**3GPP TSG-SA3 Meeting #116 *S3-242631***

Jeju, South Korea, 20th - 24th May 2024 Revision of *S3-242324*

**Source: Indian Institute of Technology Bombay**

**Title: Diameter Session security requirements on SGd interface for Security Assurance Specifications for SMSF**

**Document for: Approval**

**Agenda Item: 4.4**

# 1 Decision/action requested

***SA3 is kindly asked to approve the addition of requirement in draft 33.529 v0.4.0 of 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 Diameter session requirements on SMSF specific SGd interface.*

# 4 Detailed proposal

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

##### 4.2.7.x Protection of Diameter Session on SGd Interface

*Requirement Name:* Diameter session on SGd interface

*Requirement Reference:* TS 29.338 [8], clause 4.5; RFC 6733 [12], clause 8.8

*Requirement Description*:

SMSF supports implicit termination of SGd Diameter application sessions. The client (server) includes in its requests (responses) the Auth-Session-State AVP set to the value NO\_STATE\_MAINTAINED (1), as described in IETF RFC 6733 [12]. The server sets the Auth-Session-State AVP value to NO\_STATE\_MAINTAINED (1), irrespective of what value the client sets. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP be present in requests or responses [8].

To protect Diameter sessions, SMSF supports the following requirements:

1. Diameter session ID AVP be unique, i.e., uniquely identify the user session and distinguish the session from all other active sessions.

2. The session ID be generated by the Diameter application node that initiates the session.

*Threat References:* TBA

*Test Case:*

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

**Purpose:**

Verify that the above Diameter session and session ID related requirements have been met.

**Procedure and execution steps:**

**Pre-Conditions:**

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

- The Diameter application node uses a session ID to identify a session between the node and its peer.

- The documentation should describe the algorithm used to generate the session IDs, for details see Section 8.8 in RFC 6733 [12].

**Execution Steps:**

1. The tester logs in the network product.
2. The tester sends SGd application request message as follows:
   1. Auth-Session-State AVP is set to the value NO\_STATE\_MAINTAINED (1).
   2. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP is present in requests.
   3. The tester generates session ID as per the documentation and uses it as session ID AVP in the message.
3. The tester sends SGd application request message as follows:
   1. Auth-Session-State AVP is set to the value STATE\_MAINTAINED (0).
   2. Authorization-Lifetime AVP and Session-Timeout AVP are present in request.
   3. The tester generates session ID as per the documentation and uses it as session ID AVP in the message.
4. The tester checks the response for its request message in step 2 and 3. In the both cases, the tester verifies that:
   1. Auth-Session-State AVP is set to the value NO\_STATE\_MAINTAINED (1).
   2. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP is present in response.
   3. The session IDs in two request messages are different and unique.
5. The tester sends SGd application request message with same session ID in a row and checks the response.
6. The tester sends SGd application request message with different session ID in a row and checks the response.
7. The tester logs in with different user ID and sends SGd application request message with same session ID in step 2 and checks the response.

**Expected Results:**

1. A confirmation from the tester that the Auth-Session-State AVP is indeed set correctly in response messages.
2. A confirmation from the tester that the neither the Authorization-Lifetime AVP nor the Session-Timeout AVP is present in response messages.
3. In case of a duplicate or non-unique session ID, an error response is generated with Result-Code AVP as DIAMETER\_INVALID\_AVP\_VALUE 5004 and Session-ID AVP is added in Failed AVP.
4. A response message indicating success is received to the request message when session ID is unique.

**Expected format of evidence:**

A confirmation that the tester has confirmed that:

1. The session ID AVP follows the requirments 1 and 2 in the requirement description.

2. The correct Auth-Session-State, Authorization-Lifetime and Session-Timeout AVP configurations are used.

3. The network product does not accept duplicate session IDs.

Test result (Passed or not)

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