**3GPP TSG-SA3 Meeting #115AdHoc-e *draft\_S3-241154-r2***

Electronic meeting, online, 15 – 19 April 2024 merger of S3-241320

**Source: MITRE Corporation, US NSA, Lenovo, Huawei, HiSilicon**

**Title: Resolve EN and provide updates to use case 3**

**Document for: Approval**

**Agenda Item: 5.1**

# Decision/action requested

***Approve clarification to resolve three EN in TR 33.794 [1] Clause 5.1.3, Use case #3: Unauthorized/unauthenticated NF service access request.***

# 2 References

[1] 3GPP TR 33.794, ‘Study on enablers for Zero Trust Security’, (Release 19).

# 3 Rationale

This pCR provides clarifications to resolve the following Editor’s Notes in TR 33.794 [1] clause 5.1.3

Editor’s Note: How reliable the information coming from an unauthenticated NF is FFS.

The information coming from an authenticated NF may not be reliable, however the information received by a NF producer from anywhere should be logged if it resulted in a failed NF service access request. This will help detect the following attacks 1) compromised consumer NF seeking unauthenticated or unauthorized access and 2) DoS attacks on a victim consumer NF by sending spoofed NF service access requests that result in failure. The resulting mitigation is up to operator implementation of monitoring in the Security Function or part of the solution phase i.e., make sure whatever action taken on given NF is commensurate with the risk.

**Proposal:** Make the Editor’s Note a “NOTE: Analysis of failed NF service access request prior to taking mitigating action is required”.

Editor’s Note: Exactly which data is exposed is FFS.

**Proposal:** Information related to failed NF service access request should be collected, such as authentication or authorization credentials, network related information, and reason for failure of the NF service access request.

Editor’s Note: This clause describes the necessary actions on such data (exposure, notification, logging, etc.) and an analysis of the security implications if any.

Networks typically collect data related to failed authentication and analyze the data to identify potential security threats. 5G network should have similar data collection to allow the operator to detect potentially compromised or misconfigured NFs.

**Proposal:** Indicate actions to perform with collected data.

Oauth 2.0 tokens include claims that define the scope of access granted to the NF consumer. Failed audience claim in

the access token indicate that the NF consumer does not have the required permissions to access the requested NF producer resources. Establishing clear criteria for failed token claims enables security monitoring systems to accurately track and analyse elevation of privilege attempts. Therefore, this contribution proposes to consider count for failed token claims use case for TR 33.794 [1] related to objective.

# 4 Detailed proposal

SA3 is kindly requested to agree the pCR below to TR 33.794 [1].

\*\*\*\*\*Start of Change 1\*\*\*\*\*

### 5.1.3 Use case #3: Unauthorized/unauthenticated NF service access request

#### 5.1.3.1 Description

A NF service access request that is made by an unauthenticated or unauthorized NF could be logged and reported for security monitoring and evaluation.

In the context of network function (NF) security, it is essential for an NF Service Producer to verify the audience claim in the access token received from an NF consumer. This verification process ensures that the NF Service Producer only accepts tokens intended for its own identity or the specific type of NF service it provides.

The "Elevation of Privilege" threat from the STRIDE model refers to the risk of an NF consumer attempting unauthorized access to NF producer resources or performing actions beyond their intended privileges by misuse of already issued token access by the NRF. By checking the audience claim, the NF Service Producer validates the access permissions to the intended resource associated with the issued access token and confirms that the access token is appropriate for its use and prevents unauthorized access or misuse of its resources.

The benefits of collecting data related to an unauthorized or unauthenticated NF service request attempt include:

- Traceability and accountability (e.g., non-repudiation, forensic analysis of security event)

- Indicators of potentially compromised NFs

- Indication of elevation of privilege attempt [aa], [bb]

One could include the collection of data relevant to failed authentication and authorization during NF service access requests.

NOTE: Analysis of failed NF service access request prior to taking mitigating action is required.

Not monitoring or collecting data related to failed NF service access request (i.e., unauthorized or unauthenticated NF) can reduce the ability to detect key indicators of potentially compromised NFs.

Analysis of security events lacks trustworthy information that helps with threat detection.

#### 5.1.3.2 Relevant data

Information related to failed NF service access request can be collected, such as:

- In failed authentication use case:

- TLS certificate information: expiration time, subjectAltName (nfInstanceID), Subject DN, unsupported operator CA, Serial Number, public key info.

- In failed authorization use case:

- Token Claims Information: Access tokens issued by the NRF (e.g., expiration time, scope / additional scope, token identifiers in the claim i.e associated NF Consumer ID, NF Producer ID, nfInstanceID of NF Consumer or NRF (issuer), expected NF service name, nfType, unsupported NRF (issuer signature), PLMN ID)

- Authorization decisions made by the NRF, if there were any prior attempts from this NF consumer towards the NRF for the target producer indicating whether access requests were denied based on NRF policy evaluations.

- Include details of authorized resources, requested actions, and enforcement decisions.

- Network related information (e.g., source/target IP address).

- Reason for failure

NOTE: The specific data for collection will be determined in the conclusions

#### 5.1.3.3 Evaluation of the identified data

Information related to a failed NF service access request may help to indicate misconfigured or compromised NF(s). Notifying the Operator Security Function when there is a failed NF service access request and exposing/logging the identified relevant data to the Operator Security Function is crucial for conducting an analysis and performing any mitigating actions on the NF that made the NF service access request attempt.

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

\*\*\*\*\*Start of Change 2\*\*\*\*\*

# 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 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[3] 3GPP SP-231784, "New Study on enablers for Zero Trust Security".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] RFC 6749, "The OAuth 2.0 Authorization Framework".

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] 3GPP TR 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[8] NIST Special Publication 800-207: "Zero Trust Architecture".

[9] 3GPP TR 33.738: "Study on security aspects of enablers for network automation for the 5G system phase 3".

[10] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

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

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

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