**3GPP TSG-CT WG4 Meeting #125C4-244331**

**Hefei, P.R. China; 14th – 18th October 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.573** | **CR** | **0216** | **rev** | **1** | **Current version:** | **19.0.0** |  |
|  |
| *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:***  | Autonomous correlation of N32-c and N32-f |
|  |  |
| ***Source to WG:*** | NTT DOCOMO, Nokia, Ericsson, China Mobile |
| ***Source to TSG:*** | CT4 |
|  |  |
| ***Work item code:*** | SBIProtoc18 |  | ***Date:*** | 2024-10-04 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | This CR addresses issue on correlation of N32-c and N32-f when the initial N32-f message does not appear for quite some time which could lead to unverfied TLS session for N32-f for quite some time.---In order to correlate TLS sessions for N32-c and N32-f between a pair of SEPPs especially when multiple N32 Purposes are used, “N32 Handshake ID” was introduced to cover these aspects. N32Purpose can also be used for such correlation.However, in order for SEPP to be able to correlate the TLS sessions for N32-c and N32-f, initial message over N32-f is required. But such message over N32-f may not be sent for quite some time, as it is out of control from SEPP, and SEPP will not be able to correlate or verify the TLS session for N32-f for some time.To avoid such issue, it is proposed to have the initiating SEPP send an HTTP OPTIONS request to responding SEPP over N32-f, so that responding SEPP will be able to receive the value of “N32 Handshake ID” within the controlled time by SEPPs. |
|  |  |
| ***Summary of change:*** | * Define procedures so that HTTP OPTIONS request/response over N32-f which allows correlation of N32-c and N32-f to be made immediately after N32-c Security Capability Negotiation.
* Add a new feature for supported features to allow this autonomous N32-c and N32-f correlation
 |
|  |  |
| ***Consequences if not approved:*** | SEPPs is not be able to autonomously correlate TLS sessions for N32-c and N32-f on their own if the initiating SEPP does not immediately send HTTP Service request message after establishing the TLS connection for N32-f. |
|  |  |
| ***Clauses affected:*** | 5.3.3.2.X (modified to new subclause), 5.3.3.2.Y (new), 6.1.7 |
|  |  |
|  | **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 does not introduce or modify any OpenAPI. |
|  |  |
| ***This CR's revision history:*** | Rev1: Aspects related to keepalive are deleted. Updates are made on the newly added note to be normative part of text. |

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

#### 5.3.3.2 Correlation of N32-c context and N32-f Connection for TLS Security

##### 5.3.3.2.X General

This clause addresses the correlation between a N32-f connection and its parent N32-c context when the negotiated security mode is TLS. When TLS Security is used, the correlation between a N32-f connection to its parent N32-c context shall be identified with following mechanism:

- When there is only one N32-c context successfully negotiated between a pair of SEPPs, one SEPP shall correlate a N32-f connection to its N32-c context by matching the peer SEPP's identifier (i.e. the FQDN of the peer SEPP) in the received TLS certificate with the FQDN(s) of the peer SEPP in the corresponding N32-c context (i.e. the FQDNs carried in the "sender" IE and/or the "senderN32fFqdn" IE); or

NOTE: If the received certificate contains FQDNs for different SEPPs (e.g. one common certificate used for all the SEPPs in the whole network), one SEPP can use the peer SEPP FQDN in the Via header (see clause 6.10.10.3 of 3GPP TS 29.500 [4]) of the incoming N32-f HTTP message to perform the matching with the FQDN in the corresponding N32-c context.

- When multiple N32-c contexts were successfully negotiated between a pair of SEPPs, then

- if the N32 Handshake Ids were exchanged during the N32-c negotiation, one SEPP shall correlate the N32-f connection to its parent N32-c context by matching the N32 Handshake Id in the incoming N32-f HTTP messages (carried in the "3gpp-Sbi-N32-Handshake-Id" header) with the received N32 Handshake Id (carried in the "n32HandshakeId" IE) in corresponding N32-c context; or

- if the N32 Handshake Ids were not successfully exchanged during the N32-c negotiation (i.e. if at least one SEPP did not signal its N32 Handshake Id during the Security Capability Negotiation Procedure) and if different N32 purposes were successfully negotiated for N32-c contexts, one SEPP shall correlate the N32-f connection to its parent N32-c context by matching the N32 purpose of the incoming N32-f HTTP messages (as stated in the "3gpp-Sbi-Interplmn-Purpose" HTTP header if present or as "ROAMING" if the "3gpp-Sbi-Interplmn-Purpose" HTTP header is not present, see clause 6.14 of 3GPP TS 29.500 [4]) with the supported N32 purpose(s) in the corresponding N32-c context.

