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

**E-Meeting, 18th – 28th August 2020** *Revision of C4-204186*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.500** | **CR** | **0150** | **rev** | **1** | **Current version:** | **16.4.0** |  |
|  | | | | | | | | |
| *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:*** | 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 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 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.*  TS 29.500 needs to be aligned to reflect that the the 3gpp-Sbi-Target-apiRoot header may be used with TLS security over N32f. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The 3gpp-Sbi-Target-apiRoot header may be used between SEPPs to indicate the apiRoot of the target NF in another PLMN, when TLS security with the 3gpp-Sbi-Target-apiRoot header is used between the SEPPs.  Routing requirements between SEPPs are clarified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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:*** | | 5.2.3.2.1, 5.2.3.2.4, 6.1.4.3.2, 6.1.4.3.3, 6.1.4.3.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Rev. 1: Changes proposed in clause 5.3.3 of C4-204185 are moved in clause 6.1.4.3.4 of this CR. Routing requirements between SEPPs are clarified. | | | | | | | | |

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

##### 5.2.3.2.1 General

The 3GPP NF Services shall support the HTTP custom headers specified in Table 5.2.3.2.1-1 below. A description of each custom header and the normative requirements on when to include them are also provided in Table 5.2.3.2-1.

Table 5.2.3.2.1-1: Mandatory HTTP custom headers

|  |  |  |
| --- | --- | --- |
| Name | Reference | Description |
| 3gpp-Sbi-Message-Priority | Clause 5.2.3.2.2 | This header is used to specify the HTTP/2 message priority for 3GPP service based interfaces. This header shall be included in HTTP/2 messages when a priority for the message needs to be conveyed (e.g HTTP/2 messages related to Multimedia Priority Sessions). |
| 3gpp-Sbi-Callback | Clause 5.2.3.2.3 | This header is used to indicate if a HTTP/2 message is a callback (e.g notification).  This header shall be included in HTTP POST messages for callbacks towards NF service consumer(s) in another PLMN via the SEPP (See 3GPP TS 29.573 [27]).  This header shall also be included in HTTP POST messages for callbacks in indirect communication (See clause 6.10.7). |
| 3gpp-Sbi-Target-apiRoot | Clause 5.2.3.2.4 | This header is used by an HTTP client to indicate the apiRoot of the target URI when communicating indirectly with the HTTP server via an SCP.  This header may also be used by an HTTP client towards its local SEPP to indicate the apiRoot of the target URI towards HTTP server in another PLMN.  This header may also be used between SEPPs to indicate the apiRoot of the target URI towards HTTP server in another PLMN, when TLS security with the 3gpp-Sbi-Target-apiRoot header is used between the SEPPs. |
| 3gpp-Sbi-Routing-Binding | Clause 5.2.3.2.5 | This header is used in a service request to signal binding information to direct the service request to an HTTP server which has the targeted NF Service Resource context (see clause 6.12). |
| 3gpp-Sbi-Binding | Clause 5.2.3.2.6 | This header is used to signal binding information related to an NF Service Resource to a future consumer (HTTP client) of that resource (see clause 6.12). |
| 3gpp-Sbi-Discovery-\* | Clause 5.2.3.2.7 | Headers beginning with the prefix 3gpp-Sbi-Discovery- are used in indirect communication mode for discovery and selection of a suitable producer by the SCP. Such headers may be included in any SBI message and include information allowing an SCP to find a suitable producer as per the consumer's included delegated discovery parameters. |
| 3gpp-Sbi-Producer-Id | Clause 5.2.3.2.8 | This header is used in a service response from the SCP to the NF Service Consumer, when using indirect communication with delegated discovery and the NF Service Producer does not return a binding indication in a service response creating a resource. See clause 6.10.3.4. |
| 3gpp-Sbi-Oci | Clause 5.2.3.2.9 | This header may be used by an overloaded NF Service Producer in a service response, or in a notification request to signal Overload Control Information (OCI) to the NF Service Consumer.  This header may also be used by an overloaded NF Service Consumer in a notification response or in a service request to signal Overload Control Information (OCI) to the NF Service Producer. |
| 3gpp-Sbi-Lci | Clause 5.2.3.2.10 | This header may be used by a NF Service Producer to send Load Control Information (LCI) to the NF Service Consumer. |
| 3gpp-Sbi-Client-Credentials | Clause 5.2.3.2.11 | This header may be used by an NF Service Consumer to send Client Credentials Assertion to the NRF or to the NF Service Producer. See clause 6.7.5. |

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

##### 5.2.3.2.4 3gpp-Sbi-Target-apiRoot

The header contains the apiRoot of the target URI (see clause 4.4 of 3GPP TS 29.501 [5]) in a request sent to an SCP when using Indirect Communication. It may also be used in a request sent to a SEPP and in a request between SEPPs (see clause 6.1.4.3.2).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

3gpp-Sbi-Target-apiRoot header field = "3gpp-Sbi-Target-apiRoot" ":" OWS scheme "://" authority [ prefix ]

scheme = "http" / "https"

authority = host [ ":" port ]

port = \*DIGIT

prefix = path-absolute ; path-absolute production rule from IETF RFC 3986 [14], clause 3.3

An example is: 3gpp-Sbi-Target-apiRoot: <https://example.com/a/b/c>

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

##### 6.1.4.3.2 Use of telescopic FQDN between NFs and SEPP within a PLMN

When using TLS wildcard certificate and telescopic FQDN between the SEPP and NFs within the SEPP's PLMN, the SEPP on the HTTP/2 client side shall form the telescopic FQDN, as specified in 3GPP TS 23.003 [15], for the following cases:

