**3GPP TSG-CT WG4 Meeting #99eC4-204xxx**

**E-Meeting, 18th – 28th August 2020** *Revision of C4-204185*

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **29.573** | **CR** | **0041** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | TLS security with the 3gpp-Sbi-Target-apiRoot header on N32f |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, NTT DOCOMO |
| ***Source to TSG:*** | CT4 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 2020-08-03 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | 1) TS 33.501 enables the use of the 3gpp-Sbi-Target-apiRoot header with TLS security on N32f. *13.1.1.2 TLS protection based on 3gpp-Sbi-Target-apiRoot HTTP header* *The NF uses the 3gpp-Sbi-Target-apiRoot HTTP header in the HTTP Request to convey the target FQDN to the SEPP.**…**If TLS is used on the N32 interface, the following applies: The sending SEPP shall replace the authority header in the HTTP Request with the FQDN of the receiving SEPP before forwarding the protected HTTP Request on the N32 interface. The sending SEPP shall not change the 3gpp-Sbi-Target-apiRoot header.*Corresponding requirements are missing in TS 29.573.2) For backward compatibility with Rel-15 SEPPs (the 3gpp-Sbi-Target-apiRoot header has been defined from Rel-16 onwards), when negotiating TLS security over N32f, SEPPs need to indicate whether they support TLS security using the 3gpp-Sbi-Target-apiRoot header. 3) In case the originating NF consumer does not support 3gpp-Sbi-Target-apiRoot header (e.g. Rel-15 NF) and TLS with the 3gpp-Sbi-Target-apiRoot header is used over N32f, the local SEPP inserts a 3gpp-Sbi-Target-apiRoot header with the value derived from the telescopic FQDN received from the originating NF consumer.  |
|  |  |
| ***Summary of change:*** | 1) SEPP requirements and call flows are specified to describe the SEPP behaviour when TLS security is used on N32f with the 3gpp-Sbi-Target-apiRoot header. This covers both cases where telescopic FQDN or the 3gpp-Sbi-Target-apiRoot header are used between NFs and their local SEPP.2) The Security Capability Negotiation Procedure is extended to enable SEPPs to indicate whether they support TLS security using the 3gpp-Sbi-Target-apiRoot header. |
|  |  |
| ***Consequences if not approved:*** | Misalignment between TS 33.501 and TS 29.573, that will cause interoperability issues over N32f. Regular HTTPS cannot be used over N32f. |
|  |  |
| ***Clauses affected:*** | 5.2.2, 5.3.3, 6.1.5.2.2, 6.1.5.2.3, C.2.1, C.2.1.z (new), C.2.2.2, C.2.2.3, C.2.2.x (new), C.2.2.y (new), A.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 29.500 CR 0150  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** | This CR introduces backward compatible corrections to the N32 Handshake OpenAPI specification file. |
|  |  |
| ***This CR's revision history:*** | Rev. 1: Changes that were proposed in clause 5.3.3 are moved into CR 29.500 #0150. "Other specs affected" is updated to indicate a dependency on the 29.500 CR. |

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

### 5.2.2 Security Capability Negotiation Procedure

The initiating SEPP shall initiate a Security Capability Negotiation procedure towards the responding SEPP to agree on a security mechanism to use for protecting NF service related signalling over N32-f. An end to end TLS connection shall be setup between the SEPPs before the initiation of this procedure. The procedure is described in Figure 5.2.2-1 below.



Figure 5.2.2-1: Security Capability Negotiation Procedure

1. The initiating SEPP issues a HTTP POST request towards the responding SEPP with the request body containing the "SecNegotiateReqData" IE carrying the following information:

- Supported security capabilities (i.e PRINS and/or TLS);

- whether the 3gpp-Sbi-Target-apiRoot HTTP header is supported, if TLS security is supported.

2a. On successful processing of the request, the responding SEPP shall respond to the initiating SEPP with a "200 OK" status code and a POST response body that contains the following information:

- Selected security capability (i.e PRINS or TLS);

- whether the 3gpp-Sbi-Target-apiRoot HTTP header is supported, if TLS security is selected.

