### 13.2.4.3.1.2 metadata

The JSON object containing information added by the sending SEPP. It shall contain:

a) N32-f **message ID**: Unique identifier (64-bit integer) representing a HTTP Request/Response transaction between two SEPPs. The N32-f message ID is generated by the sending SEPP and included in the HTTP Request sent over the N32 interface. The receiving SEPP uses the same N32-f message ID when it responds back with a HTTP Response. The N32-f message ID is included in the metadata portion of the JSON structure.

b) **authorizedIPX** **ID**: String identifying the first hop RI (, e.g., cIPX or pIPX) that is authorized to update the message. This field shall always be present. When there is no RI that is authorized to update, the value of this field is set to null. The sending SEPP selects one of the RI providers from the list exchanged with the other SEPP during parameter exchange over N32-c and includes its identifier value in this field.

c) **N32-f context ID**: Unique identifier representing the N32-f context information used for protecting the message. This is exchanged during parameter exchange over N32-c (clause 13.2.2.4.1).

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 13.2.4.5 Message modifications by Roaming intermediary

##### 13.2.4.5.1 modifiedDataToIntegrityProtect



Figure 13.2.4.5.1-1 Example of JSON representation for RI with IPX1 provider modifications

This is a temporary JSON object generated by a RI provider as it modifies the original message. It shall contain the following:

a) **Operations** – This is a JSON patch document that captures RI modifications based on RFC 6902 [64]. If no patch is required, the operations element shall be set to null.

b) **Identity** – This is the identity of the RI performing the modification.

c) **Tag** – A JSON string element to capture the “tag” value (JWE Authentication tag) in the JWE object generated by the sending SEPP. This is required for replay protection.

NOTE: Since there is no central registry that can ensure unique RI Identities, it is expected that an RI will include its Fully Quantified Domain Name (FQDN) in the JSON modification object.

##### 13.2.4.5.2 Modifications by RIs

NOTE 1: It is assumed that operators act as a certification authority for RI 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 RI providers and provide it to both the RI provider itself as well as their roaming partners to enable them to validate any modifications by this RI provider.

Only the maximum two RIs, e.g., 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 RI, while the cIPX is the second RI.

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

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

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

The second RI 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 RI with the JWE object created by the sending SEPP.

The second RI shall use the modifiedDataToIntegrityProtect JSON object as input to JWS to create a JWS object. The second RI 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 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 CHANGE

#### 13.2.4.6 Protecting RI modifications using JSON Web Signature (JWS)

The RI providers shall use JSON Web Signature (JWS) as specified in RFC 7515 [45] for the protection of RI provider modified attributes. The mechanism described in this clause uses signatures, i.e. asymmetric methods, with private/public key pairs.

More specifically, when a RI node modifies one or more attributes of the original HTTP message and creates a modifiedDataToIntegrityProtect object to record its modifications, it shall use JWS to integrity protect the modifiedDataToIntegrityProtect object.

The RI provider shall use its private key as input to JWS for generating the signature representing the contents of the modifiedDataToIntegrityProtect object.

The "alg" parameter in the JOSE header indicates the chosen signature algorithm. The 3GPP profile for supported algorithms is described in clause 13.2.4.9.

The Flattened JWS JSON Serialization syntax shall be used to represent JWS as a JSON object.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

#### 13.2.4.7 Message verification by the receiving SEPP

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

If the received messages is not generated by a Roaming Hub :

- 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").

- 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 in clearTextEncapsulatedMessage with values in the dataToIntegrityProtectAndCipher array.

- The receiving SEPP shall next verify RI 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 RI's Identity in the modifiedDataToIntegrity block matches to the RI provider referred to in the "authorizedIPX ID" field added by the sending SEPP, based on the information given in the RI provider security information list.

- The receiving SEPP shall check whether the modifications performed by the Roaming Intermediaries, i.e. cIPX and pIPX, 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 RI'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 CHANGE

#### 13.2.4.8 Procedure

The following clause illustrates the message flow between the two SEPPs with modifications from RIs, e.g., 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.

## 

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

## 13.5 Security capability negotiation between SEPPs

The security capability negotiation over N32-c allows the SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32-f. There shall be an agreed security mechanism between a pair of SEPPs before conveying NF service-related signalling over N32-f.

When a SEPP notices that it does not have an agreed security mechanism for N32-f protection with a peer SEPP or if the security capabilities of the SEPP have been updated, the SEPP shall perform security capability negotiation with the peer SEPP over N32-c in order to determine, which security mechanism to use for protecting NF service-related signalling over N32-f. Certificate based authentication shall follow the profiles given in 3GPP TS 33.210 [3], clause 6.2.

A mutually authenticated TLS connection as defined in clause 13.1 shall be used for protecting security capability negotiation over N32-c. The TLS connection shall provide integrity, confidentiality and replay protection.



Figure 13.5-1 Security capability negotiation

1. The SEPP which initiated the TLS connection shall issue a POST request to the exchange-capability resource of the responding SEPP including the initiating SEPP’s supported security mechanisms for protecting the NF service-related signalling over N32-f (see table Table 13.5-1). The security mechanisms shall be ordered in the initiating SEPP’s priority order.

2. The responding SEPP shall compare the received security capabilities to its own supported security capabilities and selects, based on its local policy (e.g. based on whether there are RI providers on the path between the SEPPs), a security mechanism, which is supported by both initiating SEPP and responding SEPP.

3. The responding SEPP shall respond to the initiating SEPP with the selected security mechanism for protecting the NF service-related signalling over N32.

Table 13.5-1: NF service-related signalling traffic protection mechanisms over N32

|  |  |
| --- | --- |
| N32-f protection mechanism | Description |
| Mechanism 1 | PRINS (described in clause 13.2) |
| Mechanism 2 | TLS |
| Mechanism n | Reserved |

If the selected security mechanism is PRINS, the SEPPs shall behave as specified in clause 13.2.

If the selected security mechanism is TLS, the SEPPs shall behave as specified in clause 13.1.2, tear down the N32-c connection and forward the NF service related signalling over N32-f using a TLS connection.

If the selected security mechanism is a mechanism other than the ones specified in Table 13.5-1, the two SEPPs shall terminate the N32-c TLS connection.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES