2/c

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

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 **5G-Binding Service Function (BSF)** . 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)

Binding Support Function (BSF) of 5G

NCCS/ITSAR/Core Equipment/5G sub systems/Binding Support Function (BSF)

(ITSAR No: ITSAR11124YYMM)

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

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 of telecommunication equipment 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.	Binding Support Function (BSF) of 5G	ITSAR11124YYMM	1.1.0		

Contents

A) Outline

The objective of this document is to present comprehensive, country-specific security requirements for the Binding Support Function (BSF), a network function of the 5G Core. BSF was first specified in 3GPP TS 23.501, Release 15. The BSF is used for binding an Application-Function (AF) request targeting a particular UE to a specific Policy Control Function (PCF) instance. It stores the session bindings for a particular User Equipment (UE) or a particular Protocol Data Unit (PDU) session. BSF functionalities also involve binding data registration/deregistration/update/discovery/retrieval and enabling subscriptions to the notifications of PCF registration/deregistration events.

The specifications produced by various regional/international standardization bodies/organizations/associations like the 3rd Generation Partnership Project (3GPP), International Telecommunication Union - Telecommunications Standardization Sector (ITU-T), International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), Next Generation Mobile Networks alliance (NGMN), Global System for Mobile communication Association (GSMA), Telecommunications Standards Development Society (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 the 5G system architecture, BSF overview and its functionalities, BSF interfaces, coexistence scenario with 4G Diameter Routing Agent (DRA), Proxy BSF, Redirect BSF and then proceeds to address the common and entity specific security requirements of BSF related to SBI based interface, Diameter based interface, security of the sessions binding database, backups and Nbsf management API.

B) Scope

This document targets on the security requirements of the 5G Core BSF network function as defined by 3GPP. This document does not cover the security requirements at the virtualization and infrastructure layers.

Remote Access regulations are governed by the Licensing Wing of 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 requirement framework for 5G is specified by International Telecommunication Union (ITU) under International Mobile Telecommunications-(IMT)-2020. The usage scenarios/use cases identified for 5G are i) Enhanced Mobile Broadband (eMBB) ii) Massive Machine Type Communications (mMTC) and iii) Ultra Reliable and Low Latency Communications (URLLC).

1.2 5G Architecture

The 5G architecture facilitates data connectivity and supports various service deployments by using techniques like Software Defined Networking (SDN) and Network Function Virtualization (NFV). This facilitates the separation of control plane and data plane to achieve scalable and flexible deployments.

The generic 5G system (5GS) architecture consists of User Equipment (UE), Radio Access Network supporting New Radio (NR), 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 (5G-CN). The 5G base station is called the Next Generation Node B (gNB). The deployment strategies possible are Non-Stand Alone (NSA) and Stand Alone (SA). SA denotes 5G NR connected to 5G-Core Network. In the NSA mode, 5G NR gets connected to the Fourth Generation (4G) Evolved Packet Core (EPC) but uses Long Term Evolution (LTE) as an 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 enables the subscribers through access and authorization to avail the services.

These functionalities of the 5G core network are supported using 3GPP defined processing functions called as “network functions”. Network functions can be implemented using either dedicated hardware or can be instantiated as virtualized functions.

The salient features of 5G Core are as follows:

1) Separation of Control Plane and User Plane

2) Service Based Architecture (SBA)

3) Network Slicing

4) Network Function Virtualization (NFV) and Software Defined Networking (SDN)

5) Access Agnostic

6) Framework for policy control and support of QoS and

7) Storage of subscription data, subscriber access authentication, authorization and security anchoring.

In the SBA framework, the individual elements are defined as Network Functions (NFs) instead of Network entities. Through the Service Based Interface (SBI), each of the NFs consumes services offered by other service producers viz. other NFs. Representational State Transfer (REST) ful Application Programming Interfaces (APIs) are used in 5G SBA which use Hypertext Transfer Protocol (HTTP)/2 as application layer protocol. Service based architecture for the 5G system is shown in Figure 1 including some important core network functions.

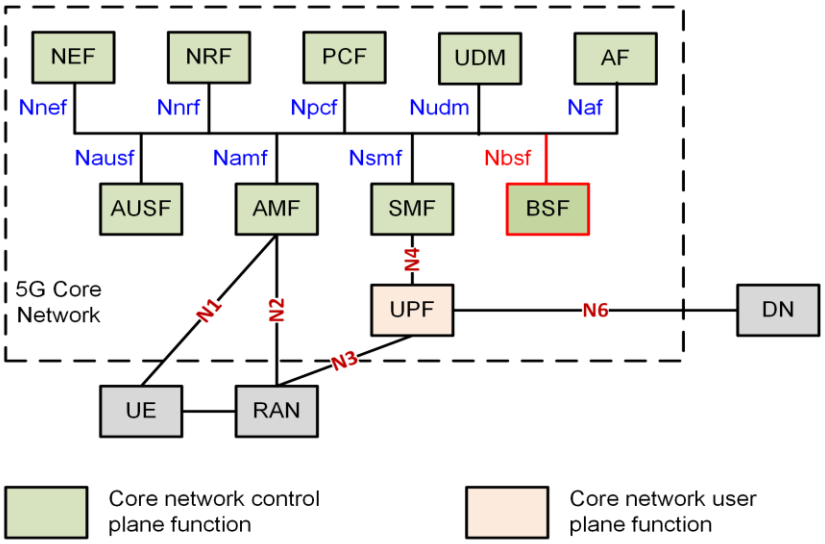

Figure 1: Service based architectural view of 5GS
[Adapted from: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

Some of the core network functions and their 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 (related to user plane part), traffic usage reporting and QoS handling 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 5G architecture to provide services and can access Network Exposure Function (NEF) (and possibly PCF) by interacting with the policy framework for policy control. In case of existence of more than one PCFs in the Core Network, 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.

Any network function in the control plane can enable other authorized network functions to access their services using the 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 N5 between PCF and AF.

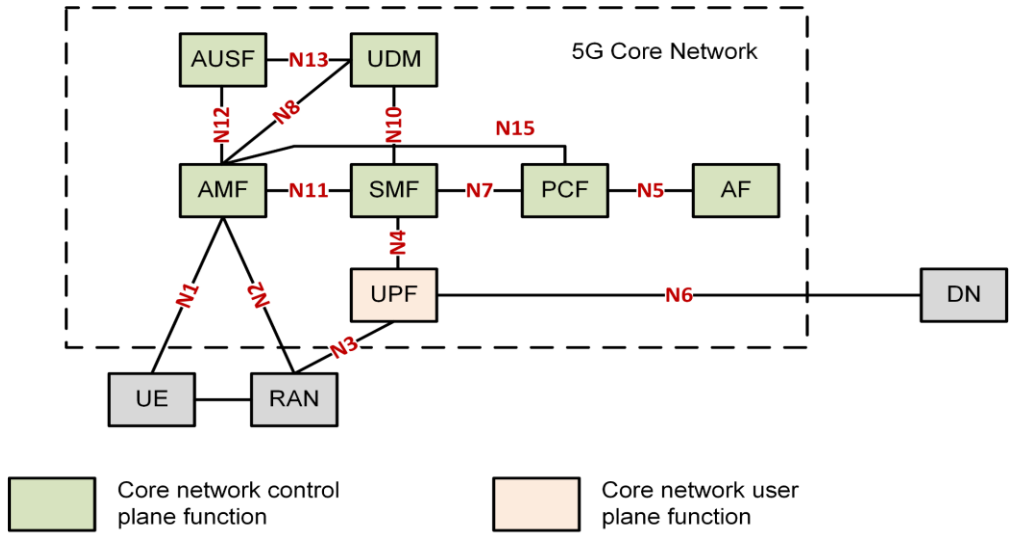

Figure 2: Reference point representation for 5GS
[Adapted from: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

1.3 General Security Architecture for 5G System

The 5G System works on the principle of cloud-native 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.

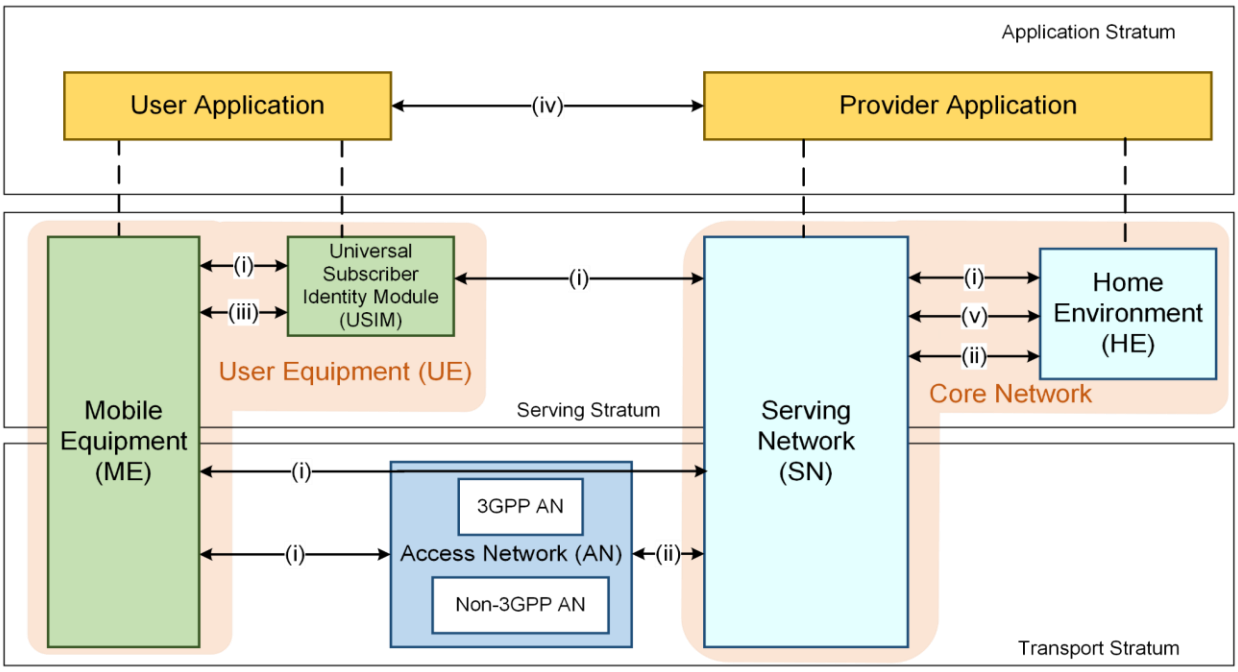

Figure 3: Overview of the security architecture [Adapted from: TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0]

Mobile Equipment (ME)/ User Equipment (UE) 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 Serving Network (or visiting 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 Serving Network is facilitated using the Universal Subscriber Identity Module (USIM).

User Application is the application layer in the UE, which facilitates user interaction with provider applications. 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 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 3.

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

The Common and specific security requirements of the Binding Support Function are covered in the present document. The following sections cover the overview of the BSF along with its security aspects.

1.4 Binding Support Function (BSF)

The Binding Support Function (BSF) was first specified in 3GPP TS 23.501, Release 15. The BSF is used for binding an Application-Function (AF) request targeting a UE address to a specific Policy Control Function (PCF) instance.

There may be multiple and separately addressable PCFs in a PLMN. When such multiple and separately addressable Policy Control Functions (PCFs) have been deployed, the BSF is required in order to ensure that an AF for a certain Protocol Data Unit (PDU) session reaches over the N5/Rx interface to the PCF holding the PDU session information.

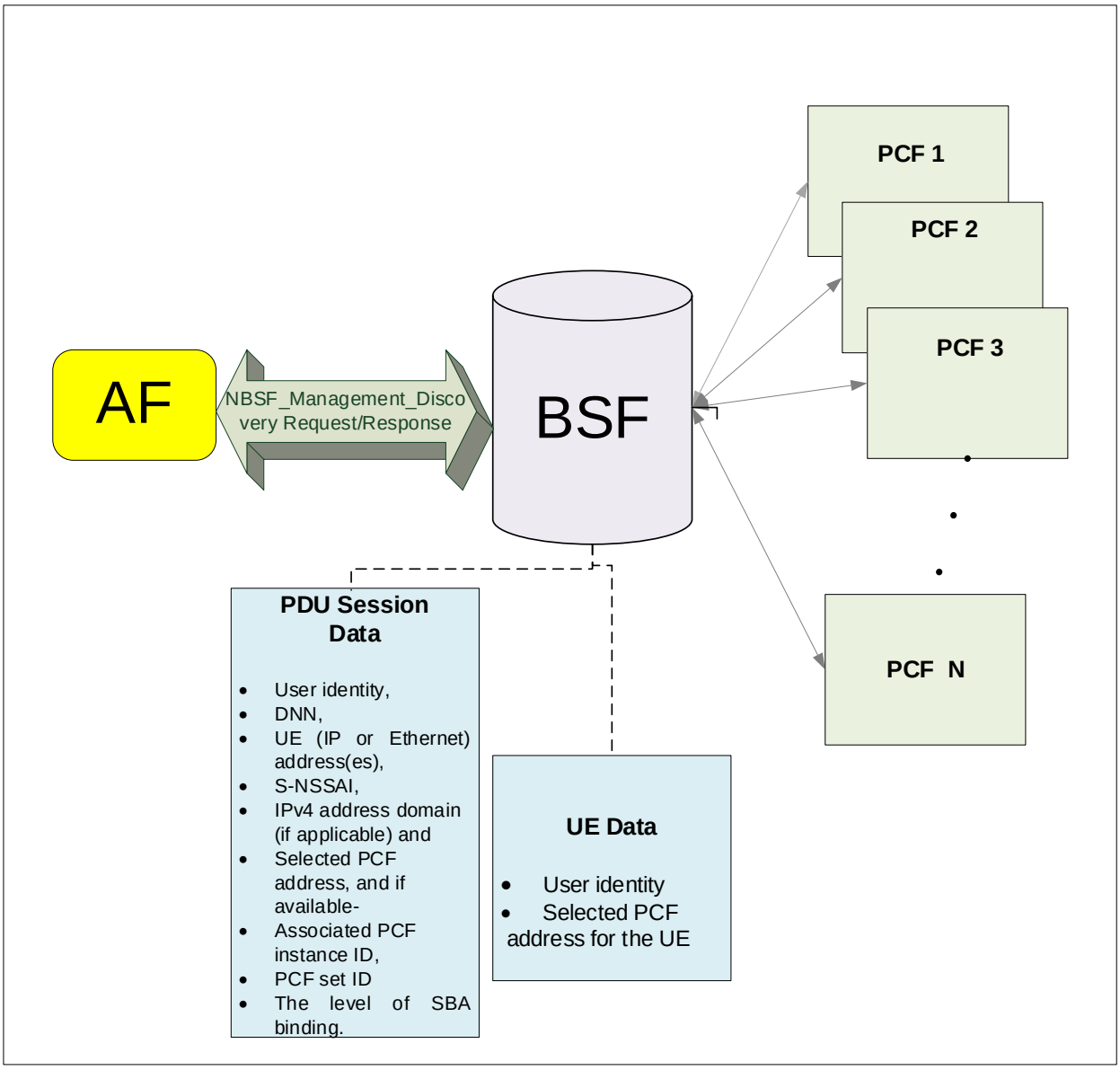

Figure 4: Any NF Consumer (e.g., AF's) request routed by BSF to the addressed PCF

1.4.1 Session Binding Mechanism:

The session binding mechanism is a part of the binding mechanism that maps the session information with the Quality of Service (QoS) flow that is intended to carry the Service Data Flow(s) (SDF).

The binding mechanism consists of three steps:

1) Session binding.
2) Policy and Charging Control (PCC) rule authorization.

