Subject: ***Notice for seeking stakeholder inputs on the DFC (Draft For Comment) of Indian Telecom Security Assurance Requirements (ITSAR) for 5G-Short Message Service Function (5G-SMSF)***

Dear Stakeholders,

In exercise of the powers conferred by Section 7 of the Indian Telegraph Act, 1885 (13 of 1885), the Central Government amended the Indian Telegraph Rules, 1951 to insert Rule 528 to 537 in Part XI under the heading Testing & Certification of Telegraph. The new rules provide that every telecom equipment must undergo prior mandatory testing and certification.

2. Telecom Engineering Centre (TEC) came out with Procedure for Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) in December 2017. The MTCTE document outlines the procedure to operationalise the new Rules.

3. The testing and certification described in the MTCTE procedure document requires that the equipment meets the Essential Requirements (ER). Security Requirement is part of ER for which the equipment must be tested and certified against. The responsibility for framing Security requirements and for Security testing and certification lies with National Centre for Communication Security (NCCS), a centre under Department of Telecommunications headquartered at Bengaluru.

4. Security Assurance Standards (SAS) vertical under NCCS is responsible for drafting and finalizing ITSARs for communication equipment. In this regard, an online meeting is scheduled for discussion with the stakeholders (TSPs, CSPs,OEMs, prospective labs, industry bodies, and academia) on the Draft ITSAR for **Short Message Service Function (SMSF)** . The details of the online meeting and registration link are as follows:

- Date of meeting: 23.08. **2023 (at 10:30 hrs onwards)**
- Registration link: will be shared later

The comments received from stakeholders will form the basis for discussion. Stakeholders are hereby requested to participate in the above meeting & send their suggestions/comments/inputs to the following e-mail addresses on or before 11.08. **2023**

1) Shri R. Babu Srinivasa Kumar Director (SAS-II), NCCS – dirnccs5.bg-dot@ gov.in
2) Ms. Adepu Mounika ADET-I (SAS-II), NCCS - adet1sasf.nccs-dot@gov.in

In case of any queries, Please call Sh.R. Babu Srinivasa Kumar, at +91 9444000960 or Ms. Adepu Mounika at +91 77804 39890

Thanks and regards

R. Babu Srinivasa Kumar
Director(SAS-II)
O/o Sr DDG(NCCS), NCCS, DoT, Bengaluru-27.

सत्यमेव जयते

Indian Telecom Security Assurance Requirements (ITSAR)

Short Message Service Function (SMSF) of 5G

NCCS/ITSAR/Core Equipment/5G sub systems/Short Message Service Function (SMSF)

(ITSAR No: ITSAR11123YYMM)

NCCS

Securing Networks

Draft For Comments (DFC)

Release Date: Version: 1.0.0
Date of Enforcement:

Security Assurance Standards Facility (SASF) Division
National Centre for Communication Security (NCCS), Bengaluru
Department of Telecommunications, Bengaluru-560027

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

S.no	Title	ITSAR no	Version	Date of release	Remark
1.	Short Message service Function (SMSF) of 5G	ITSAR11123YYMM	1.1.0		

Contents

A) Outline

The objective of this document is to present a comprehensive, country-specific security requirements for the Short Message Service Function (SMSF) of 5G Core. As an anchor point for Short Message (SM), SMSF terminates the interfaces from AMF, UDR and Service Center Gateway/Interworking SMS Router. Its main functionalities include SMS subscription management, Relaying of SMs, SMS charging, support for Lawful Intercept and interaction with other functions regarding notifications. 5GS provides SMS support through both 3rd Generation Partnership Project (3GPP) and non-3GPP accesses.

The specifications produced by various regional/ international standardization bodies/ organizations/associations like 3GPP, International Telecommunications Union-Telecommunications Sector (ITU-T), International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), , Internet Engineering Task Force (IETF), , Internet Research Task Force (IRTF), GSM Association (GSMA), Telecommunications Standards Development Society India (TSDSI) along with the country-specific security requirements are the basis for this document. The Telecommunication Engineering Center (TEC)/TSDSI references made in this document implies that the respective clause has been adopted as it is or with certain modifications.

This document commences with a brief description of 5G system architecture, SMSF and its functionalities and then proceeds to address the common and entity specific security requirements of SMSF.

B) Scope

This document targets on the security requirements of the 5G Core SMSF network function. This document does not cover the security requirements at the virtualization and infrastructure layers. Remote Access regulations are governed by the Licensing Wing of Department of Telecommunications (DoT).

C) Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above.

CHAPTER 1 – OVERVIEW

1.1 Introduction

The fifth generation of mobile technologies (5G) is expected to connect people, things, data, applications, transport systems and cities in a smart networked communication environment. 5G is standardized by the 3rd Generation Partnership Project (3GPP) and the requirements framework for 5G are specified by ITU under IMT-2020. The usage scenarios/use cases identified for 5G are i) Enhanced Mobile Broadband (eMBB) ii) Massive Machine Type Communication (mMTC) and iii) Ultra Reliable and Low Latency Communications (URLLC).

1.2 5G Architecture

The 5G architecture supports various service deployments by using techniques like Software Defined Networking (SDN) and Network Function Virtualization (NFV). The generic 5G system (5GS) architecture consists of User Equipment (UE), Radio Access Network (RAN), supporting 3GPP (e.g., New Radio (NR) and Evolved Universal Terrestrial Radio Access (E-UTRA)), as well as non-3GPP access (e.g., Wireless Local Area Network (WLAN)) and 5G Core Network. The 5G NR base station is called Next Generation Node B (gNB). The deployment strategies possible are Non-Stand Alone (NSA) and Stand Alone (SA). SA denotes 5G NR RAN connected to 5G Core Network. In NSA mode, 5G NR RAN (gNBs) gets connected to Fourth Generation (4G)'s Evolved Packet Core (EPC) but uses 4G Long Term Evolution (LTE) eNodeBs as anchor in the control plane.

1.2.1 5G Core Network

Core network is the central part of the mobile network. 5G Core network provides authentication, security, mobility management, session management services and allows the subscribers through access and authorization to avail the services.

These functionalities of the 5G Core Network are supported using 3GPP defined processing functions specified as "network functions". A network function can be realized in different ways, e.g., as a network element on a dedicated hardware, or as a software instance running on a dedicated hardware, or as a virtualised function instantiated on shared (cloud) infrastructure. The salient features of the 5G Core Network are as follows:

a) Separation of Control Plane and User Plane.
b) Service Based Architecture (SBA)
c) Network Slicing Support
d) Enable usage of Network Function Virtualization (NFV) and Software Defined Networking (SDN)
e) Access Agnostic
f) Framework for policy control and support of QoS
g) Secure exposure of network capability to 3rd party providers.
h) Storage of subscription data, subscriber access authentication, authorization and security anchoring

In an SBA framework, the individual elements are defined as Network Functions (NFs) instead of Network entities. Through Service Based Interface (SBI), an NF consumes services offered by other NFs. RESTful APIs are used in 5G SBA which use HTTP/2 as the application layer protocol. Service based architecture for the 5G system is shown in Figure 1 including some important core network functions.

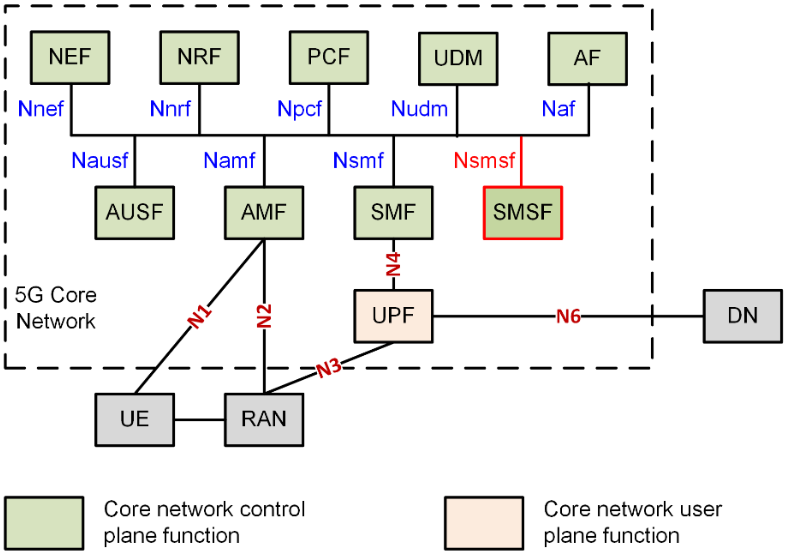

Figure 1: Service based architectural view of 5GS
[Adapted from TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

Some of the core network functions and their respective functionalities are as follows:

1) Access and Mobility Management Function (AMF): Some of the functionalities of AMF are registration management, connection management, mobility management, access authentication and authorization, termination of Non-Access Stratum (NAS) and support for Short Message Service (SMS).

2) Session Management Function (SMF): Some of the functionalities of SMF are session establishment, modification and release, UE Internet Protocol (IP) address allocation and management, charging data collection and termination of interfaces towards Policy Control Function (PCF).

3) Authentication Server Function (AuSF): AuSF resides in the Home Network. It supports UE authentication for 3GPP and non-3GPP accesses.

4) User Plane Function (UPF): Some of the UPF functionalities include packet routing and forwarding, policy enforcement and QoS handling (related to user plane part) and traffic usage reporting for user planes. It is the anchor point for UE in case of Intra or Inter RAT mobility.

5) Application Function (AF): It interacts with the 3GPP Core Network to provide services, influences traffic routing by accessing Network Exposure Function (NEF) (and possibly PCF) and by interacting with the policy framework for policy control. In case of existence of more than one PCF in the CN, it reaches the concerned PCF through Binding Support Function (BSF).

6) Network Exposure Function (NEF): Some of the functionalities of NEF are exposure of capabilities, events and analytics, and secure provisioning of information from external applications to the 5G network.

7) Network Repository Function (NRF): NRF supports service discovery function and maintains NF profiles of available NF instances and their supported services. It receives NF discovery request from NF instances and provides information of the discovered NF instances to them.

8) Policy Control Function (PCF): PCF functionalities include support for a unified policy framework to govern the network behavior. PCF provides policy rules to control plane for enforcement and accesses subscription information relevant to policy decisions from Unified Data Repository (UDR).

