**3GPP TSG-SA3 Meeting #119 draft\_S3-245180-r1**

Orlando, US, 11 -15 November 2024 *revision of S3-244678*

**Source: MITRE-FFRDC, US National Security Agency, Johns Hopkins University APL**

**Title: KI 1 Conclusion Clarifications on Replay Use Case**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***It is proposed to approve the proposed changes to TR 33.794 clause 8.1***

# 2 References

[1] 3GPP TR 33.794 Study on enablers for Zero Trust Security

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

# 3 Rationale

In TR 33.794 [1] clause 8.1 the following bullet d is concluded:

*d. The NF collects information about potential replay attacks on the SBA layer (Clause 5.1.6).*

Additionally, the following EN is added requesting clarification:

Editors note: Bullet d) is FFS.

**This contribution resolves the EN by adjusting the bullet d to the following:**

*d. The NF collects information about fraudulent or replayed access tokens. (Clause 5.1.6).*

Rationale for changes:

* The use case (in clause 5.1.6) is targeting a scenario where an OAuth 2.0 access token is captured and replayed by an attacker. Although this scenario is unlikely due to the access token typically being confidentiality, integrity, and replay protected using SBA communications, there are scenarios where the access token can be exposed in cleartext within a protected environment.
* An access token can be reused for the duration of the token lifetime; thus, reuse of the same access token is not uncommon. To detect a fraudulent or replayed access token, the NF would need to compare the expected identity of the access token claims with the actual identity of the received service request, using multiple layers of the protocol stack (e.g., as described in TS 33.501 [2] clause 13.4.1.1.2 access token verification steps). The discrepancies found (e.g., *NF Instance ID in the subject claim within the access token* DOES NOT match *the NF Instance ID in the subjectAltName in the NF Service Consumer's TLS client certificate*) can be used by the MNO to perform continuous security monitoring and evaluation.

# 4 Detailed proposal

## 8.1 Key Issue #1: Data exposure for security evaluation and monitoring

The security incidents or scenarios in SBA where data can be collected in the SBA layer includes

1) authentication and authorization failure event;

2) unexpected setup of TLS session and API invocation related to unauthorized reconnaissance;

3) malformed message event;

4) high service load;

5) unexpected SBI call flows; and

6) unexpected use of APIs exposed by services in SBA layer

Editor’s Note: Further aspects if any related to KI#1 is FFS.

The key issue will be addressed by requirements for data collection to enable security evaluation and monitoring on the SBA layer. No new interface nor protocol will be specified as result of the work in this report.

The following requirements address KI#1 Data exposure for security evaluation and monitoring. The requirements also address the use cases for security evaluation and monitoring described in clause 5.1.

General requirements for security event logs:

1. The NF supports the generation of security event logs.

Security event logs contain security relevant events data. Requirements related to security relevant events data for monitoring:

a. The NF collects information on the SBA layer about received malformed messages that deviate from the 3GPP specified messages or are considered invalid according to the protocol specification and network state are to be logged. (Clause 5.1.1)

b. The NF collects information about events involving a massive number of incoming messages on the SBA layer. (Clause 5.1.2).

c. The NF collects information about authentication and authorization failure on the SBA layer. (Clause 5.1.3).

d. The NF collects information about invalid use of access token. (Clause 5.1.6).

Editors note: Additional details if any are FFS.