3) QoS flow binding.

The Session binding is the association of the AF session information to one and only one PDU session. The Session binding information is received by the AF. The AF determines the relevant PDU session. With this information, the PCC rule authorization function runs the policy rules and constructs the PCC rule(s), if the authorization is granted. Finally, the QoS flow binding function selects the QoS flow(s) to carry the service data flow (defined in a PCC rule by means of the SDF template), within the PDU session.

1.4.2 Functionalities of the BSF:

The 5G BSF:

1) stores the binding information for a certain PDU Session;
2) stores the binding information for a certain UE;
3) enables subscriptions to the notifications of PCF for PDU session registration /deregistration events;
4) enables subscriptions to the notifications of the PCF for UE registration/de-registration events;
5) and enables the discovery of binding information (e.g., the address information of the selected PCF for a PDU session) by the NF consumers (elaborated in Section 1.4.3).

The AF can also select a PCF based on the local configuration for Ethernet PDU sessions.

The 5G Binding Support Function (BSF) is comparable with the Session Binding Function on the Diameter Routing Agent (DRA) used in 4G.

The BSF has the following characteristics:

1) The BSF stores internally information about the corresponding selected PCF.
    i) For a certain PDU session, the BSF stores internally information about the a) The User Identity, b) Data Network Name (DNN), c) UE (IP or Ethernet) address(es), d) Specific-Network Slice Selection Assistance Information (S-NSSAI), e) IPv4 Address Domain (if applicable) and f) Selected PCF address, and if available g) Associated PCF instance ID, h) PCF set ID and the I) Level of SBA binding.

    ii) For a certain UE, the BSF stores internally information about the a) UE identity, b) Selected PCF address for the UE, and if available c) the associated PCF instance ID and d) the level of SBA binding.
2) The PCF utilizes the Nbsf_Management service of the BSF to register, update or remove the stored information in the BSF.

1.4.3 BSF Service Architecture:

The Binding Support Management Service (Nbsf_Management) is provided by the Binding Support Function (BSF). The known consumers of the Nbsf_Management service, as shown in Figure 5 are: a) Policy Control Function (PCF), b) Network Exposure Function (NEF), c) Application Function (AF), d) Network Data Analytics Function (NWDAF) and e) Time Sensitivity Communication and Time Synchronization Function (TSCTSF).

The BSF can be deployed either standalone or as a functionality provided by other network functions (collocated) such as PCF, UDR, NRF and SMF.

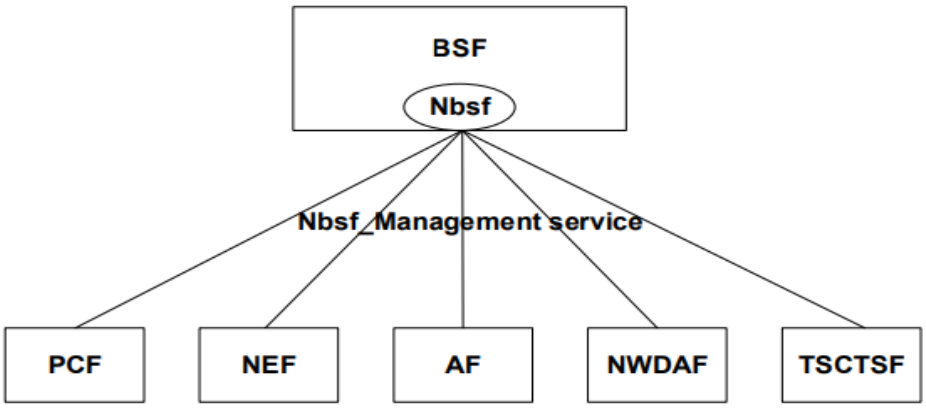

Figure 5: Architecture for the Nbsf_Management service; SBI representation: [Adapted from: 3GPP TS 29.521 V17.0.0 (2021-03]

NOTE 1: The PCF accesses the Nbsf_Management service at the BSF via an internal interface when it is collocated with BSF.

NOTE 2: The PCF in the figure represents both, the PCF for a UE and the PCF for a PDU session.

NOTE 3: The DRA decides to select a BSF based on the UE's IP address range when the DRA has no binding information of the UE, to get to the relevant PCF for a PDU session address.

NOTE 4: Collocation allows combined implementation.

1. The PCF for a UE and the PCF for a PDU session separately and independently register themselves at the BSF, regardless of whether they are deployed in the same NF instance or separately in different NF instances.

2. The PCF for a PDU session registers the binding information of a UE in the BSF using the Nbsf_Management_Register service operation, whenever an IPv4 address and/or IPv6 prefix is allocated to the UE, or a MAC address is used for the PDU session.
3. The PCF removes the binding information in the BSF using the Nbsf_Management_Deregister service operation and updates the same using the Nbsf_Management_Update operation.
4. The service consumers AF, NEF, NWDAF, TSCTSF can discover the binding information using the Nbsf_Management_Discovery operation and subscribe to the notifications of PCF registration/deregistration events using the Nbsf_Management_Notify operation.
5. Optionally, the BSF can store and retrieve data from the UDR. using the Nudr_DataRepository_Update request service operation and Nudr_DataRepository _Update response service operation.

