**3GPP TSG-SA3 Meeting #101eS3-202973**

**e-meeting, 9 – 20 November 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **Draft CR** | **rev** | **-** | **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:***  | Threat analysis on NAS based redirection from 5GS to EPS  |
|  |  |
| ***Source to WG:*** | Huawei;Hisilicon,Nokia,Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eSCAS |  | ***Date:*** | 17-08-2020 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | R-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 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:*** | If the Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC is not protected, the attacker can modify the cause and the UE will try to connect to the EPS.When state transition from inactive state to the connected state, if the gNB does not reactivate the UP security based on UP activation status, the UP activation status between the gNB and the UE will be different. This will cause the misalignment on UP activation status.For indirect communication where NF service consumer and NF service producer/NRF cannot mutually authenticate each other, the authentication of NF service consumer towards NF service producer can only implicitly rely on authentication between NF service consumer and SCP and between SCP and NRF/NF service producer with hop-by-hop security protection. An additional authentication for indirect communication is to use a client credentials assertion signed by the NF service consumer and validated by NRF/NF service producer, as defined in TS 33.501 clause 13.3.8. Since a client credentials assertion is not sent directly to NRF/NF service producer but forwarded by one or even several SCPs, there is the risk that the assertion could possibly be swapped by one of the SCPs accidentally on the forwarding path or even be compromised to an attacker. Therefore, it is proposed to analyse the potential threats when the NF service producer/NRF receiving the client credentials assertion cannot correctly validate it.As defined in TS 33.501 clause L.3, the UP security enforcement information shall be set to "required" for data transferred from gNB to a 5GS TSC-enabled UE. This is also applicable to the gPTP messages sent in the user plane.If the UP security enforcement information is not set to "required", the gPTP message transferred from gNB to a 5GS TSC-enabled UE, may be tampered or intercepted by the attacker. Hence, new test on this feature is required.As defined in TS 33.501 clause K.3, to reduce incremental complexity added by security, all PDU sessions associated with a specific 5G LAN group should have the same UP security policy.If the UP security policy within a specific 5G Lan group is not the same, the data may be leaked from the unprotected air interface. Especially, for the case that one security policy is “required’, while the other security policy is “not needed”.The definition of access token claims was updated in TS 29.510 R16.Therefore, it is proposed to update the threat analysis of Incorrect Verification of Access Tokens in TR 33.926 R17 accordingly.In TS 33.501 Release 16, two methods were defined for TLS protection between the SEPP and NFs within a PLMN: telescopic FQDN and 3gpp-Sbi-Target-apiRoot header. When telescopic FQDN is used between the NF and the SEPP, the NF shall use a telescopic FQDN in the Request URI of the HTTP Request to convey the target apiRoot to the SEPP. When 3gpp-Sbi-Target-apiRoot header is used between the NF and the SEPP, the NF shall use the 3gpp-Sbi-Target-apiRoot HTTP header in the HTTP Request to convey the target apiRoot to the SEPP. However, there may be the case that a potentially malicious or misbehaving NF would include both the 3gpp-Sbi-Target-apiRoot header and a request URI containing a telescopic FQDN when communicating with the SEPP. In this case, the SEPP is given two references for routing the NF request across PLMN. According to TS 33.501 clause 13.1.1.1, when communication between the NF and the SEPP that generated the telescopic FQDN is based on using 3gpp-Sbi-Target-apiRoot header, the NF uses the telescopic FQDN in the 3gpp-Sbi-Target-apiRoot header of the HTTP Request. That means whenever the telescopic FQDN is available on the NF, it shall be used to convey the target apiRoot to the SEPP. In the case that a malicious or misbehaving NF includes a 3gpp-Sbi-Target-apiRoot header containing an element different than the telescopic FQDN contained in the Request URI, if the SEPP ignores the telescopic FQDN and uses the 3gpp-Sbi-Target-apiRoot header to route the request, the NF request will not be correctly routed. This can result in Denial of Service and Information Disclosure. Therefore, it is proposed to add a new clause under the normative Annex G.2 in TR 33.926 R17 for the potential threats analysed above.TLS protection between the SEPP and NFs within a PLMN may rely on using telescopic FQDN or 3gpp-Sbi-Target-apiRoot header. Security mechanism negotiated between the SEPPs can be TLS security or PRINS security, and PRINS security shall be used if there are IPX entities on the path between the SEPPs. When PRINS security is used between the SEPPs and 3gpp-Sbi-Target-apiRoot header is used between the NF and the SEPP, the HTTP Request from the NF received by the SEPP will include the 3gpp-Sbi-Target-apiRoot header, which is set to the apiRoot of the target NF. If the sending SEPP forwards the 3gpp-Sbi-Target-apiRoot header together with the HTTP Request on the N32-f interface, there are potentially two threats:* Even if both negotiating SEPPs support the 3gpp-Sbi-Target-apiRoot custom HTTP header, the IPX entities on the path between the SEPPs may possibly not support this custom HTTP header, which will lead to failed message transmission. This can result in Denial of Service.
* Even if all the IPX entities on the path between the SEPPs support the 3gpp-Sbi-Target-apiRoot custom HTTP header, the apiRoot of the target NF in the 3gpp-Sbi-Target-apiRoot header could be potentially modified by a malicious IPX entity, which will lead to the message delivery to the incorrect target. This can result in Information Disclosure and Denial of Service.

