**3GPP TSG-SA3 Meeting #115AdHoc-e *draft\_S3-241156-r2***

Electronic meeting, online, 15 - 19 April 2024

**Source: US National Security Agency, MITRE Corporation, OTD\_US, JHU APL**

**Title: Abnormal SBI Call Flow**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Seeking approval of a new use case***

# 2 References

[1] 3GPP TS 23.501: " System architecture for the 5G System (5GS)"

# 3 Rationale

Annex E of TS 23.501[1] identifies four distinct communication models for NF-to-NF interactions. Each of these communication models have clearly defined call flows. Once a 5GC is configured to use one of these communication models, a NF deviating from that call flow is a strong indicator that there is either a misconfiguration, an attack in progress, or it is an aritifact of an already exploited NF.

# 4 Detailed proposal

\*\*\*\*\*Start of 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 33.894, 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".

[X] 3GPP TS 23.501: " System architecture for the 5G System (5GS)".

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

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

### 5.1.X Use case #X: Abnormal SBI Call Flow

#### 5.1.X.1 Description

There are four distinct communication models that are defined in 3GPP TS 23.501 Annex E[x] that NFs and NF services can use to interact which each other. Once the SBI communications have been configured to follow a defined communication model(s) as specified in 3GPP TS 23.501 Annex E[x], the SBI call flows specified between the NF and NF services should be considered the normal communication path. Any deviation from the normal communications model could be an indicator of either a misconfiguration, an attack on the NF or NF services in the 5GC that may be in progress, or an artifact of a successfully exploited NF.

 Note: It is up to the operator to properly configure the monitoring system with the correct communication model in use.

Note: If more then one communication model is in use it is up to the operator to properly configure the monitoring system with the correct communication models in use and which NFs belong to each communication model.

#### 5.1.X.2 Relevant data

When traffic pattern logging is enabled, the serving NF logging the source IP address of SBI requests can expose each of the following examples of abnormal SBI call flows:

* For communication model A, a deviation from the normal call flow could mean communication flows that would not normally occur between two NFs. (e.g., PCF attempting to connect to the AUSF.)
* For communication model B, a deviation from the normal call flow could mean communication that bypasses the NRF and its functionality. (e.g., Consumer NF never connects to NRF before attempting to connect to a Serving NF.)
* For communication model C and communication model D, deviation from the normal indirect communication call flow modes could mean bypassing the SCP and its functionality. (e.g., Consumer NF never connect to SCP and instead attempts to connect to Serving NF.)

Editor’s Note: The collection entity is FFS.

Editor’s Note: Traffic patterns indicating abnormal SBI call flow at the NF level is FFS.

#### 5.1.X.3 Evaluation of the identified data

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

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