- FQDN of the target NF service in HPLMN is modified into a telescopic FQDN by the SEPP in the VPLMN;

- FQDN of the target NF service in VPLMN is modified into a telescopic FQDN by the SEPP in the HPLMN;

- FQDN (authority) part of callback URI of NF service resources in VPLMN is modified into a telescopic FQDN by the SEPP in the HPLMN;

- FQDN (authority) part of callback URI of NF service resources in HPLMN is modified into a telescopic FQDN by the SEPP in the VPLMN;

- FQDN (authority) part of link relation URI of NF service resources in VPLMN is modified into a telescopic FQDN by the SEPP in the HPLMN;

- FQDN (authority) part of link relation URI of NF service resources in HPLMN is modified into a telescopic FQDN by the SEPP in the VPLMN.

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

##### 6.1.4.3.3 Use of 3gpp-Sbi-Target-apiRoot between NFs and SEPP within a PLMN

When using the 3gpp-Sbi-Target-apiRoot header between the SEPP and NFs within the SEPP's PLMN, HTTP requests between the NFs and the SEPP shall be routed as specified in clause 6.10.2 for indirect communications, with the SEPP taking the role of the SCP.

When sending an HTTP request targeting a URI with an authority of a remote PLMN, NFs shall include the 3gpp-Sbi-Target-apiRoot header in the HTTP request, containing the apiRoot of the target URI in the remote PLMN, and shall set the apiRoot in the request URI to the apiRoot of the SEPP (or to the apiRoot of the SCP if the communication between the NF and SEPP goes through an SCP). The apiRoot of the SEPP (or SCP) may include an optional deployment-specific string of the SEPP (or SCP).

An SCP that receives an HTTP request targeting a URI with an authority of a remote PLMN shall route the HTTP request towards the SEPP as specified in clause 6.10.2 for indirect communications, i.e. the SCP shall forward the 3gpp-Sbi-Target-apiRoot header in the HTTP request it forwards to the SEPP, containing the apiRoot of the target URI in the remote PLMN, and it shall set the apiRoot in the request URI to the apiRoot of the SEPP.

If the SEPP receives an HTTP request from a NF with a request URI containing a telescopic FQDN and with a 3gpp-Sbi-Target-apiRoot header, the SEPP shall ignore the 3gpp-Sbi-Target-apiRoot header and route the request using the telescopic FQDN.

NOTE 1: This is to address the case of a potentially malicious or misbehaving NF that would include the 3gpp-Sbi-Target-apiRoot header and a request URI containing a telescopic FQDN when communicating with the SEPP.

NOTE 2: This solution does not require the SEPP to support TLS wildcard certificate for its domain name, nor the SEPP to modify URI attributes in HTTP request and response payloads with telescopic FQDNs.

NOTE 3: The communication between the NF and SEPP can be direct or go through an SCP.

##### 6.1.4.3.4 Routing between SEPPs

The 3gpp-Sbi-Target-apiRoot header shall not be used between SEPPs if PRINS security is negotiated between the SEPPs. The apiRoot of the Request URI of the HTTP request encapsulating the protected message shall be set to the apiRoot of the remote SEPP. See clause 5.3.2.4 of 3GPP TS 29.573 [27].

If TLS security is negotiated between the SEPPs and at least one SEPP does not indicate support of the 3gpp-Sbi-Target-apiRoot header when negotiating the security policy, the SEPP shall use a pre-established TLS connection towards the other SEPP to forward the HTTP/2 messages sent by the NF service producers and NF service consumers, as is without reformatting. Additionally,

- if the NF uses the 3gpp-Sbi-Target-apiRoot HTTP header in the HTTP Request to convey the target apiRoot to the sending SEPP, the sending SEPP shall remove the 3gpp-Sbi-Target-apiRoot header and set the apiRoot of the request URI it forwards on the N32-f interface to the apiRoot received in the 3gpp-Sbi-Target-apiRoot header from the HTTP client;

- if the NF uses a telescopic FQDN in the HTTP Request to convey the target apiRoot to the sending SEPP, or if TLS is not used between the NF and the sending SEPP, the sending SEPP shall set the apiRoot of the Request URI in the HTTP Request towards the remote SEPP to the apiRoot of the target NF derived from the telescopic FQDN or from the request URI respectively.

If TLS security is negotiated between the SEPPs and both SEPPs indicate support of the 3gpp-Sbi-Target-apiRoot header when negotiating the security policy, HTTPS shall be used to forward messages between SEPPs. The sending SEPP shall replace the apiRoot of the Request URI in the HTTP Request with the apiRoot of the receiving SEPP before forwarding the HTTP Request on the N32 interface. Additionally,

- if the NF uses the 3gpp-Sbi-Target-apiRoot HTTP header in the HTTP Request to convey the target apiRoot to the sending SEPP, the sending SEPP shall forward the 3gpp-Sbi-Target-apiRoot header unmodified in the HTTP request towards the remote SEPP;

- if the NF uses a telescopic FQDN in the HTTP Request to convey the target apiRoot to the sending SEPP, or if TLS is not used between the NF and the sending SEPP, the sending SEPP shall insert the 3gpp-Sbi-Target-apiRoot header in the HTTP request towards the remote SEPP and set it to the apiRoot of the target NF derived from the telescopic FQDN or from the request URI respectively.

NOTE: Rel-15 compliant NFs and SEPP do not support the 3gpp-Sbi-Target-apiRoot header.

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