**3GPP TSG-SA3 Meeting #116 *draft S3-242460-r2***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **-** | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | Resolving EN on roaming and interconnect | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Roaming5G | | | | |  | ***Date:*** | | | 2024-05-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | Clause 4.2.0 states that the security specified in 33.501 applies to both roaming and PLMN interconnect. This CR is to resolve the following EN.  Editor's Note: check full specification on removing references to roaming unless specific to roaming. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Some typos are also corrected. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | ***S3-242214*** | | | | | | | | |

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

4.2.0 General

The security specified in this document applies to both roaming and PLMN interconnect.

\*\*\*\*\*\*\*\*\*\* 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: Typical example for such a case is IPX providers modifying messages for routing purposes.

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 feature of supporting roaming hubs by SEPPs introduced in Release 18, i.e. in TS 33.501 (the present document) and TS 29.573 [73], addresses the requirements that may be applicable to SEPPs starting from Release 16.

In order to support PRINS functionality using roaming intermediaries, the feature specified in this document may be supported by Release 16 and 17 implementations of SEPPs.

NOTE: It is implementation specific on how to support the scenario where the Rel 16 and 17 SEPP of the roaming partners are not aligned regarding the support of roaming hub/intermediaries.

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 with the SEPP in the roaming network.

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

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

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

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

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

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

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

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

The SEPP shall discard malformed N32 signaling messages.

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

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

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

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

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

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

NOTE 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 (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'). See details in clause 5.9.3.2a.

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 receiving 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

## 9.9 Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs

Non-SBA interfaces internal to the 5G Core such as N4 and N9 can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, these interfaces shall be confidentiality, integrity, and replay protected.

Roaming interfaces between PLMNs except for N32, shall be confidentiality, integrity, and replay protected. Protection for the N32 interface is specified in clauses 13.1 and 13.2..

For the protection of the above-mentioned non-SBA internal and roaming interfaces except N32, IPsec ESP and IKEv2 certificate-based authentication shall be supported as specified in sub-clauses 9.1.2 of the present document with confidentiality, integrity and replay protection. This security mechanism shall be used, unless security is provided by other means, e.g. physical security. A SEG may be used to terminate the IPsec tunnels.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

NOTE: It is up to the operator choice to use cryptographic solutions or other mechanisms to protect internal non-SBA interfaces such as N4 and N9.

\*\*\*\*\*\*\*\*\*\* 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 Intermediaries 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. 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 Intermediaries 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 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 providers as Roaming Intermediaries, but equally apply to Roaming Hubs as Roaming Intermediaries.

It is assumed that there are interconnect providers between cSEPP and pSEPP. The interconnect provider with which the cSEPP's operator has a business relationship with is called cIPX, while the interconnect provider with which 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

#### 13.3.2.3 Inter-PLMN NF to NF communication

NOTE 1: Void

NOTE 2: Void

The Inter-PLMN UP Security functionality (IPUPS) as described in clauses 4.2.2 and 5.9.3.4 provide a standardised solution for binding 5G SBA REST Service Operations between the PLMN V-SMF and H-SMF over N16 / N32 to GTP-U over N9 in roaming scenarios.

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

# G.1 Introduction

The SEPP as described in clause 4.2.1 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.

NOTE: In the following, the descriptions are provided for IPXs as one example of Roaming Intermediary, but equally apply to Roaming Hubs as Roaming Intermediaries.



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 roaming intermediary IPX nodes to see what the two PLMNs have negotiated by policy to be visible, and possibly to 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