9) Unified Data Management (UDM): Some of the UDM functionalities are user identification handling, access authorization based on subscription data and UE's serving NF registration management.

10) Short Message Service Function (SMSF): Some of the SMSF functionalities are to support SMS over NAS, checking SMS management subscription data and conducting SMS delivery,

SMS charging, relaying message between UE and SMS-GMSC/IWMSC/SMS-Router, and Lawful Interception.

Any network function in the control plane can enable other authorized network functions to access their services using standard service-based interfaces.

Figure 2 shows reference point representation for a few functions of the core network. Point to point reference points are shown between two network functions, for example N11 between AMF and SMF.

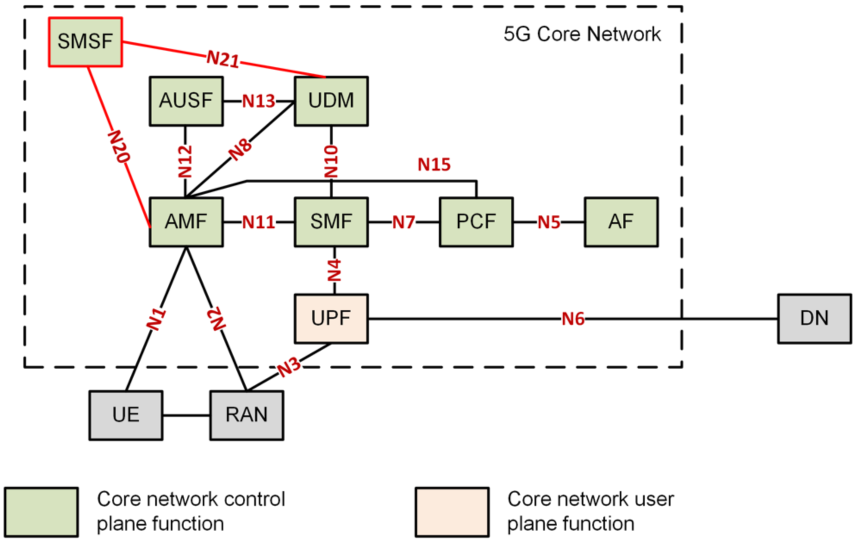

Figure 2: Reference point representation for [Adapted from TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

1.3 General Security Architecture for 5G System

The 5G System works on the principle of service-based architecture which presents the need for consideration of security aspects. Secure interactions between the network functions are governed by the security features, i.e., Confidentiality, Integrity and Availability. The architecture enabling secure communications between the network entities is shown in Figure 3.

Mobile Equipment is served by 3GPP and non-3GPP access networks to facilitate connectivity with the Core Network. When MEs are outside the coverage area of the Home Environment (their primary service provider), they are served by the Visiting Network (as serving network). When the ME is in the coverage area of its primary service provider, there will be no distinction between the Serving Network (SN) and Home Environment (HE), they will be one and the same. ME's communication with the provider network is enabled using the Universal Subscriber Identity Module (USIM).

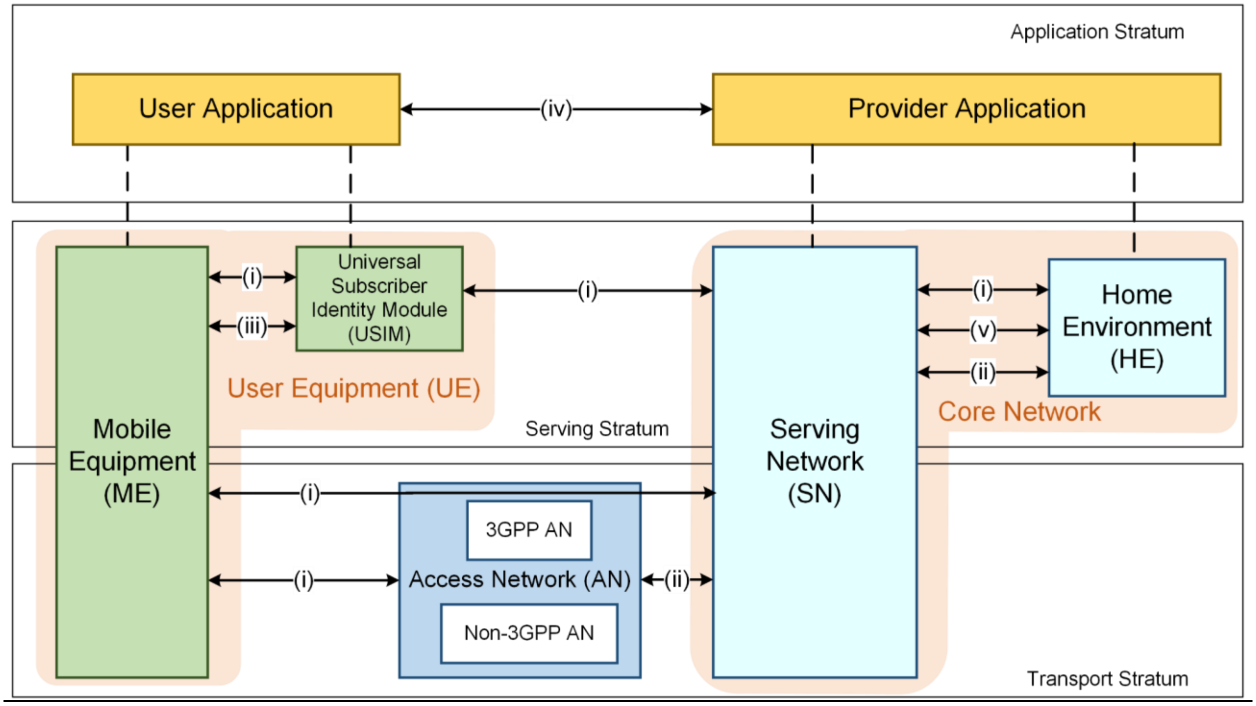

Figure 3: Overview of the security architecture [Adapted from TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0]

User Application is the application layer in the UE, which facilitates user interaction with provider application. Provider Application communicates with the user application using the logical link established through the 5G System.

The security features and the security mechanisms for the 5G System and the 5G Core can be categorized in following domains:

i) Network Access security: UEs are authenticated and provided access to the network using security features of this domain. It provides secure access via the 3GPP and non-3GPP networks, in particular protects radio interfaces against attacks. In addition, it includes security context delivery from Serving Network (SN) to Access Network (AN) to support access security.

ii) Network Domain security: The security features of this domain allow network nodes to securely exchange signaling data and user plane data.

iii) User domain security: Users can securely access the mobile equipment using security features of this domain.

iv) Application domain security: The features of this security domain facilitate secure exchange of messages between applications in user domain and provider domain.

v) SBA domain security: The security features of this domain facilitate secure communication between NFs over the service-based interfaces within the serving network domain and other network domains.

vi) Visibility and configurability of security: The security features of this domain provide information about availability of security features to the user. This domain is not shown in the figure.

The common and specific security requirements of the Short Message Service Function (SMSF) are covered in the present document. SMSF is also a part of the 5G core network whose functionalities are associated with the Short Message Service (SMS). The following sections cover the overview of the SMS support in 5GS, SMSF functionalities, and SMSF security aspects.

1.4 Short message service (SMS)

This service is a means to transfer short messages between a UE and a Short Message Entity (SME) via a Service Center (SC) through the 5GS. The SC serves as an interworking and relaying function for message transfer between the UE and the SME. Short messages have limited length and can be sent as a payload through NAS signaling in the 5GS (if SMS over NAS is supported by the 5GS). The Short Message (SM) is of following two types based on the origination and termination of the message.

SM MT (Short Message Mobile Terminated): SM MT denotes the short message destined to a UE. For this type of message, a delivery report is sent by UE to provide SM transfer status (success/failure).

SM MO (Short Message Mobile Originated): SM MO denotes the short message originating at a UE and destined to an SME via an SC. For this type of message, a delivery report is sent by SC to provide SM transfer status (success/failure).

1.4.1 Support of SMS over NAS in 5GS

If a UE wants to use SMS and can support SMS over NAS, it provides “SMS supported” indication to the AMF during registration. If 5GS also supports SMS via NAS functionality, the AMF includes “SMS allowed” in the response as an indication to UE that SMS delivery over NAS is accepted by the network.

Following are the features to support SMS over NAS in 5GS:

i) There is support for SMS over NAS transport between UE and AMF.
ii) This applies to both 3GPP and Non 3GPP accesses.
iii) There is support for AMF determining the SMSF for a given UE
iv) There is support for subscription checking and actual transmission of MO/MT-SMS transfer by the SMSF.
v) There is support for MO/MT-SMS transmission for both roaming and non-roaming scenarios.
vi) There is support for selecting proper domains (over NAS or through IMS) for MT SMS message delivery including initial delivery and re-attempting in other domains.

Note: Domain selection is supported by connecting SMSF to IP-Short Message-Gateway (IP-SM-GW) via standardized interface.

1.5 Short Message Service Function (SMSF)

Short Message Service Function (SMSF) is a dedicated function in the 5G core network to support some SMS specific functionalities and to interact with SC gateway/interworking SC router for relaying short messages between UE and SC. If SMS over NAS is supported by both 5GS and UE, AMF allocates an SMSF instance to manage the short messages for a UE. AMF checks with UDM on the SMS subscription status of a UE. If SMS is allowed for the UE, AMF includes an SMSF address to the stored UE context. AMF uses that SMSF address for providing SM services to the UE. Otherwise, the AMF discovers and selects an SMSF to serve the UE.

Functionalities of SMSF are as follows:

i) It handles SMS management subscription data checking (with SC and UDM) and conducts SMS delivery accordingly.

ii) It supports SM Relay Protocol (RP)/ SM-Control Protocol (CP) with the UE [3GPP TS 24.011].

iii) It relays the SM from UE towards SMS-gateway/router.

iv) It relays the SM from SMS-interworking/router towards the UE.

v) It supports SMS charging related aspects.

vi) It supports Lawful interception for SMS.

vii) It interacts with AMF and SMS-Gateway Mobile-Services Switching Center (MSC) for notifying if the UE is unavailable for SMS transfer (further SMS-Gateway MSC informs UDM regarding UE unavailability).

1.5.1 Architectural representation for SMS over NAS support

Architectural representation including network functions to support SMS over NAS using service-based interfaces for non-roaming and roaming scenarios are shown in Figures 3 and 4 respectively.

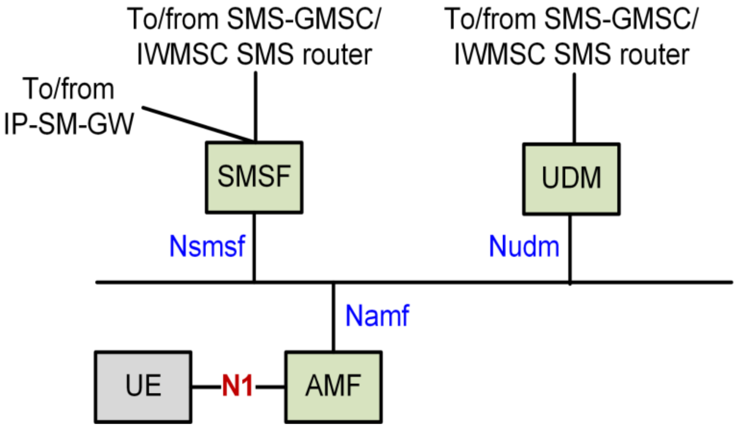
To/from SMS-GMSC/ IWMSC SMS router
To/from SMS-GMSC/ IWMSC SMS router
To/from IP-SM-GW
SMSF
UDM
Nsmsf
Nudm
Namf
UE
N1
AMF

Figure 3: Non-roaming architecture for SMS over NAS support in 5GS [Ref: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

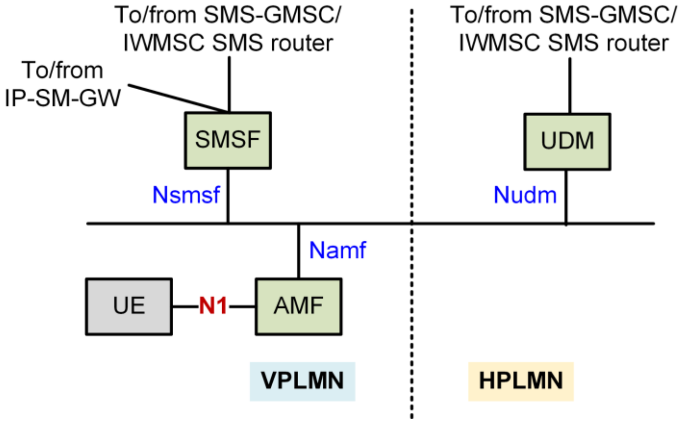
To/from SMS-GMSC/ IWMSC SMS router
To/from SMS-GMSC/ IWMSC SMS router
To/from IP-SM-GW
SMSF
UDM
Nsmsf
Nudm
Namf
UE
N1
AMF
VPLMN
HPLMN

Figure 4: Roaming architecture for SMS over NAS support in 5GS [Ref: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

Reference point representation for network functions to support SMS over NAS for non-roaming and roaming scenarios are shown in Figures 5 and 6 respectively.

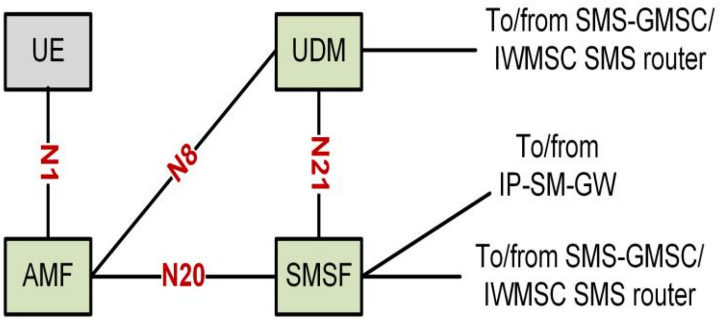

Figure 5: Reference point representation for SMS over NAS support in 5GS (Non roaming) [Ref: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

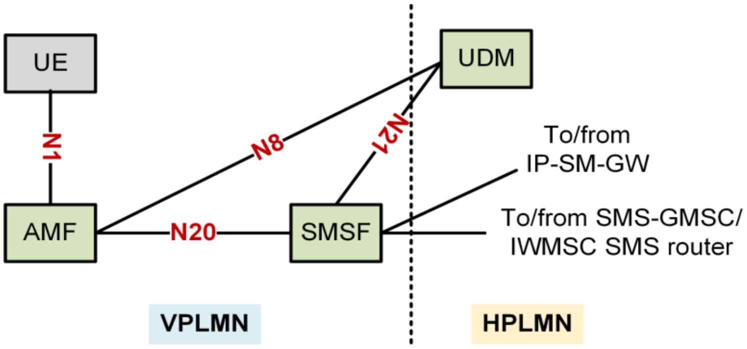

Figure 6: Reference point representation for SMS over NAS support in 5GS (Roaming) [Ref: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

N1 is a reference point for communication between UE and AMF via NAS. Following reference points are realized by service-based interfaces: N8 is a reference point for SMS subscription data retrieval between AMF and Unified data management (UDM), N20 is a reference point for SMS transfer between AMF and SMSF, and N21 is a reference point for SMSF address registration management and SMS management subscription data retrieval between SMSF and UDM.

1.5.1.1 Coexistence with Legacy System

5G SMS over NAS may expose SMSF to security vulnerabilities of MAP or Diameter based interfaces when an SMSF interoperates with legacy 3G/4G system entities, as shown in Figure 7.

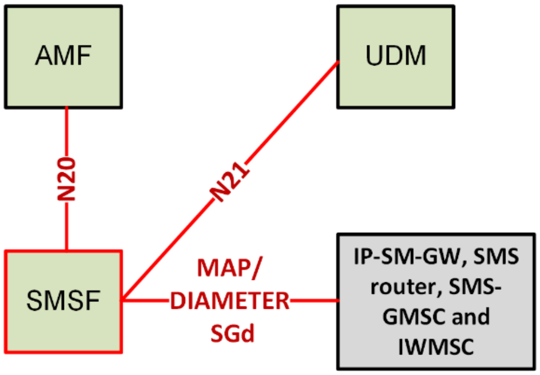

Figure 7: SMSF Interfaces with Legacy Systems
[Adapted from: GSMA, NG.111, "SMS Evolution"]

1.6 SMSF security aspects

The SMSF interacts with a number of Network functions (as shown in Figures 3 and 4) both inter PLMN and Intra-PLMN NFs based on roaming privileges. The network domain security features can cover the security concerns related with SMSF and its interactions with other NFs so that network nodes can securely exchange control and user plane data using features of this domain.

In case of SBA based implementations, SBA domain security features are required to ensure secure communication between network functions over SBI.

Other than SMSF interactions and security concerns between NFs (AMF and UDR), security concerns can be there for SMSF interactions with IP-SM-GW, SMS router, SMS-GMSC and IWMSC. SMS related traffic shall be protected towards IP-SM-GW, SMS router, SMS-GMSC and IWMSC IP-SM-GW, SMS router and SMSCs while sending/receiving through SMSF on MAP and Diameter interfaces.

There is also a provision to support Service based Short Message Service (SBI-SMS) in the 5G system (5GS) [TSDSI STD T1.3GPP 23.540-17.1.0 V1.1.0 Section 4.1] as shown in Figure 8. Ngmsc, Niwmsc, Nipsmgw, and Nrouter are the additional SBIs which facilitate service-based SMS support towards entities IP-SM-GW, SMS router, SMS-GMSC and IWMSC.

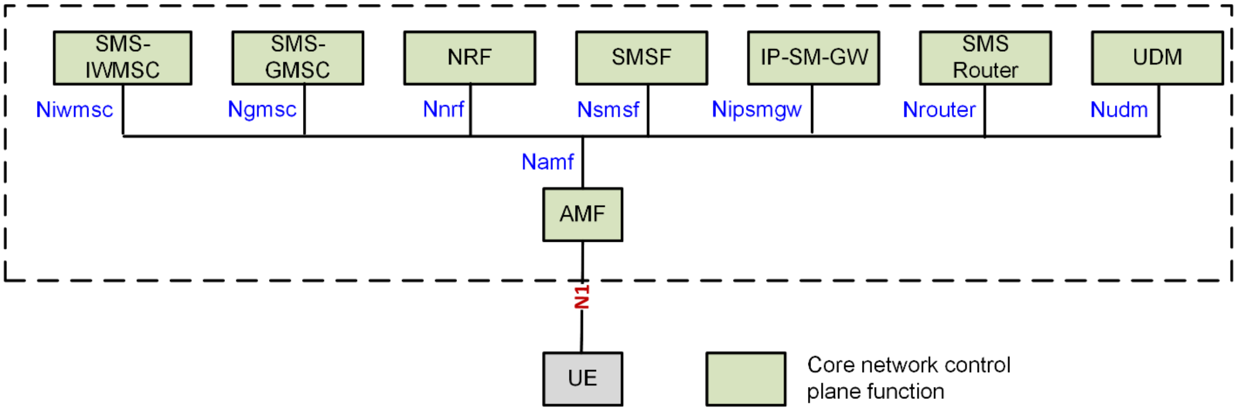

Figure 8: SBI-based SMS Architecture [Ref: TSDSI STD T1.3GPP 23.540-17.1.0 V1.1.0 Section 4.1]

Security of the SMSF data, like SMS Record Data and UE SMS context data and its access aspects needs due consideration. SMSF also has Lawful Interception (LI) capabilities to generate Intercept Related Information (xIRIs) when SMS related to the target UE are handled. The IRI-Point of Interception (POI) present in the SMSF detects the target UE's SMS, generates and delivers the xIRI to the LI entities.

Note: On the network side, for SMS over NAS via any access (3GPP/non-3GPP) when UE has already activated NAS security with AMF before sending/receiving SMS, NAS transport message shall be ciphered, and integrity protected using the NAS security context by UE/AMF.

The next sections cover the common and SMSF-specific security requirements within the context of these domains.