The responding SEPP compares the initiating SEPP's supported security capabilities to its own supported security capabilities and selects, based on its local policy, a security mechanism, which is supported by both the SEPPs. If the selected security capability indicates any other capability other than PRINS, then the HTTP/2 connection initiated between the two SEPPs for the N32 handshake procedures shall be terminated. The negotiated security capability shall be applicable on both the directions. If the selected security capability is PRINS, then the two SEPPs may decide to create (if not available) / maintain HTTP/2 connection(s) where each SEPP acts as a client towards the other (which acts as a server). This may be used for later signalling of N32-f error reporting procedure (see clause 5.2.5) and N32-f context termination procedure (see clause 5.2.4).

2b. On failure, the responding SEPP shall respond to the initiating SEPP with an appropriate 4xx/5xx status code as specified in clause 6.1.4.2.

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

### 5.3.3 Message Forwarding to Peer SEPP when TLS is used

When the negotiated security policy between the SEPPs is TLS, then the procedures described in clause 5.3.2 shall not be applied. Messages shall be forwarded to the peer SEPP as specified in clause 6.1.4.3.4 of 3GPP TS 29.500 [4].

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

##### 6.1.5.2.2 Type: SecNegotiateReqData

Table 6.1.5.2.2-1: Definition of type SecNegotiateReqData

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| sender | Fqdn | M | 1 | This IE shall uniquely identify the SEPP that is sending the request. This IE is used to store the negotiated security capability against the right SEPP. |
| supportedSecCapabilityList | array(SecurityCapability) | M | 1..N | This IE shall contain the list of security capabilities that the requesting SEPP supports. |
| 3GppSbiTargetApiRootSupported | boolean | C | 0..1 | This IE should be present and indicate that the 3gpp-Sbi-Target-apiRoot HTTP header is supported, if TLS security is supported for N32f message forwarding.When present, it shall indicate if TLS security using the 3gpp-Sbi-Target-apiRoot HTTP header is supported: - true: supported- false (default): not supported |

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

##### 6.1.5.2.3 Type: SecNegotiateRspData

Table 6.1.5.2.3-1: Definition of type SecNegotiateRspData

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| sender | Fqdn | M | 1 | This IE shall uniquely identify the SEPP that is sending the response. This IE is used to store the negotiated security capability against the right SEPP. |
| selectedSecCapability | SecurityCapability | M | 1 | This IE shall contain the security capability selected by the responding SEPP. |
| 3GppSbiTargetApiRootSupported | boolean | C | 0..1 | This IE should be present and indicate that the 3gpp-Sbi-Target-apiRoot HTTP header is supported, if TLS security is negotiated for N32f message forwarding and the initiating SEPP indicated support of this header.When present, it shall indicate if TLS security using the 3gpp-Sbi-Target-apiRoot HTTP header is supported: - true: supported- false (default): not supported |

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

## C.2 TLS security between SEPPs

### C.2.1 When http URI scheme is used

#### C.2.1.1 General

The following figure shows the end to end call flow between an NF service consumer and a NF service producer in different PLMNs when:

- the SEPP in each PLMN acts as a security proxy;

- the negotiated security policy between the SEPPs is TLS;

- "http" scheme URI is used between the NF service consumer and NF service producer; and

- "http" scheme URI is used for accessing NRF's NF discovery service.

#### C.2.1.2 Without TLS protection between NF and SEPP and with TLS security without the 3gpp-Sbi-Target-apiRoot header used over N32f



Figure C.2.1.2-1: End to end call flow when http scheme URI is used and TLS security without the 3gpp-Sbi-Target-apiRoot header used is used between SEPPs

1. The SEPP on the NF service consumer side (c-SEPP) and the SEPP on the NF service producer side (p-SEPP) negotiate the security capabilities using the procedure specified in clause 5.2.2. The SEPPs mutually negotiate to use TLS as the security policy.

2. A TLS connection is setup between the c-SEPP and the p-SEPP for N32-f forwarding.

3. Before the NF service consumer starts using the API of the NF service producer it needs to discover the NF service profile of the producer by querying the NRF. The NF service consumer uses "http" scheme URI to access the Nnrf\_NFDiscovery service.

4. The NRF on the NF service consumer side (c-NRF) needs to further initiate a discovery request to the NRF on the NF service producer side (p-NRF). The c-NRF is configured to route all HTTP messages with inter PLMN FQDN as the "authority" part of the URI via the c-SEPP. The c-SEPP acts as a HTTP proxy.

5. The c-SEPP forwards the NF discovery request within the N32-f TLS tunnel established in step 2.

6. The p-SEPP forwards the NF discovery request to the p-NRF.

7. The p-NRF sends the NF discovery response. The NF service profile contains service URI with "http" scheme. The FQDN of the NF service is an inter PLMN FQDN.

