**3GPP TSG-SA3 Meeting #116 *S3-242633***

Jeju, Korea, 20 - 24 May 2024 Revision of *S3-242362*

**Source: Indian Institute of Technology Bombay**

**Title: Disabling Peer Discovery 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 peer discovery 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 peer discovery 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".

 [14] 3GPP TS 32.299: " Diameter charging applications "

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

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

##### 4.2.7.x Protecting from unknown peers on Diameter-based SGd interface

*Requirement Name:* Disabling peer discovery on the SGd interface

*Requirement Reference*: 3GPP TS 32.299 [14]; RFC 6733 [12], clause 5.2;

*Requirement Description*:

Capability Exchange Request (CER) and Capability Exchange Answer (CEA) are Diameter messages used on SGd interface to discover diameter nodes and know their capability. If peer discovery is enabled, an attacker can connect to the SMSF and learn about its capabilities by sending CER messages. Network products with SGd interface be configured only to accept known peers.

To protect SMSF from attacks by unknown peers (attackers), it supports the following requirements:

1. It maintains list of all trusted nodes with static IP addresses in a peer table.
2. It is configured only to respond to the CER messages from trusted nodes listed in the peer table, and it ignores CERs from all other nodes.

*Threat References:* TBA

*Test case:*

**Test Name**: TC\_DIAMETER\_SGd\_PEERDISCOVERY

**Purpose:**

To verify that the SMSF ignores requests from any unauthorized nodes that tries to discover its capabilitie

**Procedure and execution steps:**

**Pre-Conditions:**

- This test case is applicable only if the network product supports Diameter SGd Interface

- The tester has the privileges to configure network product’s peer table to include only directly connected peers with static IP addresses.

- The vendor declares that peer discovery is disabled on the network product.

**Execution Steps**

1. The tester logs in the network product.
2. The tester configures the peer tables of the network product with a list of static IP addresses.
3. The tester configures its source IP using one from the list in the network product’s peer table. The tester then sends a CER message by replaying a pcap file or using a network generator.

a) Using the network analyser, the tester verifies that the message is correctly received by the network product.

b) The tester verifies that the network product responds with a CEA.

1. The tester configures its source IP to one that is not in the peer table list of the network product. The tester then sends a CER message by replaying a pcap file or using a network generator.

a) Using the network analyser, the tester verifies that the message is discarded by the network product.

b) The tester verifies that the the network product does not respond with a CEA.

**Expected Results:**

- The network product responds with a CEA for CERs received from the peers listed in its peer table and ignores CERs from all others.

**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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*