Therefore, it is proposed to add a new clause under the normative Annex G.2 in TR 33.926 R17 for the potential threats analysed above. |
|  |  |
| ***Summary of change:*** | Add a new threat analysis to 33.926 related to State translation, NAS based redirection from 5GS to EPS in 5G CIoT, and client credentials assertion validation by NRF/NF service producer.Adding threats related to incorrect security enforcement configurationAdding threats related to security policy misalignment on the 5G LAN services.Updated the threat analysis of Incorrect Verification of Access Tokens in clause 6.3.3.1 of TR 33.926 R17.Added a new clause to analyse the threats related to TLS protection between NF and SEPP under the normative Annex G.2 in TR 33.926 R17.Added a new clause to analyse the threats related to TLS protection between NF and SEPP under the normative Annex G.2 in TR 33.926 R17. |
|  |  |
| ***Consequences if not approved:*** | The threat cannot be well identified and the test on it cannot find its threat reference.No reference of threats related to incorrect security enforcement configuration.No reference of threats related to security policy misalignment on the 5G LAN services.Insufficient threat anslysis for the purpose of the corresponding test case updated in TS 33.117 R17.Lack of threat anslysis for the purpose of the corresponding test case for security assurance.Lack of threat anslysis for the purpose of the corresponding test case for security assurance. |
|  |  |
| ***Clauses affected:*** | 2, 6.2, 6.3.1, 6.3.x(new), D.2.2.X(new), E.2.2.X(new), E.2.2.Y(new), G.2.x.a(new), G.2.x.b(new), K.2.X(new) |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Change 1\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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 TR 33.916: "Security Assurance Methodology for 3GPP network products classes".

[3] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[4] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)".

[5] 3GPP TS 33.116: "Security Assurance Specification for MME network product class".

[6] 3GPP TS 33.511: "5G Security Assurance Specification (SCAS); NR Node B (gNB)"

[7] 3GPP TS 38.300 v15: "NR; NR and NR-RAN Overall Description; Stage 2".

[8] 3GPP TS 23.501 v15: "System Architecture for 5G System; Stage 2".

[9] 3GPP TS 38.323 v15: "NR; Packet Data Convergence Protocol (PDCP) specification".

[10] 3GPP TS 38.322 v15: "NR; Radio Link Control (RLC) protocol specification".

[11] 3GPP TS 33.250: "Security assurance specification for the PGW network product class".

[12] 3GPP TS 33.516: "5G Security Assurance Specification (SCAS) for the AUSF network product class".

[13] 3GPP TS 33.517: "5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class".

[14] 3GPP TS 33.501 Release 15: "Security architecture and procedures for 5G system".

[15] 3GPP TS 33.518: "5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class".

[16] 3GPP TS 33.519: "5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class".

[17] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[18] 3GPP TS 33.513: "5G Security Assurance Specification (SCAS); User Plane Function (UPF)".

[19] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN);Overall description;Stage 2."

[20] 3GPP TS 33.216: "Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class."

[21] 3GPP TS 33.514: "5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class".

[22] 3GPP TS 33.512: "5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)".

[xx] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (Release 16).

[yy] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (Release 16).

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 2\*\*\*\*\*\*\*\*\*\*\*\*

## 6.2 Generic critical assets

The generic critical assets of NF to be protected are:

- NF Application.

- NF API data (e.g. API message IEs, access tokens, client credentials assertions).

Editor's Note: A formulation for indicating the applicable release for the critical assets is needed.

- The interfaces of NF to be protected and which are within SECAM scope:

- Service Based Interfaces.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 2\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 3\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.3.3.1 Elevation of privilege via incorrect verification of access tokens

- *Threat name*: Incorrect Verification of Access Tokens.

- *Threat category*: Elevation of Privilege, Information Disclosure, Denial of Service.