8. The p-SEPP forwards the NF discovery response within TLS tunnel to the c-SEPP.

9. The c-SEPP forwards the NF discovery response to c-NRF.

10. The c-NRF sends the NF discovery response to NF service consumer.

11. The NF service profile received at the NF service consumer contains service URI with "http" scheme. The NF service consumer initiates a HTTP message (as supported by the NF service producer API) using "http" scheme URI. The NF service consumer is configured to route all HTTP messages with inter PLMN FQDN as the "authority" part of the URI via the c-SEPP. The c-SEPP acts as a HTTP proxy.

12. The c-SEPP forwards the HTTP service request within the N32-f TLS tunnel established in step 2.

13. The p-SEPP forwards the HTTP service request to the NF service producer.

14. The NF service producer sends the HTTP service response.

15. The p-SEPP forwards the HTTP service response within TLS tunnel to the c-SEPP.

16. The c-SEPP forwards the HTTP service response to the NF service consumer.

#### C.2.1.z Without TLS protection between NF and SEPP and with TLS security with the 3gpp-Sbi-Target-apiRoot header used over N32f



Figure C.2.1.z-1: End to end call flow when http scheme URI is used and TLS security with the 3gpp-Sbi-Target-apiRoot header used is used between SEPPs

1. Same as step 1 of Figure C.2.1.2-1.

2. Same as step 3 of Figure C.2.1.2-1

3. Same as step 4 of Figure C.2.1.2-1

4. The c-SEPP setups a TLS connection with the authoritative server for the p-SEPP FQDN (in the apiRoot of the Request URI) and verifies that the certificate presented by the endpoint of the TLS connection belongs to the authoritative server of the p-SEPP. The c-SEPP is configured with the p-SEPP FQDN.

5. The c-SEPP sets the apiRoot in the request URI with the apiRoot of the p-SEPP, inserts the 3gpp-Sbi-Target-apiRoot header set to the apiRoot of the p-NRF, and sends the request towards p-SEPP.

6. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the apiRoot of the p-SEPP FQDN in the request URI with the apiRoot of the p-NRF received in the 3gpp-Sbi-Target-apiRoot header, and then seeing that the URI scheme of the NF discovery service of the p-NRF is "http", the p-SEPP forwards the NF discovery request to the p-NRF.

7 to 11. Same as steps 7 to 11 of Figure C.2.1.2-1.

12. The c-SEPP sets the apiRoot of the p-SEPP FQDN in the request URI, inserts the 3gpp-Sbi-Target-apiRoot header set to the apiRoot of the p-NF, and sends the request towards p-SEPP.

13. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the apiRoot of the p-SEPP FQDN in the request URI with the apiRoot of the p-NF received in the 3gpp-Sbi-Target-apiRoot header and then seeing that the URI scheme of the NF service producer is "http", the p-SEPP forwards the request to the p-NF.

13 to 16. Same as steps 13 to 16 of Figure C.2.1.2-1.

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

#### C.2.2.2 With TLS protection between NF and SEPP relying on telescopic FQDN, and TLS security without the 3gpp-Sbi-Target-apiRoot header used over N32f



Figure C.2.2.2-1: End to end call flow when https scheme URI is used, telescopic FQDNs are used between NF and SEPP and TLS security without the 3gpp-Sbi-Target-apiRoot header is used between SEPPs

1. The SEPP on the NF service consumer side (c-SEPP) and the SEPP on the NF service producer side (p-SEPP) negotiate the security capabilities using the procedure specified in clause 5.2.2. The SEPPs mutually negotiate to use TLS as the security policy.

2. A TLS connection is setup between the c-SEPP and the p-SEPP for N32-f forwarding.

3. Before the NF service consumer starts using the API of the NF service producer it needs to discover the NF service profile of the producer by querying the NRF. The NF service consumer uses "https" scheme URI to access the Nnrf\_NFDiscovery service. This implies that the NF service consumer sets up a TLS connection to the c-NRF and then sends the HTTP request over the TLS connection to the c-NRF.

