**3GPP TSG-SA3 Meeting #116 *draft\_S3-242426-r4***

Jeju, South Korea, 20th - 24th May 2024 revision S3-241850

**Source: MITRE Corporation, Johns Hopkins University APL, OTD\_US, US National Security Agency**

**Title: New solution for KI#1: New Data Collection NFs**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Approve the solution and include in TR 33.794 [1]***

# 2 References

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

# 3 Rationale

ZTS [1] has identified Key Issue 1 which looks to find architectural solutions to facilitate the collection of data.

|  |
| --- |
| 6.1.3 Potential security requirementsThe 5GS should provide the means to facilitate collection of data potentially relevant for operator-based security evaluation and monitoring.NOTE 1: The actual set of data that can be collected to realize any threat assessments is up to the solution discussions in Clause 7.NOTE 2: The algorithms or logic for trust monitoring and evaluation are outside the scope of 3GPP.NOTE 3: The handling of potentially compromised NFs (e.g. based on detection) with required security aspects (e.g. applying necessary security patches/fixes) is Operator's implementation choice.NOTE 4: Solutions to this key issue need to address one of or both of the following aspects: (1) Specification of data (stage-2) to be collected for security evaluation and monitoring of the 5G SBA, (2) Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA.Editor's Note: Architectural aspects of the 5GS need to be confirmed by SA WG2.  |

This contribution proposes an architecture that can be used to facilitate the transfer of data from an NF to the operator’s security function.

# 4 Detailed proposal

**\*\*\*\*Start of First Change\*\*\*\***

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

AMF Access and Mobility Management Function

NF Network Function

NRF Network Repository Function

OSF Operator Security Function

SCP Service Communication Proxy

SDCF Security Data Collection Function

SDRF Security Data Repository Function

SDPI Security Data Point of Ingest

SMF Session Management Function

**\*\*\*\*End of First Change\*\*\*\***

**\*\*\*\*Start of Second Change\*\*\*\***

##  7.Y Solution #Y: New Data Collection NFs

### 7.Y.1 Introduction

This solution addresses KI#1 *Data exposure for security evaluation and monitoring*. Specifically, it addresses the requirement: *(2) Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA*.

The basic principle of this architectural solution is to define security architecture elements that function as the security data points of ingest (SDPIs) which can be used by the operator’s security function (OSF) to execute policy decision points (PDPs). SDPIs, in this proposal can read all SBI related data on the NF and are configured to send this data (on a per NF basis per operator policy) to intermediate functions described below which then delivers the data to the operator’s security function (OSF).

The following functions are defined:

1. Security Data Collection Function (SDCF) which is responsible for consuming the data collected from either SDPIs or via other existing interfaces.

2. Security Data Repository Function (SDRF) which is responsible for storage of the SDCF data and is configured by the operator.

3. Security administration function (SADF) which is configured by the operator and acts as an intermediary, coordinating, authorizing, and monitoring the tasks present at the various SDPIs present in NFs.

NOTE: The conclusion phase could determine if some of the functions defined in steps 1-3 can be combined.

The OSF remains outside the scope of 3GPP but is expected to provide logic of PDP. The SDRF is defined to act as the producer which then interfaces via an internal mechanism to the OSF.

There could be one to many SDRFs. The solution is based on the existing SBA allowing SDCF and SDRF to communicate via direct communication or use an NRF and or SCP as defined in 3GPP 33.501 [4].

NOTE: If an NRF and/or SCP is used, these might be separate physical entities on the SBA network to reduce the impact of security network being compromised. This is an operational deployment decision and is outside the scope of 3GPP.

Editor’s Note: How current SBI interfaces and messages (e.g. Nadrf, Nnwdaf) can be reused between the SDPIs and OSF is FFS.

Editor’s Note: The security risk of handling security data together with non-security related data needs to be evaluated against best practice of handling security logs, e.g., in NIST SP 800-92

### 7.Y.2 Solution details

#### 7.Y.2.1 General

The solution is split into 2 components, 1st is how the OSF configures an NF to provide data and the 2nd how data is then delivered to the OSF.

#### 7.Y.2.2 Data Configuration

 

Figure 7.Y.2.2-1: Data analytics information request

0. The operator provisions OSF policy including SDPI rule sets.

1. The OSF sends a message analytics info request message to the SADF identifying the SDPIs (e.g. SDPI in Nf1, NF2, NF3) it requires to be activated, storage criteria, and event generation reporting schemas.

NOTE: This interface between the SADF and the OSF is not a 5G SBA interface and is outside the scope of 3GPP. However, a secure channel is setup between them.

2. SADF sends an analytics info request message to the SDCF. The message shall include the NF types that the OSF wanted analytics information from. E.g. NF1, NF2 and NF3.

 SDCF receives a analytics info message from the SADF.

Editor’s Note: If the SADF sends individual NF Instance IDs and or NF types that it wants analytics information from is FFS.

3 SDCF sends a analytics info message to all relevant SDPIs in the identified NF types indicated by the SADF, derived from the SDPI rules set by the OSF.

Editors Note: How current SBI interfaces and messages (e.g. Nadrf, Nnwdaf) can be reused is FFS.

NOTE 1: Operator policy and or configuration identifies the type of interface to use.

#### 7.Y.2.3 Data delivery



Figure 7.Y.2.3-1: Data transfer

1a/b/c. SDCF receives analytic payload from an NF SDPI (e.g. NF1, Nf2, Nf3). .

Editor’s Note: The analytic payload data is FFS.

Editors Note: How current SBI interfaces and messages (e.g. Nadrf, Nnwdaf) can be reused is FFS.

2 SDCF decides, based on operator policy, to send analytic payload it has received to SDRF for storage and future retrieval by the SADF or directly by OSF.

Editor’s Note: It is FFS if any specific policies are required for this storage and retrieval.

3. SDCF sends the analytic payload it has received from (e.g. Nf1, Nf2, NF3) to SDRF.

 SDRF performs necessary validation to ensure that the NF sending the analytic payload (SDCF) is allowed to send SDRF analytic payload and that SDCF is allowed to send analytic payload from NF instance Id from step 1a) and from NF instance ID from step 1b).

NOTE: SDCF could only send analytic payload from one NF e.g. AMF and SDCF send the other NFs analytic payload e.g. SMF data later.

Editor’s note: The impact to both standardization and products of sending the same data over multiple interfaces needs to be evaluated.

4 SDRF decides, based on operator policy, to send analytic payload it has received to the OSF.

Editor’s Note: It is FFS if any specific policies are required for this storage and retrieval.

5. SDRF sends the identified analytic payload if received from SDCF to the OSF.

Editor’s Note: What triggers data to be transported to the OSF is FFS.

### 7.Y.3 Evaluation

Editor’s Note: Identifying the capabilities of the operator’s security function is out of scope of 3GPP.

**\*\*\*\*End of Second Change\*\*\*\***