CHAPTER 2- COMMON SECURITY REQUIREMENTS

2.1 Access and Authorization

2.1.1 Authentication for Product Management and Maintenance interfaces

Requirement:

There is mutual authentication of entities for management interfaces on SMSF, the authentication mechanism can rely on the management protocols used for the interface or other means.

Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecom Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used for SMSF management and maintenance.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0 Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

SMSF management traffic (information exchanged during interactions with OAM) shall be protected strictly using secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.2.4]

2.1.3 Role-based access control policy

Requirement:

SMSF shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that determines how users interact with domains and resources. The RBAC system controls how users or groups of users are allowed access to the various domains (the domains could be Fault Management, Performance Management, System Admin, etc.) and what type of operation they can perform, i.e., the specific operation command or command group (e.g., View, Modify, Execute). SMSF supports RBAC with minimum of 3 user roles, in particular, for OAM privilege management for SMSF Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.6.2]

Note: The reference to Console interface may not be applicable here for Generalized Virtual Network Product (GVNP) Models of Type 1& 2

2.1.4 User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, enables unambiguous authentication and identification of the authorized user.
Authentication attributes include

a) Cryptographic keys
b) Token
c) Passwords

This means that authentication based on a parameter that can be spoofed (e.g., phone numbers, public IP addresses or Virtual Private Network (VPN) membership) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker. Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

Direct Login to SMSF as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to SMSF remotely.

This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the SMSF.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.3.2.6]

2.1.5 Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.

Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g., configuration and logging files).

Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.6 Unambiguous identification of the user & group accounts

Requirement:

Users shall be identified unambiguously by the SMSF.

SMSF shall support the assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.

SMSF shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.1.2]

2.2 Authentication Attribute management

2.2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.1.1]

Note: The reference to 'Local access' and 'Console' may not be applicable here for GVNP Models of Type 1& 2

2.2.2 Authentication Support – External

Requirement:

If the SMSF supports external authentication mechanism such as AAA server (for authentication, authorization, and accounting services), then the communication between SMSF and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:

A protection against brute force and dictionary attacks that hinder authentication attribute (i.e., password) guessing shall be implemented in SMSF.
Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.

Various measures or a combination of the following measures can be taken to prevent this:

a) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
b) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.
c) Using an authentication attribute blacklist to prevent vulnerable passwords.
d) Using Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to prevent automated attempts (often used for Web applications).

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by SMSF. An exception to this requirement is machine accounts.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

a) The configuration setting shall be such that SMSF shall only accept passwords that comply with the following complexity criteria:

- i) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the SMSF). It shall not be possible setting this absolute minimum length to a lower value by configuration.
- ii) Password shall mandatorily comprise all the following four categories of characters:
    1) at least 1 uppercase character (A-Z)
    2) at least 1 lowercase character (a-z)
    3) at least 1 digit (0-9)
    4) at least 1 special character (e.g. @;!$.)

b) The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.
c) If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.

d) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the SMSF.
e) When a user is changing a password or entering a new password, SMSF /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g., application-level, OS-level, etc.).

Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.3.1]

2.2.5 Inactive Session timeout

Requirement:

An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.

SMSF shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on pre-configured timers. Unlocking the session shall be permissible only by user authentication. If the inactivity period further continues for a defined period, session /user ID time out must occur after this inactivity.

Reauthentication of the OAM user shall be repeated following any period of inactivity lasting 15 minutes or longer.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used, it shall be possible to implement this function on this system.

Password change shall be enforced after initial login (after successful authentication).

SMSF shall enforce password change based on password management policy. In particular, the system shall enforce password expiry.

SMSF shall support a configurable period for expiry of passwords. Previously used passwords shall not be allowed up to a certain number (Password History). The number of disallowed previously used passwords shall be:

a) Configurable;
b) Greater than 0;
c) And its minimum value shall be 3. This means that the SMSF shall store at least the three previously set passwords. The maximum number of passwords that the SMSF can store for each user is up to the manufacturer.

When a password is about to expire, a password expiry notification shall be provided to the user.

Above requirements shall be applicable for all passwords used (e.g., application-level, OS level, etc.). An exception to this requirement is machine accounts.

SMSF to have an in-built mechanism to support this requirement.

If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause. And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the SMSF.

The minimum password age shall be set as one day i.e., recycling or flipping of passwords to immediate return to favorite password is not possible.

The password shall be changed (need not be automatic) based on key events including, not limited to

- Indication of compromise (IoC)
- Change of user roles
- When a user leaves the organization

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.3.2]
[Ref [34]: CIS Password Policy guide]

2.2.7 Protected Authentication feedback

The Authentication attribute shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "*".

This requirement shall be applicable for all passwords used (e.g., application-level, OS-level, etc.). An exception to this requirement is machine accounts.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, Original Equipment Manufacturer (OEM) or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the OEM provides instructions on how to manually change it.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:

The system shall have a function that allows a signed-in user to logout at any time. All processes under the logged-in user ID shall be terminated on logout. SMSF shall be able to continue to operate without interactive sessions.

Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement Description:

a) The maximum permissible number of consecutive failed user account login attempts shall be configurable by the operator. The definition of the default value set at manufacturing time for maximum number of failed user account login attempts shall be less than or equal to 8, typically 5. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user, there shall be a block delay in allowing the user to attempt login again. This block delay and the capability to set a period of the block delay, e.g., double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure should be configurable by the operator. The default value set at manufacturing time for this delay shall be greater than or equal to 5 sec.

b) If supported, infinite (permanent) locking of an account that has exceeded the maximum permissible number of consecutive failed user account login attempts shall also be possible via configuration, with the exception of administrative accounts which shall get only temporarily locked.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.4.5]

2.2.11 Suspend accounts on non-use

Requirement:

It shall be possible for the system to automatically suspend an account after ‘X’ days without a valid login.

Note: X may be specified by operator. It can be implemented centrally also.

[Ref [34]: CIS Password Policy Guide]

2.3 Software Security

2.3.1 Secure Update

Requirement:

a) Software package integrity shall be validated during software update stage.
b) SMSF shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, SMSF has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update is originated from only these sources.
c) Tampered software shall not be executed or installed if integrity check fails.
d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in (b) above.

Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

a) Software package integrity shall be validated during software upgrade stage.
b) SMSF shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, SMSF has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software upgrade is originated from only these sources.
c) Tampered software shall not be executed or installed if integrity check fails.
d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade, and modify the list mentioned in (b) above.

Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at Telecom Security Testing

Laboratory (TSTL) premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).

b) Also, OEM shall submit the undertaking as below:

i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the SMSF software which includes OEM developed code, third party software and opensource code libraries used/embedded in the SMSF.

ii) SMSF software shall be free from Common Weakness Enumeration (CWE) top 25, Open Worldwide Application Security Project (OWASP) top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.

iii) The binaries for SMSF and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

[Ref [10]: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html]
[Ref [11]: https://owasp.org/www-project-top-ten/]
[Ref [12]: https://owasp.org/www-project-api-security/]

2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that SMSF is free from all known malware and backdoors as on the date of offer of SMSF to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the SMSF to the designated TSTL.

2.3.5 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the SMSF shall not be present.

Orphaned software components /packages shall not be present in SMSF.

OEM shall provide the list of software that are necessary for SMSF's operation. In addition, OEM shall furnish an undertaking as "SMSF does not contain software that is not used in the functionality of SMSF."

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:

SMSF shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on SMSF by the vendor except if services are needed during deployment. In that case those services shall be disabled according to vendor's instructions after deployment is done. Disabled protocols may still need to be enabled for other reasons by the operators, e.g., remote diagnostics.

SMSF shall not support following services:

a) File Transfer Protocol (FTP)
b) Trivial File Transfer Protocol (TFTP)
c) Telnet
d) rlogin, Rate Control Protocol (RCP), Remote Shell Protocol (RSH)
e) HTTP
f) Simple Network Management Protocol (SNMP)v1 and v2
g) SSHv1
h) Transmission Control Protocol (TCP)/ User Datagram Protocol (UDP) Small Servers (Echo, Chargen, Discard and Daytime)
i) Finger
j) Bootstrap Protocol (BOOTP) server
k) Discovery protocols (Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP))
l) IP Identification Service (Identd)
m) Packet Assembler/Disassembler (PAD)
n) Maintenance Operations Protocol (MOP)

Any other protocols, services that are vulnerable are also to be permanently disabled.

Full documentation of required protocols and services (communication matrix) of the SMSF and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

The SMSF can boot only from the memory devices intended for this purpose.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section- 4.2.3.3.2]

Note: This may not be applicable here for GVNP Models of Type 1& 2.

2.3.8 Secure Time Synchronization

Requirement:

SMSF shall establish secure communication channel with the Network Time Protocol (NTP)/ Precision Time Protocol (PTP) server.

SMSF shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with NTP/PTP server.

SMSF shall generate audit logs for all changes to time settings.

Note: RFC 8915 [12] which proposes Network Time Security (NTS) as an extension field for the NTP version 4 is also permitted.

2.3.9 Restricted reachability of services

Requirement:

The SMSF shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers. This limitation shall be realized on the SMSF itself (without measures (e.g., firewall at network side) according to the requirement detailed in section 2.7.1 Traffic Filtering.

Administrative services (e.g., SSH, Hyper Text Transfer Protocol Secure (HTTPS), Remote Desktop Protocol (RDP)) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.3.2.2]

2.3.10 Self Testing

Requirement:

The SMSF's cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up during System bootup/restart. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

2.4 System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e., the software and hardware functions which are not needed for operation or functionality of the SMSF shall be permanently deactivated. Permanently means that they shall not be reactivated again after the SMSF system's reboot. If unused functions of software cannot be deleted or uninstalled individually as required in clause "2.3.5 No unused software" of the present document, such functions shall be deactivated in the configuration of system permanently.

The list of hardware and software functions installed in the system shall match with the ones that have been mentioned and deemed necessary for the operation of the SMSF.

EXAMPLE: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the SMSF network product.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.3.2.4]

Note: The reference to hardware may not be applicable here for GVNP Models of Type 1& 2.

