**3GPP TSG-SA3 Meeting #120 *S3-25XXXX***

Athens, Greece, February 2025

**Source: vice chair (NTT DOCOMO)**

**Title: New WID on security management service**

**Document for: Approval**

**Agenda Item: 6**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Security management service

Acronym:

SecMS

Unique identifier:

TBD

Potential target Release: Rel-19

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | X |  |
| No | X | X | X |  |  |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Study |
|  | Normative – Stage 1 |
| X | Normative – Stage 2 |
| X | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| N/A |  | {optional free text} |

# 3 Justification

3.1 Background of security management

The Service Based Architecture (SBA) is the dominant method for both control plane and management communications. In additions to the many benefits to using SBA, e.g. agility to increase and decrease the number of services in coordination with demand, comes an expanded attack surface. TS. 28.533 does provides authentication and authorization security controls and TS 33.501 provides integrity and confidentiality. However, visibility in the form of continuous monitoring is missing.

In TS 28.533, section 4.6, it states "The management data analytics utilize the network management data collected from the network (including e.g. service, slicing and/or network functions related data) and make the corresponding analytics based on the collected information. For example, the information provided by PM data analytics services can be used to optimize network performance, and the information provided by FM data analytics services can be used to predict and prevent failures of the network. Security benefits like more efficient security detection and higher protection can also be achieved in a similar way by utilizing security data collected from the network.

3.2 Security Requirement

Currently, legacy security requirements include certificate management, confidentiality, integrity, authorization, and SCAS. While those legacy security requirements are still practical today. They do not address emerging Advanced Persistent Threats (APTs) and the visibility into the SBA needed to detect them.

With the introduction of SBA, new security requirements are needed.

1. Service-based architecture enhances flexibility and scalability of 5G network. It also introduces additional threats. Although there is TLS and Oauth to enhance protection in SBA, it still faces the problem that a breach of the network can then used to attack to other NFs. The network lacks security detection functionality into NFs. Traffic analysis alone is not efficient enough to detect compromised NFs. Security operations center requires more visibility into NFs. Because add-on solutions can come with their own set of security or interoperability issues, built-in security detection capabilities should be applied to 5G networks. This argument also applies to east-west traffic as well as network management operations.

In the SBA there are gaps in the current security requirements that make detection of threats difficult.

The security incidents or scenarios in the network where data can be collected include

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

4 Objective

The objective of this WID is to specify a data collection solution for continuous security monitoring. It proposes security management service enhancements under service based management architecture to collect necessary data related to 3GPP features. Following objectives are proposed:

WT1:

- Specify the security requirements to transfer or communicate security events.

- It specifies the general requirements for security event message handling.

Security event messages contain information about security relevant events that can be used by an operator security management.

WT2:

- This work will specify the events that need to be reported as part of continuous security monitoring.

Examples for security relevant events data for monitoring:

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

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

c. The NF collects information about failed authentication and authorization attempts from inbound connections on the SBA layer. (Clause 5.1.3)

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

e. The NF collects information about potential abnormal SBI call flows as defined for the communication models in Annex E of TS 23.501 [17]. (Clause 5.1.5)

Collect and report sensitive network management operations at SBA or platform level like management login/logoff events, configuration modification, etc.

Specify for each of the events which set of data (e.g., information elements as applicable) needs to be reported for the security messages.

NOTE 1: The format of this reporting will be selected by SA5. Coordination with SA5 will be required.

NOTE 2: The method for collecting this data in the NF is up to implementation.

## TU estimates and dependencies

|  |  |  |  |
| --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe) |
|  |  |  |  |
| WT1: Security reporting requirements |  | 0.25 | No |
| WT2: Security events definition |  | 3.75 | No |

Total TU estimates for the study phase: N/A

Total TU estimates for the normative phase: 4

Total TU estimates: 4

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type | TS/TR number | Title | For info at TSG# | For approval at TSG# | Rapporteur |
|  | TS33.abc | Security monitoring | SA#108(June 2025) | SA#109(September 2025) |  |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

TBA

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Event reporting mechanism to be defined by SA5

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |