**3GPP TSG-SA3 Meeting #100e *S3-202148***

**e-meeting, 17 -28 August 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 seertion cannot correctly validate it. |
|  |  |
| ***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. |
|  |  |
| ***Consequences if not approved:*** | The threat cannot be well identified and the test on it cannot find its threat reference. |
|  |  |
| ***Clauses affected:*** | 2, 6.2,6.3.x(new), D.2.2.X(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).

\*\*\*\*\*\*\*\*\*\*\*\*\* 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.

### 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 2\*\*\*\*\*\*\*\*\*\*\*\*

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

### D.2.2.X State translation 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 3\*\*\*\*\*\*\*\*\*\*\*\*

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

### 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 \*\*\*\*\*\*\*\*\*\*\*\*