**3GPP TSG-SA3 Meeting #115 *draft\_S3-240905-r1***

Athens, Greece, 26th February - 1st March 2024 *revision of S3-240383*

**Source: MITRE**

**Title:** **ZTS New Data exposure use case: Unauthorized/unauthenticated NF service access request**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***This pCR proposes a New Data exposure use case for TR 33.794: Unauthorized/unauthenticated NF service access request***

# 2 References

[1] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[2] RFC 6749 The OAuth 2.0 Authorization Framework

# 3 Rationale

A NF service access request that is made by an unauthenticated or unauthorized NF should be logged and reported for security monitoring and evaluation to enable traceability and accountability and detect potentially compromised NFs.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 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*.

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

[Z] RFC 6749 The OAuth 2.0 Authorization Framework

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

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

### 5.1.X Data exposure use case X: Unauthorized/unauthenticated NF service access request

#### 5.1.X.1 Description

A NF service access request that is made by an unauthenticated or unauthorized NF should be logged and reported for security monitoring and evaluation. The benefits of collecting data related to an unauthorized or unauthenticated NF service request attempt are:

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

- Indicators of potentially compromised NFs

It is recommended to include collection of data relevant to failed authentication and authorization during NF service access requests.

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.X.2 Data to be exposed

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

- In failed authentication use case:

- Data for collection can include, but not limited to, any data related to a rejected TLS certificate (e.g., lapsed expiration time, subjectAltName (nfInstanceID), Subject DN, unsupported operator CA).

Editor's Note: Whether the NF instance ID of the peer NF is reliable information in case of authentication failure is FFS.

- In failed authorization use case:

* Data for collection can include, but not limited to, any data related to a rejected OAuth 2.0 Token (e.g., lapsed expiration time, scope / additional scope, nfInstanceID of NF Consumer or NRF (issuer), expected NF service name, nfType, unsupported NRF (issuer signature), PLMN ID).

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

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