##### 5.3.3.2.Y Use of HTTP OPTIONS for N32-c and N32-f connections correlation

When multiple N32-c contexts were successfully negotiated between a pair of SEPPs and if the initiating SEPP does not send any HTTP service request message to the responding SEPP after establishing TLS session for the N32-f connection and both SEPPs indicated the support of the feature TLSCOR, i.e. support of autonomous correlation of N32-c and N32-f, the initiating SEPP shall send a HTTP OPTIONS request towards the Authority of the responding SEPP over the established TLS session for N32-f to correlate TLS sessions established for N32-c and N32-f, immediately after each N32-f TLS connection is established, as shown in Figure 5.3.3.2.Y-1.

The HTTP OPTIONS request shall include "3gpp-Sbi-N32-Handshake-Id" header and "3gpp-Sbi-Interplmn-Purpose" header along with the corresponding values as same as all other messages sent over N32-f. This HTTP OPTIONS request will avoid pending TLS session waiting for long duration before the first N32-f message is sent when the correlation can be done for the first time.



Figure 5.3.3.2.Y-1: Use of HTTP OPTIONS for N32-c and N32-f connections correlation

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

### 6.1.7 Feature Negotiation

The feature negotiation mechanism specified in clause 6.6 of 3GPP TS 29.500 [4] shall be used to negotiate the features applicable between the c-SEPP and the p-SEPP, for the N32 Handshake service, if any.

The c-SEPP shall indicate the features it supports for the N32 Handshake service, if any, by including the supportedFeatures attribute in the HTTP POST request message for following service operations:

- Security Capability Negotiation procedure, as specified in clause 5.2.2 to negotiate the security capability;

The p-SEPP shall determine the supported features for the requested network as specified in clause 6.6 of 3GPP TS 29.500 [4] and shall indicate the supported features by including the supportedFeatures attribute in content of the HTTP response for the service operation.

The syntax of the supportedFeatures attribute is defined in clause 5.2.2 of 3GPP TS 29.571 [12].

The following features are defined for the N32 Handshake service.

Table 6.1.7-1: Features of supportedFeatures attribute used by N32 Handshake service

|  |  |  |  |
| --- | --- | --- | --- |
| Feature Number | Feature | M/O | Description |
| 1 | NFTLST | O | N32-f TLS Connection Termination SupportA SEPP that supports this feature shall support handling of Security Capability Negotiation procedure to tear down the N32-f TLS connection as specified in clause 5.2.2). |
| 2 | PSEPRO | O | PRINS Security Profiles SupportA SEPP that supports this feature shall support the negotiation of security profiles as specified in clause 5.2.3.3. |
| 3 | PSIU | M | Protection of Sensitive Information in URI (Path and Query Parameters)A SEPP that complies with this release of the specification shall support this feature, i.e. the protection of sensitive information in URI path and query parameters in HTTP messages to be forwarded. |
| 4 | SNDN32F | O | Support of N32-f FQDN and N32-f Port.A SEPP that supports this feature: - may signal an N32-f FQDN and Port within the Security Capability Negotiation towards the remote SEPP; - shall support receiving a N32-f FQDN and Port(s) within the Security Capability Negotiation from the remote SEPP- shall support forwarding the N32-f traffic towards the N32-f FQDN and Port received from the peer SEPP. |
| X | TLSCOR | O | Correlation of TLS for N32-c and N32-fA SEPP that supports this feature:- shall correlate the context of N32-c and N32-f at time of N32 connection establishment, using procedures as specified in clause 5.3.3.2.Y if the initiating SEPP does not send any pending HTTP service request message to the responding SEPP immediately after establishing the TLS session for the N32-f connection. This enables N32-c and N32-f correlation in case there is not any N32-f messages sent by the initiating SEPP. |
| Feature number: The order number of the feature within the supportedFeatures attribute (starting with 1).Feature: A short name that can be used to refer to the bit and to the feature.M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O").Description: A clear textual description of the feature. |

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