- *Threat Description*: there are following threats if the generic NF cannot correctly verify the access tokens:

- An access token may be tampered so that an attacker can arbitrarily access any services from any NF service providers within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services of any slices provided by the NF producer instances (excluded from the list of NSSAIs or the list NSI IDs) within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the services provided by the NF producer instances outside the NF Set which it is allowed to access within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can arbitrarily access the disallowed resources or conduct disallowed actions on the resources for the services provided by a NF service provider within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

- An access token may be tampered so that an attacker can block service access by replacing the granted services/NF service providers with unavailable services/NF service providers, which leads to denial of service.

- An expired access token can be replayed so that an attack can access the services which may no longer be allowed by the NF service provider, which leads to elevation of privilege and consequently information disclosure.

*- Threatened Asset:* NF API data, NF Application, Sufficient processing capacity.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 3\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 4\*\*\*\*\*\*\*\*\*\*\*\*

### 6.3.x Threats related to authentication for indirect communication

#### 6.3.x.1 Incorrect validation of client credentials assertion

- *Threat name*: Incorrect Validation of Client Credentials Assertion.

- *Threat category*: Spoofing Identity, Information Disclosure, Denial of Service, Elevation of Privilege.

- *Threat Description*: for indirect communication where NF service consumer and NRF/NF service producer cannot mutually authenticate each other, the authentication of NF service consumer towards NRF/NF service producer can only implicitly rely on authentication between NF service consumer and SCP and between SCP and NRF/NF service producer with hop-by-hop security protection. An additional authentication for indirect communication is using client credentials assertions signed by NF service consumer and validated by NRF/NF service producer, as defined in TS 33.501 [xx] clause 13.3.8. Client credentials assertions are sent end-to-end from NF service consumer to NRF/NF service producer via one or several SCPs. There are following threats if the generic NF (including all typers of NF service producer, NRF) receiving the assertion cannot correctly validate it:

- If the NF could not verify the integrity of the assertion, an attacker can deceive the NF by tampering the instance ID of the consumer NF, audience claim, timestamp and expiration time in the client credentials assertion. This can lead to spoofing identity, information disclosure, denial of service, elevation of privilege.

- If the NF could successfully verify the integrity of the client credentials assertion but could not verify the audience claim in the assertion, an attacker can deceive the NF with an assertion detined for another NF type intercepted from the consumer NF. This can lead to spoofing identity, information disclosure, elevation of privilege.

- If the NF could successfully verify the integrity and audience claim of the client credentials assertion but could not verify the expiration time (exp) in the assertion, it can be replayed by an attack, who can abuse the use of assertion for authentication out of its lifetime. This can lead to spoofing identity, information disclosure.

*- Threatened Asset:* NF API data, NF Application, Sufficient processing capacity.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 4\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 5\*\*\*\*\*\*\*\*\*\*\*\*

### D.2.2.X State transition from inactive state to connected state

*- Threat name:* State transition from inactive state to connected state

*- Threat Category*: Denial of Service.

*- Threat Description*: When state transits from inactive state to the connected state, if the gNB does not reactivate/activate the UP security based on UP activation status included in the UE 5G AS security context, the UP activation status between the gNB and the UE may be different. This will cause the misalignment on UP activation status, and result in the UE has to reconnect to the Network again which wastes resource both at UE and gNB.

*- Threatened Asset*: Sufficient Processing Capability.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 5\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 6\*\*\*\*\*\*\*\*\*\*\*\*

### E.2.2.X Incorrect security enforcement configuration

* *Threat name:* Incorrect security enforcement configuration
* *Threat Reference*: Tampering data, Information Disclosure
* *Threat Description*: In case where the UDM is configured to set and provide the User Security Policy to the SMF for TSC service, if the UP security policy is not set to "required", the gPTP message transferred from gNB to a 5GS TSC-enabled UE in the user plane may be removed, tampered or intercepted by an attacker.

\*\*\*\*\*\*\*\*\*\*\*\* End of Change 6\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 7\*\*\*\*\*\*\*\*\*\*\*\*

### E.2.2.Y Incorrect UP security policy configuration for 5G LAN service

* *Threat name:* Incorrect UP security policy configuration for 5G LAN service
* *Threat Reference*: Tampering data, Information Disclosure
* *Threat Description*: It is assumed that two UEs are belonging to one 5G LAN group. In case where the UDM is configured to set and provide User Plane Security policy to the SMF, if the UP security policies set for all the UEs belonging to a specific 5G LAN service are not consistent, e.g. the UP security policy1 for the UE1 is set to "required", and the UP security policy2 for the UE2 is set to "not needed", the 5G LAN service data transferred from gNB to UE2 may be removed, tampered or intercepted by the attacker, even if the service data transferred to the UE1 is protected. That means, the 5G LAN service data will be in the risk of being attacked with the lowest security level set in the the UP security policy.
* *Threatened Asset*: User Subscription Data