2.4.2 No unsupported components

Requirement:

OEM to ensure that the SMSF shall not contain software and hardware components that are no longer supported by them or their 3rd Parties (e.g., vendor, producer or developer) including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be provided by OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.3.2.5]

Note: The reference to hardware may not be applicable here for GVNP Models of Type 1& 2.

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

SMSF shall not contain any access mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM as follows:
"The SMSF does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel."

2.5 User Audit

2.5.1 Audit trail storage and protection

Requirement:

The security event log shall be access-controlled (file access rights) such only privileged users have access to the log files.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

SMSF shall log all important Security events with unique System Reference details as given in the Table below.

SMSF shall record within each audit record at least information pertaining to date and time of the event, type of event, subject identity, protocol, service, or program used for access, source and destination IP addresses & ports, and the outcome (success or failure) of the event.

Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event Types (Mandatory or Optional)	**Description**	**Event data to be logged**
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to SMSF	Username
		Source (IP address) if remote access
		Outcome of event (Success or failure)
		Timestamp
Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username
		Timestamp
		Length of session
		Outcome of event (Success or failure)
		Source (IP address) if remote access
Account administration (Mandatory)	Records all account administration activity, i.e., configure, delete, copy, enable, and disable.	Administrator username
		Administered account
		Activity performed (configure, delete, enable and disable)

		Outcome of event (Success or failure)
		Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded
		Value reached
		(Here suitable threshold values shall be defined depending on the individual system.)
		Outcome of event (Success or failure)
		Timestamp
Configuration change (Mandatory)	Changes to configuration of the SMSF	Change made
		Timestamp
		Outcome of event (Success or failure)
		Username
Reboot/shutdown /crash (Mandatory)	This event records any action on the network device/ SMSF that forces a reboot or shutdown OR where the network device/ SMSF has crashed.	Action performed (boot, reboot, shutdown, etc.)
		Username (for intentional actions)
		Outcome of event (Success or failure)
		Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the network device/ SMSF (e.g., shutdown)	Interface name and type
		Status (shutdown, down, missing link, etc.)
		Outcome of event (Success or failure)
		Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	Administrator username
		Administered account
		Activity performed (group added or removed)

		Outcome of event (Success or failure)
		Timestamp
Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	Administrator username
		Administered account
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service Identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure update (Optional)	Attempt to initiate manual update, initiation of update, completion of update	User identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	Old value of time
		New value of time
		Timestamp
		Origin of attempt to change time (e.g. IP address)
		Subject identity

		Outcome of event (Success or failure)
		User identity
Session unlocking /termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session	User identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Audit data changes (Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure)
		Subject identity
		User identity
		Origin of attempt to change time (e.g. IP address)
		Details of data deleted or modified
User Login and logoff (Mandatory)	All use of Identification and authentication mechanisms	User identity
		Origin of attempt (IP address)

		Outcome of event (Success or failure)
		Timestamp

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:

a) SMSF shall support (preferably immediate) forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through diverse links.

b) Log functions should support secure uploading of log files to a central location or to a system external for SMSF.

c) SMSF shall be able to store the generated audit data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit data. Service Provider/OEM shall submit justification document for sufficiency of local storage requirement.

d) Secure Log export shall comply with the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.6.2]

2.5.4 Logging access to personal data

Requirement:

In some cases, access to personal data in a clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes, such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.2.5]

2.6 Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:

SMSF shall communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

OEM shall submit to TSTL, the list of the connected entities with SMSF and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing communication with each entity and any other details required for verifying this requirement.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the SMSF (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the SMSF (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards."

[Ref [21]: ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019]

[Ref [14]: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf]

2.6.3 Cryptographic Algorithms implementation Security Assurance

Requirement:
Cryptographic algorithm implemented inside the Crypto module of SMSF shall be in compliance with the respective FIPS standards (for the specific crypto algorithm).

Till further instructions, this clause will be considered ‘complied’ by submission of an undertaking by the OEM in specified format along with self-certified test reports.
An undertaking is to be submitted by the OEM mentioning that “Cryptographic algorithms implemented inside the Crypto module of SMSF is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the SMSF).”

2.6.4 Protecting data and information – Confidential System Internal Data Requirements

Requirement:

a) When SMSF is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.

Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e., PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration.

b) Access to maintenance mode shall be restricted only to authorized privileged user.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.2.2.]

2.6.5 Protecting Data and Information in Storage

Requirement:

a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of SMSF system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” with appropriate non-repudiation controls.

b) In addition, the following rules apply for:

i) Systems that need access to identification and authentication data in the clear/readable form e.g., in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.

ii) Systems that do not need access to sensitive data (e.g., user passwords) in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.

iii) Stored files in the SMSF: Shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

a) Without authentication & authorization and except for specified purposes, SMSF shall not create a copy of data in use or data in transit.

b) Protective measures should exist against use of available system functions / software residing in SMSF to create copy of control plane and user plane data for illegal transmission.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement:

a) SMSF shall have mechanisms to prevent data exfiltration attacks for theft of control plane and user plane data in use and data in transit.

b) Establishment of outbound overt channels such as, HTTPS, Instant Messaging (IM), Peer-to-peer (P2P), Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the SMSF.

c) Session logs shall be generated for establishment of any session initiated by either user or SMSF.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) SMSF shall have mechanisms to prevent data exfiltration attacks for theft of control plane and user plane data in use and data in transit (with in its boundary).

b) Establishment of outbound covert channels and tunnels such as Domain Name System (DNS) Tunnel, HTTPS Tunnel, Internet Control Message Protocol (ICMP) Tunnel, Transport Layer Security (TLS), Secure Sockets Layer (SSL), SSH, Internet Protocol Security (IPsec), Virtual Private Network (VPN), Real-time Transfer Protocol (RTP) Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the SMSF.

c) Session logs shall be generated for establishment of any session initiated by either user or SMSF system.

2.6.9 System robustness against unexpected input

Requirement:

During transmission of data to a system it is necessary to validate input to SMSF before processing. This includes all data which is sent to the system. Examples of this are user input, inputs from SMSF's NF consumers – AMF and UDM, values in arrays and content in protocols. The following typical implementation error shall be avoided:

a) No validation on the lengths of transferred data
b) Incorrect assumptions about data formats
c) No validation that received data complies with the specification
d) Insufficient handling of protocol errors in received data
e) Insufficient restriction on recursion when parsing complex data formats
f) White listing or escaping for inputs outside the values margin

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. section 4.2.3.3.4]

2.6.10 Security of backup data

Requirement:

The service provider shall have an effective backup strategy in place and that it is well documented. Such backup copies of a particular SMSF data shall be encrypted using cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls".

[Ref [27]: "Security Guidance for 5G Cloud Infrastructure Part III: Data Protection" by NSA & CISA]

2.6.11 Secure destruction of data

Requirement:

SMSF shall be configured to securely erase sensitive data in the event of intentional deletion to prevent it from unauthorized access and replication of information. E.g., the hypervisor should be configured to securely erase the virtual volume disks in the event of application crashes or is intentionally destroyed to prevent it from unauthorized access.

[Ref [27]: "Security Guidance for 5G Cloud Infrastructure Part III: Data Protection" by NSA & CISA]

2.7 Network Services

2.7.1 Traffic Filtering – Network Level Requirement

Requirement:
SMSF shall provide a mechanism to filter incoming traffic on any interface. (Refer to RFC 3871)

In particular the SMSF shall provide a mechanism:

a) To filter incoming traffic on any interface at Network Layer and Transport Layer of the stack ISO/Open Systems Interconnection (OSI).

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

i) Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
ii) Accept: the matching message is accepted.
iii) 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.

c) To enable/disable for each rule the logging for Dropped packets, i.e., details on messages matching the rule for troubleshooting.

d) To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.

e) To reset the accounting.

f) The SMSF shall provide a mechanism to disable/enable each defined rule.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.6.2.1]
[Ref [17]: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

Requirement:

The SMSF shall support the physical or logical separation of traffic belonging to different network domains. For example, OAM traffic and control plane traffic belong to different network domains. Refer to RFC 3871 for further information.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.5.1]
[Ref [17]: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection – Anti-Spoofing

Requirement:

SMSF shall not process IP Packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.3.1.1]

2.8 Attack Prevention Mechanism

2.8.1 Network Level and application - level DDoS

Requirement:

SMSF shall have protection mechanism against Network level and Application-level Distributed Denial of Service (DDoS) attacks.

SMSF shall provide security measures to deal with overload situations which may occur as result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Potential protective measures include:

a) Restricting of available RAM per application
b) Restricting of maximum sessions for a Web application
c) Defining the maximum size of a dataset
d) Restricting Central Processing Unit (CPU) resources per process
e) Prioritizing processes
f) Limiting of amount or size of transactions of a user or from an IP address in a specific time range
g) Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:

SMSF shall act in a predictable way if an overload situation cannot be prevented. SMSF shall be built in this way that it can react on an overload situation in a controlled way.

However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that SMSF cannot reach an undefined and thus potentially insecure, state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

OEM shall provide a technical description of the SMSF's Overload Control mechanisms. (especially whether these mechanisms rely on cooperation of other network elements e.g. RAN).

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.3.3]

2.8.3 Interface robustness requirements

Requirement:

SMSF shall not be affected in its availability or robustness by incoming packets from other network elements that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of the SMSF. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.

Examples of such packets are:

a) Mass-produced TCP packets with a set Synchronize (SYN) flag to produce half-open TCP connections (SYN flooding attack).
b) Packets with the same IP sender address and IP recipient address (Land attack).
c) Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
d) Fragmented IP packets with overlapping offset fields (Teardrop attack).
e) ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IPv4 packets (Ping-of-death attack).

f) Uncorrelated reply packets (i.e., packets which cannot be correlated to any request).

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.2.6.2.2]

Note: This clause may not be applicable for GVNP Type 1

2.9 Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of SMSF are reasonably robust when receiving unexpected input.

[Ref: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. section 4.4.4]

2.9.2 Port Scanning

Requirement:

It shall be ensured that on all network interfaces of SMSF, only documented ports on the transport layer respond to requests from outside the system.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.

The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide a remediation plan.