1.4.4 DRA and BSF coexistence

In situations involving network migration, the Diameter Routing Agent (DRA) of 4G and BSF of 5G may coexist in the operator's network.

Whenever the AF sends an Rx request to the DRA for the policies of a certain UE or of a certain PDU session, the DRA can utilize the Nbsf_Management_Discovery service operation to obtain the relevant PCF address.

The DRA only applies this operation if it has no stored binding information of an ongoing Gx session for that UE.

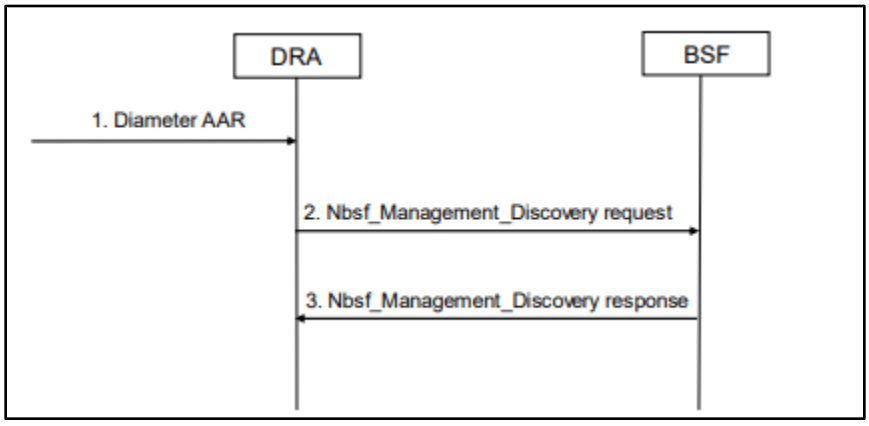

Figure 6: PCF discovery by DRA via BSF [Reference: 3GPP TS 29.513 V17.0.0 (2020-09]

1.4.5 Proxy BSF

The BSF supports and is able to proxy or redirect Rx requests based on the IP address of a UE.

When the BSF receives a Diameter AAR request from an AF, containing the session information in the form of Attribute Value Pairs (AVPs), it checks whether it already has selected a PCF for the Rx session; if it does have a PCF already selected for the Rx session, it proxies the request to the corresponding PCF. The Diameter AAA response from the PCF is proxied to the AF.

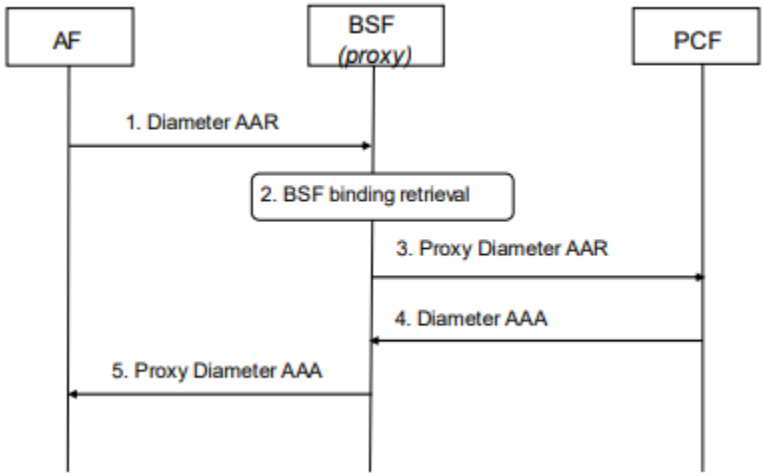

Figure 7: Rx Session establishment procedure using BSF proxy [Reference: 3GPP TS 29.513 V17.0.0 (2020-09)]

1.4.6 Redirect BSF

A BSF implemented as a Diameter Redirect agent redirects the received Diameter request messages.

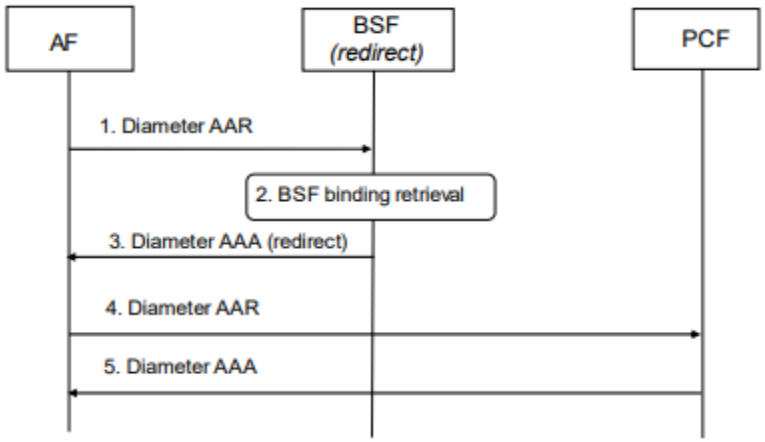

Figure 8: Rx Session Establishment procedure using BSF Redirect. [Reference: 3GPP TS 29.513 V17.0.0 (2020-09)]

A Diameter AAR indicating establishment of a new Rx Diameter session with the PCF is sent by the AF and received by a BSF (redirect). The BSF selects the PCF from the binding for the AF and sends a Diameter AAA indicating redirection as defined in IETF, RFC 6733. The AF and PCF further communicate using the Diameter AAR and AAA messages.

