**3GPP TSG-SA3 Meeting #114e *S3-24xxxx***

Electronic meeting, online, 22 - 26 January 2024

**Source: Indian Institute of Technology Bombay**

**Title: Discussion of Diameter interface at SMSF to define requirements for Security Assurance Specifications for SMSF**

**Document for: Discussion**

**Agenda Item:**

# 1 Decision/action requested

***This discussion paper provides the detailed justifications for the existence of Diameter interfaces and requirement of new test cases for SMSF SCAS.***

# 2 References

[1] 3GPP TS 23.040 Technical realization of the Short Message Service (SMS)

[2] 3GPP TS 33.501 Security architecture and procedures for 5G system

[3] 3GPP TS 33.117 Catalogue of general security assurance requirements

[4] 3GPP TS 29.002 Mobile Application Part (MAP) specification

[5] 3GPP TS 29.338 Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)

[6] 3GPP TS 29.540 5G System; SMS Services

[7] 3GPP TS 33.926 SCAS threats and critical assets in 3GPP network product classes.

[8] 3GPP TS 33.210 Network Domain Security (NDS); IP network layer security

[9] 3GPP TS 23.501 System Architecture for the 5G System (5GS)

[10] 3GPP TS 23.540 Technical Realization of Service based Short Message Service

[11] RFC 6733 Diameter Base Protocol

[12] IR.88 EPS Roaming Guidelines

[13] FS.19 Diameter Interconnect Security

[14] CSRIC CSRIC Working Group 3 Final Report- Recommendations to Mitigate Security Risks for Diameter Networks

[15] ENISA Signalling Security in Telecom SS7/Diameter/5G, EU level assessment of the current situation, MARCH 2018.

[16] S3-171540 DESS3\_02 LS to SA3 on Info about DESS Launch

# 3 Rationale

*This paper provides insights into SMSF interfaces and the related external threats resulting in new test case. It is specifically focused on threats from Diameter interface SGd between SMSF and IP-SM-GW/SMS- router/SMS-GMSC.*

# 4 Detailed Discussion

**4.1 Introduction:**



**Figure 1: The main network structure serving as a basis for the short message transfer (Base figure courtesy 3GPP TS 23.040), with 5GS mapping. Reference point 1, 2, 3, 4, 5, and 6 are interfaces between network entities.**

According to TS 23.040 [1] “Technical Realization of Short Message Service”, SMS service is facilitated by the network entities as shown in Figure 1. For SMS in 5GS, the SMSF shall implement requirements specified for MSC and VLR. "MSC" is to be replaced with "SMSF"and "VLR" is to be replaced with "SMSF internal subscriber register".

On reference point 3, the protocols used between SMSF and SMS-GMSC/SMS-IWMSC/SMS-Router may be based on **Diameter** as specified for reference point **SGd** in TS 29.338 [5] or based on **HTTP/2 [6]** as specified for Nrouter service based interface in TS 23.540 [10] or based on **MAP** as specified in TS 29.002 [4].

Note: The SGd interface is between SMSF and SMS-GMSC/IP-SM-GW/SMS-Router as per the TS 23.501 [9] and TS 23.540 [10].

Figure 2 gives an overall picture of the SMSF interfaces, with the different network entities in the 5G system, identified in the 3GPP specifications.



**Figure 2: Interface connections between SMSF and other Network Entities**

The critical assets of a GNP described in clause 5.2 of the TR 33.926 [7] document apply to SMSF as well, the critical assets of SMSF to be protected are: SMSF Application, NF and User Data, SMSF software and SMSF interfaces. The interfaces of SMSF to be protected and which are within SECAM scope: Service based interface, Reference point interface SGd (Diameter-based), MAP-based SS7 interface, Console interface, and OAM interface. **Before proceeding with the SGd related security requirements, IIT Bombay proposes to add the critical assests assessment of SMSF in 3GPP TR 33.926 [7].**

**4.1.2 SMSF security aspects**

The SMSF interacts with both Inter-PLMN and Intra-PLMN NFs based on roaming privileges. The network domain security features cover the security concerns related with SMSF and its interactions with other NFs so that network nodes can securely exchange control information using features of this domain. In case of Service-Based Architecture (SBA) implementations (Method 1 in Figure 2), SBA domain security features are required to ensure secure communication between network functions over SBI.

Security concerns can be there for SMSF interactions with IP-SM-GW, SMS router, SMS-GMSC over MAP and Diameter-based interfaces (Method 2 and 3 in Figure 2), on which cybersecurity issues were noted [13].

**4.2 DIAMETER Interfaces- an LTE signalling protocol in 5G systems**

According to different reports [14, 15], currently the percentage of 4G subscribers are far more than the 5G subscribers. This demands inter-working between 4G and 5G domains. Suppose there is a PLMN1, where 5G is deployed, and a PLMN2 where 4G is deployed. Now, when a short message (SMS) transfer must happen between these, then PLMN1 shall be having backward compatibility to support the LTE signalling protocols, and Diameter being the most-widely used protocol.

**4.2.1 SGd Diameter Interface between SMSF and other Diameter Application nodes (GMSC/SMS-Router/IP-SM-GW):**

3GPP TS 29.338 [5] defines the Diameter interfaces specific to SMS, comprising of Diameter application for SGd between SMSF and other legacy network entities.

Diameter protocol comprises of Diameter base protocol and Diameter application part (Application being SMS in SGd scenario). In TS 29.338 [5], it is mentioned that “*Diameter base protocol as specified in IETF RFC 6733 shall apply except as modified by the defined support of the methods and the commands and Attribute Value Pairs (AVPs) result and error codes as specified in this specification”.*

These SMS application specific command codes are in addition to the Diameter base protocol command codes as detailed in clause 6.3.2.3, clause 6.3.2.4, clause 6.3.2.5 clause 6.3.2.6, clause 5.3.2.5 and clause 5.3.2.6 of TS 29.338 [5].

**4.2.2 Threats from Diameter interfaces**

Refering to a number of reports [12]-[15], we found that a vast majority of attack and fraud scenarios especially in the context of international roaming are possible because the PLMN operator that receives a signalling message from another PLMN operator cannot identify the legit origination of the message. This allows attackers to manipulate/forge/tamper the signalling messages. In a kill chain, these manipulated signalling messages may be used to commit fraud or perform a variety of attacks, allowing attackers to intercept communication, impersonate subscribers, and commit fraud. The attack extends to user data information disclosure and violation of privacy.

**4.3 Securing Diameter messages:**

SMS related traffic should be protected towards IP-SM-GW, SMS-router, and SMS-GMSC while sending/receiving through SMSF on Diameter interfaces.

As mentioned in different 3GPP documents, TS 29.338 [5] and TS 33.501 [2], for secure transport of Diameter messages, the IPsec/TLS profiles mentioned in 3GPP TS 33.210 shall be used. The cipher suites mentioned in RFC 6733 [11] are discouraged to use according to TS 33.501 [2]. Using these security mechanisms, each connection can be authenticated and can be replay and integrity protected.

In addition to authenticating each connection, the entire session MUST also be authorized. The requirement of Diameter peer authorization is important as the Diameter peers may be authentic, but that does not mean that they are authorized to act as a Diameter server advertising a set of Diameter applications.

Note: Authorization related aspects have not been covered in the current study and would be taken up later.

**IIT Bombay’s proposal is to introduce the protection of SGd DIAMETER interface as a requirement and its related test case for the SCAS for SMSF (TS 33.529 V0.2.0).**