Sl. No	CVSS Score	Severity	Remediation
1	9.0 - 10.0	Critical	To be patched immediately
2	7.0 - 8.9	High	To be patched within a month
3	4.0 - 6.9	Medium	To be patched within three months
4	0.1 - 3.9	Low	To be patched within a year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.4.3]

[Ref [15]: https://nvd.nist.gov/vuln-metrics/cvss]

[Ref [35]: GSMA NG 133 Cloud Infrastructure Reference Architecture]

2.10 Operating Systems

2.10.1 Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions.

b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop SMSF from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided. The countermeasures are usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring.

[Ref [3]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of ICMP version 4 (ICMPv4) and ICMP version 6 (ICMPv6) packets which are not required for operation shall be disabled on the SMSF.

In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk.

ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those must be documented.

Certain ICMP types are generally permitted and do not need to be specifically documented. Those are marked as "Permitted" in the table below.

SMSF shall not send certain ICMP types by default but it may support the option to enable utilization of these types (e.g., for debugging) which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A

N/A	2	Packet Too Big	Permitted	N/A
N/A	135	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

SMSF shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e., do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e., as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

Requirement:

SMSF shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:

Each system user_account in SMSF shall have a unique User ID (UID) with appropriate non-repudiation controls.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.4.2.2]

2.10.5 OS Hardening - Minimized kernel network functions

Requirement:

Kernel-based network functions not needed for the operation of the network element shall be deactivated. In particular, the following ones shall be disabled by default:

a) IP Packet Forwarding between different interfaces of the network product.
b) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
c) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
d) IPv4 Multicast handling. In particular all packets with IP source or destination address belonging to the multicast IP ranges (224.0.0.0 through 239.255.255.255) shall be discarded by default and multicast route caching and forwarding shall be disabled to prevent smurf and fraggle attacks. A configuration option shall be available to enable the IPv4 multicast handling if required.
e) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.3.1.2]

Note: This clause may not be applicable for GVNP Type 1.

2.10.6 No automatic launch of removable media

Requirement:

SMSF shall not automatically launch any application when a removable media device such as Compact Disk (CD)-, Digital Versatile Disk (DVD)-, Universal Serial Bus (USB)-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.3.1.3]

Note: This clause may not be applicable for GVNP Type 1 and 2.

2.10.7 Protection from buffer overflows

Requirement:

SMSF shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in SMSF in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems. OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g., USB drive, CD ROM etc.) for data transfer.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.3.1.6]

Note: This clause may not be applicable for GVNP Type 1 and 2.

2.10.9 File-system Authorization privileges

Requirement:

SMSF shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.2.7]

2.10.10 SYN Flood Prevention

Requirement:

SMSF shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.3.1.4]

2.10.11 Handling of IP options and extensions

Requirement:

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.2.4.1.1.3]

2.10.12 Restrictions on running Scripts / Batch-processes

Requirement:

Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, SMSF shall have feature to restrict Scripts / Batch-processes / Macros usage among various users. It shall be possible to administratively configure scheduled tasks usage i.e., Cron-Job usage (permit / deny) among various users like Normal users, privileged users.

2.10.13 Restrictions on Soft-Restart

Requirement:

SMSF shall restrict software-based system restart options usage among various users. The software reset / restart either through command or use of key-combinations like CTRL+ALT+DEL is not available to normal users for prevention of unintended / malicious trigger of system reset / restart.

Note: Hardware based restart may not be applicable for GVNP Type 1 and 2.

2.11 Web Servers

This entire section of the security requirements is applicable if the SMSF supports web management interface.

2.11.1 HTTPS

Requirement:

The communication between SMSF Web client and SMSF Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:

Access to the webserver (for both successful as well as failed attempts) shall be logged by SMSF.

The web server log shall contain the following information:

a) Access timestamp
b) Source (IP address)
c) Account (if known)
d) Attempted login name (if the associated account does not exist)
e) Relevant fields in http request. The Uniform Resource Locator (URL) should be included whenever possible.
f) Status code of web server response

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:

SMSF web server shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.

SMSF web server shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:

No SMSF web server processes shall run with system privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for SMSF operation shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for SMSF operation.

In particular, Common Gateway Interface (CGI) or other scripting components, Server Side Includes (SSI), and Web based Distributed Authoring and Versioning (WebDAV) shall be deactivated if they are not required.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.4]

2.11.7 No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:

If CGI or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

Requirement:

If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:

Access rights for SMSF web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the SMSF web server shall be removed.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.9]

2.11.12 No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the SMSF web server and the modules/add-ons used.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:

User-defined error pages and Error messages shall not include version information and other internal information about the SMSF web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the SMSF web server shall be replaced by error pages defined by the OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for SMSF operation shall be deleted e.g., php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the SMSF web server's document directory.

In particular, the SMSF web server shall not be able to access files which are not meant to be delivered.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.3.4.14]

2.11.17 HTTP User sessions

Requirement:

To protect user sessions, SMSF web server shall support the following session ID and session cookie requirements:

a) The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
b) The session ID shall be unpredictable.
c) The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
d) In addition to the Session Idle Timeout, SMSF web server shall automatically terminate sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.
e) Session IDs shall be regenerated for each new session (e.g., each time a user logs in).
f) The session ID shall not be reused or renewed in subsequent sessions.
g) The SMSF shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.
h) Where session cookies are used the attribute 'HttpOnly' shall be set to true.
i) Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
j) Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
k) The SMSF shall not accept session identifiers from GET/POST variables.
l) The SMSF shall be configured to only accept server generated session ID.

[Ref [3]: TEC TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.2.5.3]

2.12 General SBA/SBI Aspects

This general baseline requirements are applicable to all Network Function (NF) within the 5G Core (5GC) utilizing Service-Based Interfaces (SBI), independent of a specific network product class.

2.12.1 No code execution or inclusion of external resources by JSON parsers

Requirement:

Parsers used by SMSF shall not execute JavaScript or any other code contained in JavaScript Object Notation (JSON) objects received on Service Based Interfaces (SBI). Further, these parsers shall not include any resources external to the received JSON object itself, such as files from the SMSF's filesystem or other resources loaded externally.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.6.2]

2.12.2 Validation of the unique key values in Information Elements (IEs)

Requirement:

For data structures where values are accessible using names (sometimes referred to as keys), e.g., a JSON object, the name shall be unique. The occurrence of the same name (or key) twice within such a structure shall be an error and the message shall be rejected.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.6.3]

2.12.3 Validation of the IEs limits

Requirement:

The valid format and range of values for each IE, when applicable, shall be defined unambiguously:

a) For each message the number of leaf IEs shall not exceed 16000.
b) The maximum size of the JSON body of any HTTP request shall not exceed 16 million bytes.
c) The maximum nesting depth of leaves shall not exceed 32.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section - 4.3.6.4]

2.12.4 Protection at the transport layer

Requirement:

NF Service Request and Response procedure shall support mutual authentication between NF consumer and NF producer.

All network functions shall support TLS 1.2 and above. Network functions shall support both server-side and client-side certificates.

Authentication between network functions within one PLMN shall use one of the following methods:

a) If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between NFs.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.2.2.2]

2.12.5 Authorization token verification failure handling within one PLMN

Requirement:

The NF Service producer shall verify the access token as follows:

a) The NF Service producer ensures the integrity of the access token by verifying the signature using NRF's public key or checking the Medium Access Control (MAC) value using the shared secret. If integrity check is successful, the NF Service producer shall verify the claims in the access token as follows:
b) It checks that the audience claim in the access token matches its own identity or the type of NF service producer. If a list of NSSAIs or list of NSI IDs is present, the NF service producer shall check that it serves the corresponding slice(s).
c) If an NF Set ID is present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.
d) If the access token contains "additional scope" information (i.e., allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.
e) If scope is present, it checks that the scope matches the requested service operation.
f) It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

If the verification is successful, the NF Service producer shall execute the requested service and respond back to the NF Service consumer. Otherwise, it shall reply based on the Oauth 2.0 error response defined in RFC 6749. The NF service consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from producer NF type listed in claims (scope, audience) during their validity time.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.2.2.3.1]

2.12.6 Authorization token verification failure handling in different PLMNs

Requirement:

The NF service producer shall check that the home PLMN ID of the audience claimed in the access token matches its own PLMN identity.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.2.2.3.2]

2.12.7 Protection against JSON injection attacks

Requirement:

NF Service Consumers communicate using JSON on the service-based interfaces with SMSF. SMSF shall never use the eval function to evaluate JSON data to prevent client-side JSON injections. SMSF shall sanitize all data before serializing it to JSON, to prevent server-side JSON injections.

[Ref [25]: ENISA THREAT LANDSCAPE FOR 5G NETWORKS, December 2020]

2.13 Other Security Requirements

2.13.1 Remote Diagnostic Procedure – Verification

Requirement:

If the SMSF is providing Remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user.

All activities performed by the remote user are to be logged with the following parameters:

a) User id
b) Time stamp
c) Interface type
d) Event level (e.g., CRITICAL, MAJOR, MINOR)
e) Command/activity performed
f) Result type (e.g., SUCCESS, FAILURE).
g) IP Address of remote machine

2.13.2 No System Password Recovery

Requirement:

No provision shall exist for SMSF System / Root password recovery.

2.13.3 Secure System Software Revocation

Requirement:

Once the SMSF software image is legally updated/upgraded with New Software Image, it shall not be possible to roll back to a previous software image. In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls.

SMSF shall support a well-established control mechanism for rolling back to previous software images.

2.13.4 Software Integrity Check- Installation

Requirement:

SMSF shall validate the software package integrity before the installation stage strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls (ITSAR)” only.

Tampered software shall not be executed or installed if integrity check fails.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.3.5]

2.13.5 Software Integrity Check- Boot

Requirement:

The SMSF shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” to the expected reference value.

Note: This may not be applicable for GVNP Type 1 and Type 2.

2.13.6 Unused Physical and Logical Interfaces Disabling

Requirement:

SMSF shall support the mechanism to verify both the physical and logical interfaces that exist in the product.

Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

Note: This may not be applicable for GVNP Type 1 and Type 2.