1.5 BSF Security Aspects

The Binding Support Function is a part of the Control Plane of the 5G Core Network. The security requirements of BSF are:

1. **SBI Interface related:** BSF has SBI interfaces with the AF, PCF, NEF, NWDAC and TSCTSF for control-signaling, data-storage and discovery, which require to be secured for information transfer.
2. **Diameter Interface related:**

The diameter interface is vulnerable to threats and Distributed Denial of Service (DDoS attacks), which needs to be addressed. There are three possibilities of BSF using the Diameter interface:

i) **Coexistence Scenario:** In the case of 4G - 5G coexistence scenario, all data transfers using the Diameter Interface during Gx sessions need to be secured.

ii) **Proxy BSF:** All sessions with Proxy BSF using the diameter protocol are required to be secured.

iii) **Redirect BSF:** All sessions with Redirect BSF using diameter protocol need to be secured.

3. Session Binding Database related: The Session's Binding Database of BSF stores vital UE credentials and Session related data that needs to be secured.

Storage/Transfer of data from the BSF database needs protection. Secured backups and secured export of BSF database is essential.

Chapter 2 - Common Security Requirements

Section 1: Access and Authorization

2.1.1 Authentication for Product Management and Maintenance interfaces

Requirement:

BSF shall support mutual authentication of entities on management interfaces, the authentication mechanism can rely on the management protocols used for the interface itself 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 BSF 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:

BSF 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 V1.1.0. Section-4.2.3.2.4]

2.1.3 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]

2.1.4 Role-based access control policy

Requirement:

BSF 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). BSF supports RBAC with a minimum of 3 user roles, in particular, for OAM privilege management for BSF 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.1.1.0. 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

2.1.5 Remote login restrictions for privileged users

Requirement:

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

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.2.6]

2.1.6 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.1.1.0. Section-4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts

Requirement:

Users shall be identified unambiguously by the BSF.

BSF shall support the assignment of individual accounts per user, where the user could be a person, or, for Machine Accounts, an application, or a system.
BSF 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 V1.1.0. Section-4.2.3.4.1.2]

Section 2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication on the 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 V1.1.0 Section-4.2.3.4.1.1]

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

2.2.2 Authentication Support – External

Requirement:

If the BSF supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services), then the communication between BSF 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:

Protection against brute force and dictionary attacks that hinder authentication attribute (i.e., password) guessing shall be implemented in BSF. Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attributes 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 on 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 the BSF. An exception to this requirement is machine accounts.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section-4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

a) The configuration setting shall be such that BSF 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 BSF). It shall not be possible setting this absolute minimum length to Absolute a lower value by configuration.
    ii) Password shall mandatorily comprise all the following four categories of characters:
        - At least 1 uppercase character (A-Z)
        - At least 1 lowercase character (a-z)
        - At least 1 digit (0-9)
        - At least 1 special character (e.g., @, $., etc.)
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 BSF.
e) When a user is changing a password or entering a new password, the BSF /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.).
f) Passwords 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 V1.1.0. 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. BSF 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 timeout 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.1.1.0. 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).

The BSF shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. BSF 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 BSF shall store at least the three previously set passwords. The maximum number of passwords that the BSF 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.

BSF shall 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 by the BSF.

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 the 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 V1.1.0. Section-4.2.3.4.3.

Ref [60]: CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf]

2.2.7 Protected Authentication feedback

Requirement:

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 V1.1.0. 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 passwords 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 V1.1.0. 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. BSF 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.1.1.0. Section-4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement:

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 the 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 the 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 33.117-16.7.0 V.1.0.0. Section-4.2.3.4.5]

2.2.11 Suspend accounts on non-use

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 [60]: CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf]

Section 3: Software Security

2.3.1 Secure Update

Requirement:

a) Software package integrity shall be validated during the software update stage.
b) BSF 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, the BSF has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update 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 V1.1.0. Section-4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

a) Software package integrity shall be validated during the software upgrade stage.
b) BSF 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, the BSF has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software installation/update/upgrade 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 V1.1.0. 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 BSF software which includes OEM developed code, third party software and opensource code libraries used/embedded in the BSF.
    ii) The BSF 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 BSF and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

[Ref [4]: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html.
Ref [5]: https://owasp.org/www-project-top-ten/.
Ref [6]: https://owasp.org/www-project-api-security/.]

2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that BSF is free from all known malware and backdoors as on the date of offer of the BSF to designated TSTL, for testing and shall submit their internal Malware Test Document (MTD) of the BSF 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 BSF shall not be present.

Orphaned software components/packages shall not be present in the BSF. OEM shall provide the list of software that are necessary for BSF's operation. In addition, OEM shall furnish an undertaking as "BSF does not contain software that is not used in the functionality of the BSF."

[Ref [3]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section-4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:

BSF 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 the BSF 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.

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 BSF and their purpose needs to be provided by the OEM as a prerequisite for the test case.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

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

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

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

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

The BSF shall generate audit logs for all changes to time settings.

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

[Ref [7]: RFC 8915 - Network Time Security for the Network Time Protocol (NTP).]

2.3.9 Restricted reachability of services

Requirement:

The BSF shall restrict the reachability of services so that they can only be reached 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 BSF 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 to support separation of management traffic from user traffic.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.2.2]

2.3.10 Self Testing

Requirement:

The BSF'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.