4. The NRF on the NF service consumer side (c-NRF) needs to further initiate a discovery request to the NRF on the NF service producer side (p-NRF). The c-NRF uses "https" scheme URI to access the NF discovery service of the p-NRF. Since "https" requires setup of TLS connection with the p-NRF and it requires that c-NRF has to verify that the certificate presented by the endpoint of the TLS connection belongs to the authoritative server of the p-NRF, a telescopic FQDN with wildcarded certificate scheme mechanism is specified in 3GPP TS 33.501 [6]. The c-NRF is configured with the telescopic FQDN of the p-NRF with the telescopic FQDN having the FQDN of the c-SEPP as the trailing part. The c-NRF sets up a TLS connection with the authoritative server for the telescopic FQDN (i.e. the c-SEPP).

5. The c-NRF forwards the NF discovery request in this TLS connection.

6. The c-SEPP extracts the NF discovery request from the TLS connection, replaces the label part of the telescopic FQDN in the request URI with a corresponding label of the p-SEPP (if the label part of the telescopic FQDN contains a label of c-SEPP's local significance) and sends the request towards p-SEPP in the TLS tunnel setup in step 2. The c-SEPP and the p-SEPP act as a man in the middle proxy in this case.

7. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the label part of the the telescopic FQDN in the request URI to the URI of the p-NRF's NF discovery service and then seeing that the URI scheme of the NF discovery service of the p-NRF is "https", the p-SEPP sets up a TLS connection with the p-NRF.

8. The p-SEPP forwards the NF discovery request to the p-NRF.

9. The p-NRF sends the NF discovery response within the TLS connection. The NF service profile contains service URI with "https" scheme. The FQDN of the NF service is an inter PLMN FQDN.

10. The p-SEPP forwards the NF discovery response within TLS tunnel setup in step 2 to the c-SEPP. The p-SEPP may replace the inter PLMN FQDN of the NF service producer's API endpoint with a label representing that FQDN. The p-SEPP re-maps the label with the NF service producer's API endpoint in step 17.

11. The c-SEPP upon receiving the HTTP response message for NF discovery response, within the TLS tunnel in step 2, replaces the trailing part of the inter PLMN FQDN of the NF service producer's API endpoint in the NF service profile with the FQDN of the c-SEPP, to form a telescopic FQDN as specified in clause 28.5.2 of 3GPP TS 23.003 [19]. The c-SEPP may replace the label part of the telescopic FQDN with a label of it's own significance. The p-SEPP re-maps the label in step 16.

12. The c-SEPP then forwards the NF discovery response to c-NRF, with the NF service profile containing the telescopic FQDN.

13. The c-NRF sends the NF discovery response to NF service consumer.

14. The NF service profile received at the NF service consumer contains service URI with "https" scheme. The NF service consumer sets up a TLS connection with the authoritative server for the telescopic FQDN (i.e. c-SEPP) received in step 13.

15. The NF service consumer sends the HTTP service request within the TLS connection to the c-SEPP.

16. The c-SEPP extracts the HTTP request from the TLS connection, replaces the label part of the telescopic FQDN in the request URI with a corresponding label of the p-SEPP and sends the request towards p-SEPP in the TLS tunnel setup in step 2. The c-SEPP and the p-SEPP act as a man in the middle proxy in this case.

17. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the label part of the the telescopic FQDN in the request URI to the URI of the NF service producer and then seeing that the URI scheme of the NF service producer is "https", the p-SEPP sets up a TLS connection with the NF service producer. The p-SEPP also replaces callback URI and link relations within the extracted HTTP message with a telescopic FQDN containing the FQDN of the p-SEPP as the trailing part, as specified in clause 6.1.4.3 of 3GPP TS 29.500 [4].

18. The p-SEPP forwards the HTTP request to the NF service producer.

19. The NF service producer sends the HTTP response within the TLS connection.

20. The p-SEPP forwards the HTTP response within TLS tunnel setup in step 2 to the c-SEPP.

21. The c-SEPP upon receiving the HTTP response message within the TLS tunnel setup in step 2, forwards the response to the NF service consumer. The c-SEPP replaces callback URI and link relations within the extracted HTTP response message with a telescopic FQDN containing the FQDN of the c-SEPP as the trailing part, as specified in clause 6.1.4.3 of 3GPP TS 29.500 [4].