2.13.7 Predefined accounts shall be deleted or disabled

Requirement
Predefined or default user accounts (other than Admin/Root) in SMSF shall be deleted or disabled.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.2.2]

2.13.8 Correct handling of client credentials assertion validation failure

Requirement:

The verification of the Client credentials assertion shall be performed by the receiving node, i.e., NF Service Producer in the following way:

a) It validates the signature of the JSON Web Signature (JWS) as described in RFC 7515.
b) If validates the timestamp (iat) and/or the expiration time (exp) as specified in RFC 7519.
c) If the receiving node is the NF Service Producer, the NF service Producer validates the expiration time and it may validate the timestamp.

d) It checks that the audience claim in the client credentials assertion matches its own type.

It verifies that the NF instance ID in the client credentials assertion matches the NF instance ID in the public key certificate used for signing the assertion.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.2.2.4.1]
[Ref [19]: RFC 7515 - JSON Web Signature (JWS)]
[Ref [20]: RFC 7519 - JSON Web Token (JWT)]

Note: Not applicable to Release 16 implementation, applicable to Release 17.

2.13.9 Isolation of Compromised Element

Requirement:

In case of any compromise of SMSF, Service Provider shall have provisions to isolate the SMSF at network and/or compute/storage level. Such provisions shall be well documented by the Service Provider.

[Ref [33]: ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section 4.1.3]

CHAPTER 3- SPECIFIC SECURITY REQUIREMENT

3.1 Secure communication with IP-SM-GW, SMS router, SMS-GMSC and IWMSC

3.1.1 In case of non-Service based interfaces with IP-SM-GW, SMS router, SMS-GMSC and IWMSC

3.1.1.1 Diameter interface-based realization

Requirement:

To remediate Diameter interface vulnerabilities between SMSF and the IP-SM-GW, SMS router, SMS-GMSC, IWMSC, Service Provider shall implement Diameter firewall to filter/block malicious Diameter traffic.

Diameter interface shall also be confidentiality, integrity and replay protected. TLS/DTLS 1.2 and above or NDS/IP shall be implemented for the diameter protocol interface and by using the secure cryptographic controls prescribed in Table 1 of the latest document of "ITSAR for Cryptographic Controls" or 3GPP TS 33.210, as applicable. SEG shall be used to terminate NDS/IP IPsec tunnels.

All security parameters for TLS/ DTLS 1.2 and above or IPsec are to be configured independent of the Diameter interface protocol.

[Ref [31]: GSMA FS.19 Diameter Interconnect Security]

[Ref [2]: TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0 Section 9.5]

[Ref [24]: RFC 6733- Diameter Base Protocol]

[Ref [7]: TSDSI STD T1.3GPP 33.210-16.0.0 V1.1.0 Section 5 and Section 6.2]

3.1.1.2 MAP interface-based realization

Requirement:

To remediate MAP/SS7 interface vulnerabilities between SMSF and the IP-SM-GW, SMS router, SMS-GMSC, IWMSC, Service Provider shall implement MAP/SS7 firewall to filter/block malicious traffic.

The MAP interface shall use Network Domain Security for IP based protocols (NDS/IP) by using the Secure cryptographic controls prescribed in Table1 of the latest document of "ITSAR for Cryptographic Controls" or 3GPP TS 33.210, as applicable. The security services provided by NDS/IP are data integrity, data origin authentication, anti-replay protection and confidentiality. SEG shall be used to terminate the NDS/IP IPsec tunnels.

[Ref [30]: GSMA FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines]

[Ref [6]: TSDSI STD T1.3GPP 29.002-17.2.0 V1.1.0]

[Ref [32]: TSDSI STD T1.3GPP 33.204-16.0.0 V1.1.0 Section 4.1]

[Ref [7]: TSDSI STD T1.3GPP 33.210-16.0.0 V1.1.0 Section 5]

3.1.2 In case of service-based interface realization between IP-SM-GW, SMS router, SMS-GMSC and IWMSC (SBI-based SMS)

Following are the security requirements related to service-based SMS:

3.1.2.1 Mutual authentication between SMSF and IP-SM-GW, SMS router, SMS-GMSC and IWMSC

Requirement:

SMS related request and response procedure shall support mutual authentication between SMSF IP-SM-GW, SMS router, SMS-GMSC and IWMSC. SMSF shall validate all incoming messages. Messages that are not valid according to the protocol specification and network state shall be either rejected or discarded by the SMSF.

[Ref [2]: TSDSI STD T1.3GPP 33.501-17.7.0 V.1.0.0. Section 5.9.2]

3.1.2.2 Registration, discovery and authorization between SMSF and IP-SM-GW, SMS router, SMS-GMSC and IWMSC

Requirement:

SMS related discovery and registration between IP-SM-GW, SMS router, SMS-GMSC and IWMSC shall support confidentiality, integrity, and replay protection. SMSF shall be able to hide the topology of the available / supported NFs in one administrative/trust domain from entities in different trust/administrative domains (e.g., between NFs in the visited and the home networks, IP-SM-GW, SMS router, SMS-GMSC and IWMSC.)

[Ref [2]: TSDSI STD T1.3GPP 33.501-17.7.0 V.1.0.0. Section 5.9.2]

3.1.2.3 Secure Communication over Ngmsc, Niwmsc, Nipsmgw, and Nrouter interfaces

Requirement:

Data shall not be transmitted in plaintext (unencrypted) over Ngmsc, Niwmsc, Nipsmgw, and Nrouter interfaces in case of SBI-based SMS. The applications shall deploy TLS / DTLS 1.2 and above as per Secure cryptographic controls prescribed in Table1 of the latest document of "ITSAR for Cryptographic Controls" or 3GPP TS 33.210, as applicable to communicate with other nodes.

[Ref [2]: TSDSI STD T1.3GPP 33.501-17.7.0 V.1.0.0. Section 13.1]

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.2.4]

[Ref [7]: TSDSI STD T1.3GPP 33.210-16.0.0 V1.1.0 Section 6.2]

3.2 Secure LI support in SMSF

SMSF shall not be able to access data in the Point of Interception (POI). If the POI is embedded, LI data leakage from the POI back into the non-secure area of the SMSF shall be prohibited. If the POI is not embedded, the implementation shall prohibit LI data leakage back into the SMSF.

[Ref [9]: TSDSI STD T1.3GPP 33.127-17.5.0 V1.1.0 Section 8.5]

3.3 Web Servers

3.3.1 Secured HTTPS methods

Requirement:

HTTPS methods over Nsmsf_SMService interface (e.g., PATCH, DELETE, PUT) that are required for SMSF general services to other Network Functions shall be secured.

Note: An example of SMSF general service is the NF Service Consumer (e.g., AMF) may update UE context in SMSF for a given service user by using the HTTP PATCH method.

[Ref [5]: TSDSI STD T1.3GPP 29.540-17.6.0 V1.2.0]

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. section 4.2.5.4,

[Ref [28]: RFC 5789- PATCH Method for HTTP]

[Ref [29]: RFC 9110- HTTP Semantics]

3.4 Protection of SMS record and UE SMS context data

3.4.1 Encryption of SMS record and UE SMS context data

Requirement:

For data (persistent or temporary) related to SMS delivery record and UE SMS context data in storage or transfer, read access rights shall be restricted. This data shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with appropriate non-repudiation controls.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.2.3]

3.4.2 Protection against copying SMS record and UE SMS context data

Requirement:

Without authentication & authorization, SMSF shall not support copying of SMS record and UE SMS context data. Protective measures should exist against use of available SMS record data residing in SMSF to create a copy for illegal transmission.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.2.1]

Annexure-I (Definition)

1. **DDoS**: DDoS is a distributed denial-of-service attack that renders the victim un-usable by the external environment.

2. **Gateway MSC for Short Message Service (SMS-GMSC)**: Function of an MSC capable of receiving a short message from an SC, interrogating an HLR for routing information and SMS info, and delivering the short message to the VMSC or the SGSN of the recipient MS. [8]

3. **Generic Network Product**: Generic Network Product (GNP) model as defined in Section 4.1 and 4.3 of TSDSI RPT T1.3GPP 33.926-16.4.0 V1.0.0

4. **Generic virtualized network product model (GVNP) Type 1**: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0

5. **Generic virtualized network product model (GVNP)Type 2**: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0

6. **Generic virtualized network product model (GVNP)Type 3**: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0

7. **Home Environment**: Responsible for overall provision and control of the Personal Service Environment of its subscribers. [16]

8. **Interworking MSC For Short Message Service (SMS IWMSC)**: Function of an MSC capable of receiving a short message from within the PLMN and submitting it to the recipient SC. [8]

9. **IP-Short-Message-Gateway (IP-SM-GW)**: Function responsible for protocol interworking between the IP-based UE and the SC. [8]

10. **Machine Accounts**: These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons. [3]

11. **Mobile Equipment (ME)**: The Mobile Equipment is functionally divided into several entities, i.e., one or more Mobile Terminations (MT) and one or more Terminal Equipment (TE). [16]

12. **Mobile-services Switching Centre (MSC)**: Exchange which performs switching functions for mobile stations located in a geographical area designated as the MSC area. [4]

13. **Network Function**: A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behaviour and 3GPP defined interfaces. A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g., on a cloud infrastructure. [1]

14. **NF service**: A functionality exposed by a NF through a service-based interface and consumed by other authorized NFs. [1]

15. **NF Set ID**: A NF Set Identifier (NF Set ID) is a globally unique identifier of a set of equivalent and interchangeable Control Plane NFs from a given network that provide distribution, redundancy and scalability. [3]

16. **Non-Access Stratum**: Protocols between UE and the core network that are not terminated in the RAN. [16]

17. **Original Equipment Manufacturer** (OEM): Manufacturer of communication and its related products under whose brand, the products are sold or proposed to be sold to operators in the country.

