**3GPP TSG-SA3 Meeting #116 *S3-242339***

Jeju, Korea, 20 - 24 May 2024

**Source: Indian Institute of Technology Bombay**

**Title: Filtering requirements on Diameter interface for Security Assurance Specifications for SMSF**

**Document for: Approval**

**Agenda Item: 4.4**

# 1 Decision/action requested

***SA3 is kindly requested to approve the addition of SGd filtering requirements and associated test cases in draft 33.529 v0.4.0 Security Assurance Specification for Short Message Service Function (SMSF).***

# 2 References

[1] 3GPP TS 33.529 “Security Assurance Specification (SCAS) for the Short Message Service Function (SMSF) network product class” v0.4.0

# 3 Rationale

*This contribution proposes to add a test case in the TS draft [1] with filtering requirements on SMSF specific SGd interface and also to include the relevant reference.*

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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 TS 33.117: "Catalogue of general security assurance requirements".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS) ".

[6] 3GPP TS 23.501: "System Architecture for the 5G System (5GS) ".

[7] 3GPP TS 29.540: "5G System; SMS Services".

[8] 3GPP TS 29.338: "Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs) ".

[9] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[10] 3GPP TS 33.210: "Network Domain Security (NDS): IP network layer security".

[11] 3GPP TS 33.310: "Network Domain Security (NDS): Authentication Framework".

[12] IETF RFC 6733: "Diameter Base Protocol".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.7.x Protecting availability and integrity on Diameter-based SGd interface

*Requirement Name:* Diameter filtering on the SGd interface

*Requirement Reference*: 3GPP TS 29.338 [8], clause 6.3.2.2;

*Requirement Description*:

3GPP TS 29.338 [8] defines the following commands and their command codes for the SGd application: MO-Forward-Short-Message-Request (OFR) - 8388645, MO-Forward-Short-Message-Answer (OFA) - 8388645, MT-Forward-Short-Message-Request (TFR) - 8388646, MT-Forward-Short-Message-Answer (TFA) - 8388646, Alert-Service-Centre-Request (ALR) - 8388648 and Alert-Service-Centre-Answer (ALA) - 8388648. It also mentions that the Application ID field for OFR, OFA, TFR, TFA commands allocated by IANA is 16777313 and that for ALR, ALA commands is 16777312.   
  
SMSF shall provide a mechanism to filter incoming Diameter messages on the SGd interface based on the Application IDs and command codes.

In particular, SMSF shall provide a mechanism:

1) To filter incoming Diameter messages on the SGd interface at the Application layer of the stack ISO/OSI.

2) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:

- Discard: the matching message is discarded; no subsequent rules are applied and no answer is sent back.

- Accept: the matching message is accepted.

- Account: the matching message is accounted for i.e., a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

3) To enable/disable the logging for each rule for troubleshooting.

4) To filter on the basis of the value(s) of any portion of the protocol header.

5) To reset the accounting.

6) To disable/enable each defined rule.

*Threat References:* TBA

*Test case:*

**Test Name**: TC\_Diameter\_SGd\_FILTERING

**Purpose:**

To verify that the Network Product provides filtering for incoming Diameter messages on the SGd interface.

NOTE 1: This test case is applicable only if network product supports Diameter SGd Interface

**Procedure and execution steps:**

**Pre-Conditions:**

- The tester has the privileges to configure Diameter filtering rules on the network product.

- The vendor declares that Diameter filtering is enabled and provides a list of the filtering rules.

- The vendor includes a guideline to configure the Diameter filtering in the documentation accompanying the network product.

- A network traffic generator or a pcap file containing the Diameter messages is available.

- A network traffic analyser on the network product (e.g., tcpdump) is available.

**Execution Steps**

1. The tester logs in the network product.

2. The tester configures the network product with the following rules:

a) Accept messages that meet the filtering rules supported by the vendor on the SGd interface.

b) Discard all other messages on the SGd interface.

c) For each rule above the accounting is also enabled.

3. The tester turns on the network traffic analyser on the SGd interface.

4. The tester sends Diameter messages to the network product by replaying a pcap file or using a network generator, ensuring that the messages pass the supported filtering rules.

a) Using the network analyser, the tester verifies that the messages are correctly received by the network product.

b) Using the accounting, the tester verifies that the messages are not discarded because response messages are sent back by the network product.

5. The tester sends Diameter messages to the network product by replaying a pcap file or using a network generator, ensuring the messages do not pass the supported filtering rules.

a) Using the network analyser, the tester verifies that the messages are discarded by the network product.

b) Using the accounting, the tester verifies that the messages are discarded and that no response is sent back by the network product.

**Expected Results:**

- For step 4 the tester receives successful Diameter response messages from the network product.

- For step 5 the tester receives no response from the network product.

- For steps 4 and 5, messages that pass and do not pass the filtering rules are correctly accounted.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- The used tool(s) name and version information

- Settings and configurations used

- Pcap trace

- Screenshot

Test result (Passed or not)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*