**3GPP TSG-SA3 Meeting #101-e *S3-203548***

**e-meeting, 9th - 20th November 2020 *revision of S3-20xxxx***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.517** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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:*** | Living CR to 33.517 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon ,Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 30-10-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | In order to address the threat analysed in S3-203118, there is the requirement defined in TS 29.500 clause 6.1.4.3.3 “*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*”.  This requirement needs to be captured for a new test case to be defined in TS 33.517 for security assurance against the threat analysed in S3-203118.  Therefore, it is proposed to add the requirement from TS 29.500 and a corresponding new test case in TS 33.517 R17.  In order to address the threat analysed in S3-203140, there is the requirement defined in TS 29.500 clause 6.1.4.3.4 “*The 3gpp-Sbi-Target-apiRoot header shall not be used between SEPPs if PRINS security is negotiated between the SEPPs*”.  This requirement needs to be captured with a new test case to be defined in TS 33.517 for security assurance against the threat analysed in S3-203140.  Therefore, it is proposed to add the requirement from TS 29.500 and a corresponding new test case in TS 33.517 R17. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added a new clause for the requirement and test case on the SEPP product for correct inter-PLMN routing.  Added a new clause for the requirement and test case on the SEPP product for correct handling of the 3gpp-Sbi-Target-apiRoot header if PRINS security is used between the SEPPs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No test case for security assurance of correct handling of inter-PLMN routing.  No test case for security assurance of correct handling of the custom HTTP header if PRINS is used between the SEPPs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | clause 2, new clause 4.2.2.x, new clause 4.2.2.y | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.117: "Catalogue of General Security Assurance Requirements".

[3] 3GPP TS 33.501 (Release 15): "Security architecture and procedures for 5G system".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] Void.

[xx] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture" (Release 16)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.x Correct Handling of Inter-PLMN Routing

*Requirement Name*: Correct Handling of Inter-PLMN Routing

*Requirement Reference:* TS 29.500 [xx], clause 6.1.4.3.3

*Requirement Description*:

"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".

*Threat References*: TR 33.926 [4], clause G.2.x.a, Inter-PLMN routing using the incorrect reference

*Test Case*:

**Test Name:** TC\_CORRECT\_INTER\_PLMN\_ROUTING

**Purpose:**

Verify that the SEPP under test correctly route the NF request to a remote PLMN when receving both a 3gpp-Sbi-Target-apiRoot header and a telescopic FQDN contained in the Request URI in the HTTP request from a NF.

**Procedure and execution steps:**

**Pre-Conditions:**

- System documentation of the SEPP under test, which details the methods supported for TLS protection between the NF and the SEPP and how internal log files can be accessed.

- A peer SEPP instance of a remote PLMN for N32 communication with the SEPP under test, which may be simulated.

- A NF for sending HTTP request to the remote PLMN of the peer SEPP via the SEPP under test, which may be simulated and supports both telescopic FQDN and the custom 3gpp-Sbi-Target-apiRoot header. The NF is configured with:

- The NF service profile containing service URI with "https" scheme and an authority of the remote PLMN for communication with the NF producer in the remote PLMN.

- The telescopic FQDN of the NF producer in the remote PLMN, having the FQDN of the SEPP under test as the trailing part.

- The FQDN of the SEPP under test.

- The SEPP under test is configured with:

- The FQDN of the peer SEPP in the remote PLMN.

- The security mechanism negotiated with the peer SEPP in the remote PLMN.

**Execution Steps**

1) The NF sets up a TLS connection with the authoritative server for the configured telescopic FQDN, i.e. the SEPP under test.

2) The NF sends a HTTP service request with the request URI containing the configured telescopic FQDN within the TLS connection to the SEPP under test, before which the tester inserts in the HTTP request a 3gpp-Sbi-Target-apiRoot header set to the apiRoot of a NF producer in another PLMN different from the remote PLMN.

3) The NF sends a HTTP service request within the TLS connection to the SEPP under test, before which the tester inserts in the HTTP request a 3gpp-Sbi-Target-apiRoot header set to the apiRoot of the NF producer in the remote PLMN and changes the telescopic FQDN in request URI to be different from the configured one.

**Expected Results:**

After step 2), the peer SEPP received the HTTP request from the NF through the SEPP under test.

After step 3), the peer SEPP did not receive the HTTP request from the NF through the SEPP under test

**Expected format of evidence:**

Evidence suitable for the interface, e.g. screenshot containing the operational results.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.y Correct Handling of Custom HTTP Header with PRINS Security

*Requirement Name*: Correct Handling of the Custom HTTP Header with PRINS Security

*Requirement Reference:* TS 29.500 [xx], clause 6.1.4.3.4

*Requirement Description*:

"The 3gpp-Sbi-Target-apiRoot header shall not be used between SEPPs if PRINS security is negotiated between the SEPPs".

*Threat References*: TR 33.926 [4], clause G.2.x.b, Tampering of target API root

*Test Case*:

**Test Name:** TC\_HANDLING\_CUSTOM\_HTTPHEADER\_WITH\_PRINS

**Purpose:**

Verify that the SEPP under test correctly handle the 3gpp-Sbi-Target-apiRoot custom HTTP header received from a NF when PRINS security is negotiated with the peer SEPP in a remote PLMN.

**Procedure and execution steps:**

**Pre-Conditions:**

- System documentation of the SEPP under test, including the security mechanisms supported for protection between SEPPs.

- A peer SEPP instance of a remote PLMN for N32 communication with the SEPP under test, which may be simulated.

- A NF for sending HTTP request to the remote PLMN of the peer SEPP via the SEPP under test, which may be simulated and supports 3gpp-Sbi-Target-apiRoot header. The NF is configured to route all HTTP messages with inter PLMN FQDN as the "authority" part of the URI via the SEPP under test.

- The SEPP under test is configured with PRINS security as the security mechanism negotiated with the peer SEPP in the remote PLMN.

- A TLS connection is setup between the SEPP under test and the peer SEPP in the remote PLMN for N32-f forwarding.

**Execution Steps**

1) The NF initiates a HTTP message sent to the SEPP under test, which includes the 3gpp-Sbi-Target-apiRoot header containing the apiRoot of the target URI in the remote PLMN and the apiRoot in the request URI set to the apiRoot of the SEPP under test.

2) The SEPP under test forwards the HTTP request to the peer SEPP in the remote PLMN within the N32-f TLS tunnel.

**Expected Results:**

The peer SEPP received the protected HTTP Request from the NF through the SEPP under test, in which the apiRoot in the request URI is the apiRoot of the target URI in the remote PLMN and no 3gpp-Sbi-Target-apiRoot header is present.

**Expected format of evidence:**

Evidence suitable for the interface, e.g. screenshot containing the operational results.

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