**3GPP TSG-SA3 Meeting #115 *draft\_S3-240385-r2***

Athens, Greece, 26th February - 1st March 2024

**Source: MITRE**

**Title:** **ZTS New data exposure use case: Topology discovery**

**Document for: Approval**

**Agenda Item: 5.1**

1 Decision/action requested

***This pCR proposes a Data exposure use case for TR 33.794: Topology discovery***

2 References

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

[2] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

3 Rationale

NFs use TLS to protect application layer traffic as specified in 3GPP 33.501 [1] sub-clause 13.1.0 between NFs. Within a security domain the validity of the certificate is checked and, if it is valid, the TLS connection is setup. 3GPP TS 33.310 [2] subclause 5.2.2.2 provides a good overview of the process when a certificate is checked by TLS client and TLS server. No validation is performed on other parameters e.g. subjectAltName, nfTypes etc (defined in 3GPP 33.310 [2] which contains NF instance ID & NF type). At this authentication phase it is not validated whether the NF is allowed to communicate with the receiving entity. Only checking to see if a certificate is valid and not applying any context (e.g. is NF consumer allowed to or expected to contact the NF producer) to the check allows the consumer NF to discover the network topology.

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*.

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

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

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

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

### 5.1.X Data exposure use case X: Service discovery

#### 5.1.X.1 Description

Secure communications between NFs and with other NFs and the NEF nodes is essential. TLS is specified to secure the transport layer (See 3GPP TS 33.501 [x] sub-clause 9.5, 12.3, 13.1.0). When a TLS connection is setup both sides of the TLS connection check to ensure that the certificate is valid and has not been revoked; however, no validation is performed to ensure that the NF setting up the TLS connection is expected to communicate with the NF terminating the TLS connection (e.g., No validation is performed on other parameters e.g. subjectAltName defined in 3GPP 33.310 [y]). A compromised NF can setup TLS connections to any number of other entities, collect the TLS certificates of the other NFs and use e.g the nfTypes certificate attribute as defined in 3GPP 33.310 [y] subclause 6.1.3c.3 to determine what service(s) are supported by targetted NF.

Not monitoring or collecting data related to successful NF TLS connections can reduce the ability to detect key indicators of potential compromise of NFs.

Analysis of security events lacks trustworthy information regarding the potential source of adversity.

#### 5.1.X.2 Data to be exposed

IEditors note: FFS what data is to be collected.

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