**3GPP TSG-SA3 Meeting #115 *S3-240709***

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

**Source: China Mobile, ZTE, Nokia, Nokia Shanghai Bell, CATT, CableLabs, China Telecom**

**Title: New SID 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: Study on security management service

Acronym:

FS\_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 | X |  |
| No | X | X |  |  |  |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study  |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | 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

In TS 28.533, it defines 3GPP network management and orchestration architecture. The management capability is provided as a service from management provider to consumer when the consumer is authenticated and authorized. TS28.533 introduces authentication service and authorization service in access control capability. However, apart from those two service, no more security related services are introduced.

What is more, as service based architecture is introduces, more security management like security policy management and sustained security monitoring should be considered. But currently there is no specific standard on that.

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. ”It implies that security benefits like more efficient security detection and higher protection can also be achieved as similar way, i.e. security data analytics service utilizing security data collected from the network. For example, security management data analytics service could behave as a service consumer, to request security related log from specific NF as a service provider. By analyzing such log, security management service could find whether there are security attacks like password brute force attack, abnormal login attempt, etc. It could help to identify security attacking attempts and to diminish the time-window for attacking.

However, in TS 28.104, there is lack of security analytics related capability and service in section 7, which describes use cases and requirements for MDA capabilities and services. In TS28.500, the description is introducing requirement and use cases for FM, CM, PM and LCM, but security is not involved.

In a word, in SBMA defined by SA5, there is lack of content about security management services.

3.2 Security Management Requirement

**Legacy Security Management Requirement**

Currently, security management includes key management, certificate management, security hardening. It usually implemented as follows: to configure NF management account and password in a secure manner from OAM for access control, to issue certificate for NF device authentication; to close un-necessary service and port to mitigate attacking possibility, etc. Those typical security management requirement are still applied under service-based architecture.

**New Security Management Requirement.**

However, with introduction of service-based architecture, some new security management requirement are raised.

1. Intrusion detection analysis. Service-based architecture enhances flexibility and scalability of 5G network. But it also introduces more threats from other NFs. Although there is TLS/Oauth to enhance security protection in SBA, it still faces the problem that an NF may be compromised in some cases and make stepping attack to other NFs. What is more, 5GC and beyond network is more and more virtualized. Such deployment NF is vulnerable to attacks from the virtual layer and other malicious virtual machines. All those require enhancement to strengthen the security protection and detection capabilities of NF itself. Currently SA3 has defines SCAS specification, which could guarantee NF security protection through security feature check, hardening and BVT. But it still lacks of security detection functionality to NF. Nowadays, in the real network, some security dedicated devices are deployed on network boarder also. But they are mainly focus on traffic detection rather than NF attacking like password brute force , abnormal signaling. So the security concerns is still not mitigated. As a result, a built-in security detection feature should be applied in 5G network, to collect data related with 3GPP features. As NF can record some security related information such as login attempt time and frequency, invalid signaling warning, etc. in the log, it bring benefit to send such information to some security analysis sub-system to detect potential attacking and improving security detection efficiency. For example, OAM can collect information from NF to help analysis against DDoS attack.
2. Security analysis and access control of east-west traffic inside: Cloud deployed NFs may suffer illegal access from other NFs which is reside in same host. The VMs may also be subject to illegal access from other VMs deployed other part of NFs. Current access control method by using VLAN separation within the resource pool cannot mitigate such abnormal access issue happened in east-west traffic, thus more detailed access control is needed. After instantiation of NFs, the security management analysis service can analyze the traffic information reported by NFs, such as {source IP, destination IP, source port, destination port, protocol}. Based on analysis, it can generate a security policy about east-west traffic, and send it to the corresponding NFs. After that, more detailed analytics for abnormal traffic and policy update could be made in further round.
3. Security configuration baseline check: Once NF is instantiated, security hardening should be made according to the security configuration baseline. And such hardening configuration should be checked periodically. The reason is that during the operation, NF may be attacked and compromised, suffering security configuration broken. For example, some closed ports which is unnecessary are forced to open. That will allow attack to visit NF through such interface to trigger further attacks. Therefore, it is necessary for the management system to regularly and automatically verify the security baseline of NF, trying to discover and repair the exposed surface of NF in a timely manner.
4. Security policy management: SBA raises security policy management requirement for authorization. When an NF consumer would like to request service from NF producer, it may need to get authorization token from NRF. Thus NRF need to maintain authorization policy. If one NF is under attack, the authorization policy needs to be updated to remove the authorization against this NF. When the NF is recovered from attack, the policy should be updated again to restore the NF’s authorization permission. That could be made through security management service.

In a word, in service based management architecture, there are gaps between security management requirements and current security management manners on how to collect necessary data related with 3GPP features. In order to improve 5G network security management capabilities, it is necessary to study the uses cases, requirements and possible ways of security management under service based management architecture with deep analysis on the 5G network architecture and business requirements.

In another aspect, there is an ongoing study about zero trust in SA3 which may also want to expose security information. However, ZTS is used to collect information for security analysis in control plane, while this is focus on helping security management in management plane. For example, the proposal considers case related with communications between NFs inside one NFVI devices, which is not in scope of ZTS. Another example is about case 4 that to help security policy management, which is not mentioned in ZTS also.4 Objective

It proposes to study the use cases, requirements and possible solutions of security management under service based management architecture to collect necessary data related with 3GPP features, including:

* The use case of security management mainly identifies new use cases under the SBMA architecture, e.g. NF intrusion detection analysis, security analysis and access control of internal traffic, security configuration baseline check, security configuration enrolment/update, etc.
* Potential requirement about security management for use cases
* Possible solutions to fulfill such requirement if needed.

## TU estimates and dependencies

|  |  |  |  |
| --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe) |
| Use Case | 1 |  | No |
| Potential req. | 1 | 0.25 | No |
| Possible Sol. | 1 | 0.25 | No |

Total TU estimates for the study phase: 3

Total TU estimates for the normative phase: 0.5

Total TU estimates: 3.5

# 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 |
| Internal TR | 33.abc | Security enhancement to Management service | SA#105(September 2024) | SA#106(December 2024) | Qi Minpeng, China Mobile |
|  |  |  |  |  |  |

|  |
| --- |
| 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

Protocol aspects covered by SA5

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| China Mobile |
| ZTE |
| CATT |
| Nokia |
| Nokia Shanghai Bells |
| CableLabs |
| China Telecom |