**3GPP TSG-SA3 Meeting #122 S3-252357-r5**

**Fukuoka, Japan, 19 - 23 May 2025** **(revision of S3-252065)**

**Source: China Mobile, ZTE, CATT, Johns Hopkins University APL, CAICT, CableLabs, Nokia, China Unicom, China Telecom**

**Title: New SID on enhanced security management service about security policy provisioning**

**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 enhanced security management service for security policy provisioning

Acronym: FS\_SPE(TBD)

Unique identifier: (TBD)

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-20

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 …

|  |  |
| --- | --- |
| 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 | N/A | N/A | 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 | N/A | N/A |

# 3 Justification

Current network security specifications mainly focus on how to protect connections between NFs, but lack consideration of how to provision and manage network security policies to execute such security procedures. It is important to standardise such abilities for network operators to improve the security protection of networks.

There are some cases that need to be considered to enhance the security management service for security policy provisioning. It should be noted that there are preconditions mentioned in cases. How to achieve such precondition is not in scope of this study.

1. *On-demand Security Enabler to Protect 3GPP NFs*

Based on 5G features like SBA, slicing, etc., network operators can provide services not only for common customers, but also for vertical markets with specified requirements and solutions. In general, legacy communication and value-added services provided for common customers can be called "To Customer" (ToC) services. The services provided to vertical markets can be called "To Business" (ToB) services. ToB services are usually associated with specified requirements/solutions for each vertical market. ToB service is crucial for mobile operators. Some 3GPP NFs in 5G have been deployed in ToB dedicated networks, e.g. PNI-NPN.

Due to the differentiated security requirements of enterprises across various industries, the operators need to be able to deploy the security capabilities on-demand to protect 3GPP NFs. Some of these security capabilities are related to NFs, including the interfaces and OS. However, operators may deploy a network with general security features at the beginning, or may extend existing networks for newly enabled vertical services.

1. *Security Policy Consistency Co-operation*

Some security attacks (e.g., GTP Door Malware) target the 3GPP NFs. Mitigating the attacks requires cooperation and coordination among 3GPP NFs which reside on multi-stakeholder on-premises networks and/or cloud networks.

The general security response policy can be decomposed into multiple different sub-policies. The NFs residing in multiple network domains need to be coordinated.

So based on above cases, it is necessary to study the security requirements for security policy provisioning, execution and management. Furthermore, it also needs to study which mechanisms to support security policies are required.

# 4 Objective

The following work tasks are proposed for this study:

WT1:

* Identify the use cases that involve for security policy provisioning and management

* Identify potential security requirements on security policy provisioning and management for each use case

Note 1: It is out of scope how the security policy is generated.

WT2:

* Identify the mechanisms to support security policies that are required.
* Develop methods for secured delivery of security policy objects to NFs, e.g., via network manager (directly or via element manager) or via manual configuration.

 Note 2：The case of PNI-NPN (e.g., ToB) and Public Network (e.g., ToC) network architectures/services will be involved in this study.

Note 3: Whether to start WT2 work is depends on progress of WT1.

## TU estimates and dependencies

|  |  |  |  |
| --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe) |
|  |  |  |  |
| WT1: Develop use cases and requirements | 2 | 0 | No |
| WT2: Identify security policy mechanisms and methods for secured delivery of security policies | 3 | 1 | No |

Total TU estimates for the study phase: 5

Total TU estimates for the normative phase: 1

Total TU estimates: 6

# 5 Expected Output and Time scale

|  |
| --- |
| 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 | Study on enhanced security management service about security policy execution | SA#110(December 2025) | SA#112(June 2026) | TBD |
|  |  |  |  |  |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

N/A

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| China Mobile |
| ZTE |
| CATT |
| Johns Hopkins University APL |
| CAICT |
| CableLabs |
| Nokia |
| China Unicom |
| China Telecom |