18. **Personal Service Environment**: Contains personalised information defining how subscribed services are provided and presented towards the user. Each subscriber of the Home Environment has her own Personal Service Environment. The Personal Service Environment is defined in terms of one or more User Profiles. [16]

19. **PLMN Area**: The PLMN area is the geographical area in which a PLMN provides communication services according to the specifications to mobile users. In the PLMN area, the mobile user can set up calls to a user of a terminating network. The terminating network may be a fixed network, the same PLMN, another PLMN or other types of PLMN. Terminating network users can also set up calls to the PLMN. The PLMN area is allocated to a PLMN. It is determined by the service and network provider in accordance with any provisions laid down under national law. In general, the PLMN area is restricted to one country. It can also be determined differently, depending on the different telecommunication services, or type of MS. If there are several PLMNs in one country, their PLMN areas may overlap. In border areas, the PLMN areas of different countries

may overlap. Administrations will have to take precautions to ensure that cross border coverage is minimized in adjacent countries unless otherwise agreed. [3]

20. **Protocol**: A formal set of procedures that are adopted to ensure communication between two or more functions within the same layer of a hierarchy of functions (source: ITU-T I.112). [16]

21. **Quality of Service (QoS)**: The collective effect of service performances which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as; [3]
    a) service operability performance;
    b) service accessibility performance;
    c) service retainability performance;
    d) service integrity performance;
    e) other factors specific to each service.

22. **Sensitive data**: Data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules. [3]

23. **Service center (SC)**: Function responsible for the relaying and store and forwarding of a short message between a Short message entity and an MS. [16]

24. **Serving Network**: The serving network provides the user with access to the services of the home environment. [16]

25. **Short message (SM)**: Information that may be conveyed by means of the Short Message Service. [4]

26. **Stratum:** Grouping of protocols related to one aspect of the services provided by one or several domains. [3]

27. **System group account**: A predefined system account in the network product, usually with special privileges, which has a predefined user id and hence cannot be tied to a single user (individual) in a normal operating environment. [3]

28. **User Equipment**: A device allowing a user access to network services. The interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains, the domains being separated by reference points. [3]

Annexure-II (Acronyms)

3GPP	-	Third Generation Partnership Project
4G	-	Fourth Generation
5G	-	Fifth Generation
5G-CN	-	5G Core Network
5GS	-	5G System
AAA	-	Authentication, Authorization and Accounting
AF	-	Application Function
AMF	-	Access and Mobility Management Function
AN	-	Access Network
API	-	Application Programming Interfaces
ARP	-	Address Resolution Protocol
AuSF	-	Authentication Server Function
BOOTP	-	Bootstrap Protocol
CAPTCHA	-	Completely Automated Public Turing test to tell Computers and Humans Apart
CD	-	Compact Disk
CDP	-	Cisco Discovery Protocol
CPU	-	Central Processing Unit
CGI	-	Common Gateway Interface
CWE	-	Common Weakness Enumeration
DDoS	-	Distributed Denial of Service
DoT	-	Department of Telecommunications
DN	-	Data Network
DNS	-	Domain Name System
DVD	-	Digital Versatile Disk
eMBB	-	Enhanced Mobile Broadband
EPC	-	Evolved Packet Core
EPS	-	Evolved Packet System
ETSI	-	European Telecommunications Standards Institute
FTP	-	File Transfer Protocol
gNB	-	Next Generation Node B
GUI	-	Graphical User Interface
GVNP	-	Generalized Virtual Network Product
HE	-	Home Environment
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hyper Text Transfer Protocol Secure
ICMP	-	Internet Control Message Protocol
ICMPv4	-	ICMP version 4
ICMPv6	-	ICMP version 6
IE	-	Information Element
IEEE	-	Institute of Electrical and Electronics Engineers
IETF	-	Internet Engineering Task Force
IP	-	Internet Protocol

IPv4	-	IP version 4
IPv6	-	IP version 6
IPSec	-	Internet Protocol Security
IM	-	Instant Messaging
IMPI	-	IP Multimedia Private Identity
IMPU	-	IMS Public User Identity
IMS	-	IP Multimedia Subsystem
IMT-2020	-	International Mobile Telecommunications-2020
IP-SM-GW	-	IP-Short-Message-Gateway
ISO	-	International Organization for Standardization
ITSAR	-	Indian Telecom Security Assurance Requirements
ITU	-	International Telecommunication Union
ITU-T	-	ITU - Telecommunications Standardization Sector
JSON	-	JavaScript Object Notation
LI	-	Lawful Interception
LLDP	-	Link Layer Discovery Protocol
LTE	-	Long Term Evolution
mMTC	-	Massive Machine Type Communication
MAC	-	Medium Access Control
ME	-	Mobile Equipment
MOP	-	Maintenance Operations Protocol
MSC	-	Mobile-services Switching Centre
N3IWF	-	Non-3GPP Interworking Function
NAS	-	Non-Access Stratum
NEF	-	Network Exposure Function
NF	-	Network Function
NFV	-	Network Function Virtualization
NG	-	Next Generation
ng-eNB	-	Next Generation e-NodeB
NG-RAN	-	Next Generation Radio Access Network
NR	-	New Radio
NRF	-	Network Repository Function
NSA	-	Non-Stand Alone
NSI ID	-	Network Slice Instance Identifier
NSSAI	-	Network Slice Selection Assistance Information
NTP	-	Network Time Protocol
NTS	-	Network Time Security
NWDAF	-	Network Data Analytics Function
OAM	-	Operations, Administration and Management
OEM	-	Original Equipment Manufacturer
OS	-	Operating System
OSI	-	Open Systems Interconnection
OWASP	-	Open Worldwide Application Security Project
P2P	-	Peer-to-peer
PAD	-	Packet Assembler/Disassembler
PCF	-	Policy Control Function

PDU	-	Protocol Data Unit
PFD	-	Packet Flow Description
PLMN	-	Public Land Mobile Network
POI	-	Point of Interception
PTP	-	Precision Time Protocol
QoS	-	Quality of Service
RAN	-	Radio Access Network
RAT	-	Radio Access Technology
RBAC	-	Role-Based Access Control
RCP	-	Rate Control Protocol
RDP	-	Remote Desktop Protocol
REST	-	Representational State Transfer
RPF	-	Reverse Path Filter
RSH	-	Remote Shell Protocol
RTP	-	Real-time Transfer Protocol
SA	-	Stand Alone
SBA	-	Service Based Architecture
SBI	-	Service Based Interface
SC	-	Service Centre
SDN	-	Software Defined Networking
SFTP	-	Secure File Transfer Protocol
SM	-	Short Message
SMF	-	Session Management Function
SMS	-	Short Message Service
SMS-GMSC	-	Gateway MSC for Short Message Service
SMS IWMSC	-	Interworking MSC For Short Message Service
SMSF	-	Short Message Service Function
SN	-	Serving Network
SNMP	-	Simple Network Management Protocol
SSH	-	Secure Shell
SSI	-	Server Side Includes
SSL	-	Secure Sockets Layer
SUPI	-	Subscription Permanent Identifier
SYN	-	Synchronize
TCP	-	Transmission Control Protocol
TEC	-	Telecommunication Engineering Centre
TFTP	-	Trivial File Transfer Protocol
TLS	-	Transport Layer Security
TSDSI	-	Telecommunications Standards Development Society
TSTL	-	Telecom Security Testing Laboratory
UDM	-	Unified Data Management
UDP	-	User Datagram Protocol
UDR	-	Unified Data Repository
UE	-	User Equipment
UID	-	User ID
UL	-	Uplink

UPF	-	User Plane Function
URLLC	-	Ultra Reliable and Low Latency Communications
URL	-	Uniform Resource Locator
USB	-	Universal Serial Bus
USIM	-	Universal Subscriber Identity Module
VN	-	Virtual Network
VPN	-	Virtual Private Network

Annexure-III (References)

1. TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0, “System architecture for the 5G System (5GS); Stage 2, 3GPP TS 23.501 V17.6.0".
2. TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0, “Security architecture and procedures for 5G system; 3GPP TS 33.501 V17.7.0”.
3. TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0, “Catalogue of general security assurance requirements”.
4. 3GPP TS 23.040 V17.2.0 (2022-03), “Technical realization of the Short Message Service (SMS)”.
5. TSDSI STD T1.3GPP 29.540-17.6.0 V1.2.0, “SMS Services”.
6. TSDSI STD T1.3GPP 29.002-17.2.0 V1.1.0, “Mobile Application Part (MAP) specification”.
7. TSDSI STD T1.3GPP 33.210-17.1.0 V1.1.0, “IP network layer security”.
8. TSDSI STD T1.3GPP 23.540-17.1.0 V1.1.0, “Technical realization of Service Based Short Message Service”.
9. TSDSI STD T1.3GPP 33.127-17.5.0 V1.1.0, “Lawful Interception (LI) architecture and functions”.
10. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
11. https://owasp.org/www-project-top-ten/
12. https://owasp.org/www-project-api-security/
13. RFC 8915 - Network Time Security for the Network Time Protocol (NTP).
14. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
15. https://nvd.nist.gov/vuln-metrics/cvss
16. 3GPP TR 21.905 V17.1.0 (2021-12), “Vocabulary for 3GPP Specifications”.
17. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure.
18. RFC 6749 - The OAuth 2.0 Authorization Framework.
19. RFC 7515 - JSON Web Signature (JWS).
20. RFC 7519 - JSON Web Token (JWT).
21. ENISA Recommendation “Standardization in support of the cybersecurity certification”, Dec 2019.

22. ETSI TS 103 221-1, "Lawful Interception (LI); Internal Network Interfaces; Part 1: X1" V1.12.1 (2022-08).
23. ETSI TS 103 221-2, "Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3" V1.4.1 (2021-04).
24. RFC 6733- Diameter Base Protocol.
25. ENISA THREAT LANDSCAPE FOR 5G NETWORKS, December 2020.
26. ENISA Signalling Security in Telecom SS7/Diameter/5G, EU level assessment of the current situation, MARCH 2018.
27. "Security Guidance for 5G Cloud Infrastructure Part III: Data Protection" by NSA & CISA https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf
28. RFC 5789- PATCH Method for HTTP.
29. RFC 9110- HTTP Semantics.
30. GSMA FS.11, "SS7 Interconnect Security Monitoring and Firewall Guidelines".
31. GSMA FS.19, "Diameter Interconnect Security".
32. TSDSI STD T1.3GPP 33.204-16.0.0 V1.1.0, "Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security".
33. ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section 4.1.3 https://www.enisa.europa.eu/publications/security-in-5g-specifications
34. CIS Password Policy guide
35. GSMA NG 133 Cloud Infrastructure Reference Architecture