\*\*\*\*\*\*\*\*\*\*\*\* End of Change 7\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 8\*\*\*\*\*\*\*\*\*\*\*\*

## G.2.x Threats related to TLS protection between NF and SEPP

### G.2.x.a Inter-PLMN routing using the incorrect reference

*- Threat name:* Inter-PLMN routing using the incorrect reference

*- Threat Category*: Denial of Service, Information Disclosure

*- Threat Description*: TLS protection between the SEPP and NFs within a PLMN may rely on using telescopic FQDN or 3gpp-Sbi-Target-apiRoot header. When telescopic FQDN is used between the NF and the SEPP, the NF shall use a telescopic FQDN in the Request URI of the HTTP Request to convey the target apiRoot to the SEPP. When 3gpp-Sbi-Target-apiRoot header is used between the NF and the SEPP, the NF shall use the 3gpp-Sbi-Target-apiRoot HTTP header in the HTTP Request to convey the target apiRoot to the SEPP. However, there may be the case that a potentially malicious or misbehaving NF would include both the 3gpp-Sbi-Target-apiRoot header and a request URI containing a telescopic FQDN when communicating with the SEPP. In this case, the SEPP is given two references for routing the NF request across PLMN. According to TS 33.501 [xx] clause 13.1.1.1, when communication between the NF and the SEPP that generated the telescopic FQDN is based on using 3gpp-Sbi-Target-apiRoot header, the NF needs to use the telescopic FQDN in the 3gpp-Sbi-Target-apiRoot header of the HTTP Request. That means whenever the telescopic FQDN is available on the NF, it shall be used to convey the target apiRoot to the SEPP. If a malicious or misbehaving NF includes a 3gpp-Sbi-Target-apiRoot header containing an element different than the telescopic FQDN contained in the Request URI and the SEPP ignores the telescopic FQDN but uses the 3gpp-Sbi-Target-apiRoot header to route the request, the NF request will not be correctly routed. This can result in Denial of Service and Information Disclosure.

*- Threatened Asset*: SEPP Application, Service Messages to be sent/received over N32.

\*\*\*\*\*\*\*\*\*\*\*\* End of Change 8\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 9\*\*\*\*\*\*\*\*\*\*\*\*

### G.2.x.b Tampering of Target API Root

*- Threat name:* Tampering of target API root

*- Threat Category*: Denial of Service, Information Disclosure

*- Threat Description*: TLS protection between the SEPP and NFs within a PLMN may rely on using telescopic FQDN or 3gpp-Sbi-Target-apiRoot header. Security mechanism negotiated between the SEPPs can be TLS security or PRINS security, and PRINS security shall be used if there are IPX entities on the path between the SEPPs. When PRINS security is used between the SEPPs and 3gpp-Sbi-Target-apiRoot header is used between the NF and the SEPP, the HTTP Request from the NF received by the SEPP will include the 3gpp-Sbi-Target-apiRoot header, which is set to the apiRoot of the target NF. If the sending SEPP forwards the 3gpp-Sbi-Target-apiRoot header together with the HTTP Request on the N32-f interface, there are potentially two threats:

- Even if both negotiating SEPPs support the 3gpp-Sbi-Target-apiRoot custom HTTP header, the IPX entities on the path between the SEPPs may possibly not support this custom HTTP header, which will lead to failed message transmission. This can result in Denial of Service.

- Even if all the IPX entities on the path between the SEPPs support the 3gpp-Sbi-Target-apiRoot custom HTTP header, the apiRoot of the target NF in the 3gpp-Sbi-Target-apiRoot header could be potentially modified by a malicious IPX entity, which will lead to the message delivery to the incorrect target. This can result in Information Disclosure and Denial of Service.

*- Threatened Asset*: SEPP Application, Service Messages to be sent/received over N32.

\*\*\*\*\*\*\*\*\*\*\*\* End of Change 9\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Change 10\*\*\*\*\*\*\*\*\*\*\*\*

### K.2.X NAS based redirection from 5GS to EPS in 5G CIoT

*- Threat name:* NAS based redirection from 5GS to EPS

*- Threat Category*: Denial of Service, Information disclosure.

*- Threat Description*: In NAS based redirection from 5GS to EPS in 5G CIoT , when a UE initiates registration procedure with the AMF, the AMF may redirect the UE from 5GC to EPC with a Registration Reject message sent to the UE, and if the Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC is not protected, the attacker can modify the cause and the UE will try to connect to the EPS. This will lead to a bidding down attack to the UE.

*- Threatened Asset*: Sufficient Processing Capability, N1 interface, Mobility Management data.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*