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

#### C.2.2.3 With TLS protection between NF and SEPP relying on 3gpp-Sbi-Target-apiRoot header, and TLS security without the 3gpp-Sbi-Target-apiRoot header used over N32f



Figure C.2.2.3-1: End to end call flow when https scheme URI is used, 3gpp-Sbi-Target-apiRoot header is used between NF and SEPP and TLS security without the 3gpp-Sbi-Target-apiRoot header is used between SEPPs

1. Same as step 1 of Figure C.2.2.2-1.

2. Same as step 2 of Figure C.2.2.2-1.

3. Same as step 3 of Figure C.2.2.2-1

4. The NRF on the NF service consumer side (c-NRF) needs to further initiate a discovery request to the NRF on the NF service producer side (p-NRF). The c-NRF uses "https" scheme URI to access the NF discovery service of the p-NRF. The c-NRF setups a TLS connection with the authoritative server for the SEPP FQDN (in the apiRoot of the Request URI) and verifies that the certificate presented by the endpoint of the TLS connection belongs to the authoritative server of the c-SEPP. The c-NRF is configured with the c-SEPP FQDN.

5. The c-NRF forwards the NF discovery request in this TLS connection, including an 3gpp-Sbi-Target-apiRoot header set to the apiRoot of the p-NRF.

6. The c-SEPP extracts the NF discovery request from the TLS connection, replaces the apiRoot of the SEPP FQDN in the request URI with the apiRoot of the p-NRF received in the 3gpp-Sbi-Target-apiRoot header and sends the request towards p-SEPP in the TLS tunnel setup in step 2. The c-SEPP and the p-SEPP act as a man in the middle proxy in this case.

7. The p-SEPP extracts the HTTP message received on the TLS connection, and then seeing that the URI scheme of the NF discovery service of the p-NRF is "https", the p-SEPP sets up a TLS connection with the p-NRF.

8. Same as step 8 of Figure C.2.2.2-1

9. Same as step 9 of Figure C.2.2.2-1

10. Same as step 10 of Figure C.2.2.2-1

11, 12. The c-SEPP forwards the NF discovery response to c-NRF.

13. Same as step 13 of Figure C.2.2.2-1

14. The NF service profile received at the NF service consumer contains service URI with "https" scheme. Since the URI of the p-NF contains an authority of a remote PLMN, the NF service consumer sets up a TLS connection with the authoritative server for the SEPP FQDN (i.e. c-SEPP). The c-NF is configured with the c-SEPP FQDN.

15. The NF service consumer sends the HTTP service request within the TLS connection to the c-SEPP, including a 3pp-Sbi-Target-apiRoot header set to the apiRoot of the p-NF.

16. The c-SEPP extracts the HTTP request from the TLS connection, replaces the apiRoot of the SEPP FQDN in the request URI with the apiRoot of the p-NRF received in the 3gpp-Sbi-Target-apiRoot header and sends the request towards p-SEPP in the TLS tunnel setup in step 2. The c-SEPP and the p-SEPP act as a man in the middle proxy in this case.

17. The p-SEPP extracts the HTTP message received on the TLS connection and then seeing that the URI scheme of the NF service producer is "https", the p-SEPP sets up a TLS connection with the NF service producer.

18. Same as step 18 of Figure C.2.2.2-1

19. Same as step 19 of Figure C.2.2.2-1

20. Same as step 20 of Figure C.2.2.2-1

21. The c-SEPP upon receiving the HTTP response message within the TLS tunnel setup in step 2, forwards the response to the NF service consumer.

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

#### C.2.2.x With TLS protection between NF and SEPP relying on telescopic FQDN, and TLS security with the 3gpp-Sbi-Target-apiRoot header used over N32f



Figure C.2.2.x-1: End to end call flow when https scheme URI is used, telescopic FQDNs are used between NF and SEPP and TLS security with the 3gpp-Sbi-Target-apiRoot header is used between SEPPs

1. Same as step 1 of Figure C.2.2.2-1.

2. Same as step 3 of Figure C.2.2.2-1.

3. Same as step 4 of Figure C.2.2.2-1.

4. Same as step 5 of Figure C.2.2.2-1

5. The c-SEPP setups a TLS connection with the authoritative server for the p-SEPP FQDN (in the apiRoot of the Request URI) and verifies that the certificate presented by the endpoint of the TLS connection belongs to the authoritative server of the p-SEPP. The c-SEPP is configured with the p-SEPP FQDN.

6. The c-SEPP sets the apiRoot in the request URI with the apiRoot of the p-SEPP, inserts the 3gpp-Sbi-Target-apiRoot header set to the apiRoot of the p-NRF derived from the telescopic FQDN received in step 4, and sends the request towards p-SEPP.

7. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the apiRoot of the p-SEPP FQDN in the request URI with the apiRoot of the p-NRF received in the 3gpp-Sbi-Target-apiRoot header, and then seeing that the URI scheme of the NF discovery service of the p-NRF is "https", the p-SEPP sets up a TLS connection with the p-NRF.

8 to 15. Same as steps 8 to 15 of Figure C.2.2.3-1.

16. The c-SEPP extracts the HTTP request from the TLS connection, sets the apiRoot of the p-SEPP FQDN in the request URI, inserts the 3gpp-Sbi-Target-apiRoot header set to the apiRoot of the p-NF derived from the telescopic FQDN received in step 15, and sends the request towards p-SEPP.

17. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the apiRoot of the p-SEPP FQDN in the request URI with the apiRoot of the p-NF received in the 3gpp-Sbi-Target-apiRoot header and then seeing that the URI scheme of the NF service producer is "https", the p-SEPP sets up a TLS connection with the NF service producer.

18 to 21. Same as steps 18 to 21 of Figure C.2.2.2-1

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

#### C.2.2.y With TLS protection between NF and SEPP relying on 3gpp-Sbi-Target-apiRoot header, and TLS security with the 3gpp-Sbi-Target-apiRoot header used over N32f



Figure C.2.2.y-1: End to end call flow when https scheme URI is used, 3gpp-Sbi-Target-apiRoot header is used between NF and SEPP and TLS security with the 3gpp-Sbi-Target-apiRoot header is used between SEPPs

1. Same as step 1 of Figure C.2.2.3-1.

2. Same as step 3 of Figure C.2.2.3-1

3. Same as step 4 of Figure C.2.2.3-1

4. Same as step 5 of Figure C.2.2.3-1.

5. The c-SEPP setups a TLS connection with the authoritative server for the p-SEPP FQDN (in the apiRoot of the Request URI) and verifies that the certificate presented by the endpoint of the TLS connection belongs to the authoritative server of the p-SEPP. The c-SEPP is configured with the p-SEPP FQDN.

6. The c-SEPP sets the apiRoot in the request URI with the apiRoot of the p-SEPP and sends the request towards p-SEPP including the 3gpp-Sbi-Target-apiRoot header received in step 4.

7. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the apiRoot of the p-SEPP FQDN in the request URI with the apiRoot of the p-NRF received in the 3gpp-Sbi-Target-apiRoot header, and then seeing that the URI scheme of the NF discovery service of the p-NRF is "https", the p-SEPP sets up a TLS connection with the p-NRF.

8 to 15. Same as steps 8 to 15 of Figure C.2.2.3-1.

16. The c-SEPP extracts the HTTP request from the TLS connection, replaces the apiRoot of the c-SEPP FQDN in the request URI with the apiRoot of the p-SEPP, and sends the request towards p-SEPP including the 3gpp-Sbi-Target-apiRoot header received in step 15.

17. The p-SEPP extracts the HTTP message received on the TLS connection, replaces the apiRoot of the p-SEPP FQDN in the request URI with the apiRoot of the p-NF received in the 3gpp-Sbi-Target-apiRoot header and then seeing that the URI scheme of the NF service producer is "https", the p-SEPP sets up a TLS connection with the NF service producer.

18 to 21. Same as steps 18 to 21 of Figure C.2.2.2-1

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

## A.2 N32 Handshake API

openapi: 3.0.0

info:

 version: '1.1.0'

 title: 'N32 Handshake API'

 description: |

 N32-c Handshake Service.

 © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

 All rights reserved.

[…]

 SecNegotiateReqData:

 type: object

 required:

 - sender

 - supportedSecCapabilityList

 properties:

 sender:

 $ref: 'TS29510\_Nnrf\_NFManagement.yaml#/components/schemas/Fqdn'

 supportedSecCapabilityList:

 type: array

 items:

 $ref: '#/components/schemas/SecurityCapability'

 minItems: 1

 3GppSbiTargetApiRootSupported:

 type: boolean

 default: false

 SecNegotiateRspData:

 type: object

 required:

 - sender

 - selectedSecCapability

 properties:

 sender:

 $ref: 'TS29510\_Nnrf\_NFManagement.yaml#/components/schemas/Fqdn'

 selectedSecCapability:

 $ref: '#/components/schemas/SecurityCapability'

 3GppSbiTargetApiRootSupported:

 type: boolean

 default: false

[…]

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