Section 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 BSF shall be permanently deactivated. Permanently means that they shall not be reactivated again after the BSF 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 BSF 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 BSF.

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

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. 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 shall ensure that the BSF does 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.1.1.0. 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:

BSF shall not contain any access mechanism which is unspecified or not declared. An undertaking shall be given by the OEM as follows:

"The BSF does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel."

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement:

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

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

The BSF shall log all important Security events with unique System Reference details as given in the table below:

BSF 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 and 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 the BSF.	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 BSF.	Change made
		Timestamp
		Outcome of event (Success or failure)
		Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the network device/BSF that forces a reboot or shutdown OR where the network device/BSF has crashed.	Action performed (boot, reboot, shutdown, etc.)
		Username (for intentional actions)
		Outcome of event (Success or failure)
		Timestamp
		Interface name and type

Interface status change (Mandatory)	Change to the status of interfaces on the network device/BSF (e.g. shutdown)	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 authorized 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.1.1.0. Section-4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:

a) BSF 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 the BSF.
c) BSF 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 documents 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.1.1.0. Section-4.2.3.6.2]

2.5.4 Logging access to personal data

Requirement:

In some cases, access to personal data in 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 T1.33.117-17.1.0 V1.1.0. Section-4.2.3.2.5]

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:

BSF 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 the BSF 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 BSF (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 BSF (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 [8]: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

Ref [50]: ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019.]

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of the BSF 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 BSF is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the BSF)."

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:

a) When BSF 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 users.

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. 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 the BSF 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 BSF 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 V1.1.0. Section- 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

a) Without authentication and authorization and except for specified purposes, BSF 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 the BSF to create a copy of data for illegal transmission.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**

a) BSF shall have mechanisms to prevent data exfiltration attacks for theft of 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 BSF.
c) Session logs shall be generated for establishment of any session initiated by either user or BSF.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

- BSF shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit (with in its boundary).
- 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 BSF.
- Session logs shall be generated for establishment of any session initiated by either user or BSF system.

2.6.9 System Robustness against Unexpected Input

During transmission of data to a system, it is necessary to validate input to the BSF, before processing. This includes all data which is sent to the system. Examples of these are user input, inputs from BSF's NF consumers viz. PCF, AF, NWDAF, TSCTSF and NEF, 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:

BSF shall support secure mechanisms for taking backup of sensitive data, configuration and log files. The service provider shall have an effective backup strategy in place and that it is well documented. Such backup copies of BSF shall be encrypted by strictly using the cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls".

Ref [32]: “Security Guidance for 5G Cloud Infrastructure”, Data Protection by NSA & CISA, Part III]

2.6.11 Secure Destruction of Data

Requirement:

BSF 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 [32]: “Security Guidance for 5G Cloud Infrastructure” by NSA & CISA https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf]

Section 7: Network Services

2.7.1 Traffic Filtering – Network Level Requirement

Requirement:

BSF shall provide a mechanism to filter incoming IP packets on any interface (Refer to RFC 3871)

In particular the BSF shall provide a mechanism:

a) To filter incoming IP packets on any IP 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 the protocol header.
e) To reset the accounting.
f) BSF shall provide a mechanism to disable/enable each defined rule.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section- 4.2.6.2.1]

2.7.2 Traffic Separation

Requirement:

The BSF 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.1.1.0. Section-4.3.5.1
Ref [24] RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection – Anti-Spoofing

Requirement:

BSF 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.1.1.0. Section- 4.3.3.1.1]

Section 8: Attack Prevention Mechanisms

2.8.1 Overload situations

Requirement:

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

BSF shall provide security measures to deal with overload situations which may occur as a 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 available RAM per application
b) Restricting 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 amount or size of transactions of an user or from an IP address in a specific time range
g) Limiting 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 V1.1.0. Section-4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:

The BSF shall act in a predictable way if an overload situation cannot be prevented. BSF shall be built in such a way that it can react to 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 a case it shall be ensured that BSF 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 BSF's Over Load 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 V1.1.0. Section-4.2.3.3.3]

2.8.3 Interface Robustness Requirements

Requirement:

BSF 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 BSF. 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 IP version 4 (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.1.1.0. Section-4.2.6.2.2]

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

Section 9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

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

[Ref [3]: 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 BSF, 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.1.1.0. 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.1.1.0. Section-4.4.3.

[Ref [62]: GSMA NG 133 Cloud Infrastructure Reference Architecture]

Section 10: Operating System

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 the BSF from operating properly. Therefore, counter measures 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 33.117-17.1.0 V.1.1.0. Section-4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of Internet Control Message Protocol version 4 (ICMPv4) and ICMPv6 packets which are not required for operation shall be disabled on the BSF.

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.

BSF 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

The BSF 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.1.1.0. Section-4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

Requirement:

BSF shall not support privilege escalation method in interactive sessions (both Command Line Interface (CLI) and Graphical User Interface (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.1.1.0. Section-4.2.4.1.2.1]

2.10.4 System Account Identification

Requirement:

Each system user account in BSF shall have a unique User ID (UID)with appropriate non-repudiation controls.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. 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:

1) IP Packet Forwarding between different interfaces of the network product.

2) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
3) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.)
4) 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.
5) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref [3]: TSDSI STD T1.3GPP 33.117-16.7.0 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:

The BSF 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.1.1.0. 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:

The BSF 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.1.1.0. 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 the BSF, 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.1.1.0. 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:

The BSF 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.1.1.0. Section-4.3.2.7]

2.10.10 SYN Flood Prevention

Requirement:

The BSF 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.1.1.0. 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.1.1.0. 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, BSF 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:

The BSF 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.

Section 11: Web Servers

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

2.11.1 HTTPS

Requirement:

The communication between BSF Web client and the BSF Web server shall be protected by 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.1.1.0. 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 BSF.

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.1.1.0. Section-4.2.5.2]

2.11.3 HTTPS input validation

Requirement:

The BSF 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.

The BSF 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.1.1.0. Section-4.2.5.4]

2.11.4 No System Privileges

Requirement:

No BSF 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.1.1.0. Section- 4.3.4.2]

2.11.5 No Unused HTTPS Methods

Requirement:

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

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. 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 the BSF 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.1.1.0. 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.1.1.0. 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.1.1.0. Section- 4.3.4.6]

2.11.9 No Execution of System Commands with SSI

Requirement:

If SSI is active, the execution of system commands shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.4.7]

2.11.10 Access Rights for Web Server Configuration

Requirement:

Access rights for BSF 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.1.1.0. 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 BSF web server shall be removed.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. 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.1.1.0. 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 BSF web server and the modules/add-ons used.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. 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 BSF 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 BSF web server shall be replaced by error pages defined by the OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.4.12]

2.11.15 Minimized File Type Mappings

Requirement:

File type or script-mappings that are not required for the BSF 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.1.1.0. 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 (e.g. via links or in virtual directories) reside in the BSF's web server's document directory.

In particular, the BSF 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.1.1.0. Section-4.3.4.14]

2.11.17 HTTP User Sessions

Requirement:

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

1) The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
2) The session ID shall be unpredictable.
3) The session ID shall not contain sensitive information in clear text (e.g. account number, social security, etc.).
4) In addition to the Session Idle Timeout, the BSF 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.
5) Session IDs shall be regenerated for each new session (e.g., each time a user logs in).
6) The session ID shall not be reused or renewed in subsequent sessions.
7) The BSF 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.
8) Where session cookies are used the attribute 'HttpOnly' shall be set to true.
9) Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
10) 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.

11) BSF shall not accept session identifiers from GET/POST variables.
12) BSF shall be configured to only accept server generated session ID's.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.2.5.3]

Section 12: General SBA/SBI Aspects

This general baseline requirements are applicable to all Network Functions (NFs) 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 BSF 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 BSF's filesystem or other resources loaded externally.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. 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.1.1.0. 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:

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

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.6.4]

2.12.4 Protection at the Transport

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 or above. Network functions shall support both server-side and client-side certificates.

Authentication between network functions within one PLMN can use the following method: -

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 V1.1.0. 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 V1.1.0. Section-4.2.2.2.3.1.
Ref [29]: RFC 6749 Oauth 2.0 IETF, October 2012, The OAuth 2.1 Authorization Framework, 2023.]

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 BSF.

The BSF shall never use the eval function to evaluate JSON data to prevent client-side JSON injections. BSF shall sanitize all data before serializing it to JSON, to prevent server-side JSON injections.

[Ref [44]: ENISA THREAT LANDSCAPE FOR 5G NETWORKS, December 2020]

Section 13: Other Security Requirements

2.13.1 Remote Diagnostic Procedure – Verification

Requirement:

If the BSF 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 the BSF System / Root password recovery.

2.13.3 Secure System Software Revocation

Requirement:

Once the BSF 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.

The BSF shall support a well-established control mechanism for rolling back to previous software image.

2.13.4 Software Integrity Check- Installation

Requirement:

BSF shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "ITSAR for Cryptographic Controls" only.

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

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section-4.2.3.3.5]

2.13.5 Software Integrity Check – Boot

Requirement:

The BSF 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:

The BSF shall support the mechanism to verify both the physical and logical interfaces 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 BSF 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

"The verification of the Client credentials assertion shall be performed by the receiving node, i.e., NRF or 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.
   If the receiving node is the NF Service Producer, the NF service Producer validates the expiration time and it may validate the timestamp.
c) 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 [27]: RFC 7515 JSON Web Signature (JWS).
Ref [28]: RFC 7519 JSON Web Token (JWT).]

Note: Not applicable to Release 16 implementation

2.13.9 Isolation of Compromised Element

Requirement:

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

[Ref [45]: ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section-4.1.3]

Chapter 3 - BSF Specific Security Requirements

3.1 Secure Communication on Nbsf Interfaces

Requirement:

The BSF interfaces with the AF, PCF, NEF, NWDAF and TSCTSF Network Functions using the service-based interface 'Nbsf_management', and with the UDR NF using the service-based interface, Nudr_DataRepository_Update within the PLMN.

The interfaces between the BSF and the NFs shall fulfill the following requirements:

a) Mutual authentication shall be performed between the BSF and NFs within the PLMN as applicable, using the "ITSAR for Cryptographic Controls" only.
b) All communication between the BSF and NFs shall be confidentiality, integrity and replay protected. If BSF endpoints are co-located with the NFs, the above two requirements may be satisfied by colocation.
c) The BSF shall provide confidentiality, integrity and replay protection for its internal communication over BSF internal network interfaces.

[Ref [2]: TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0 Section-5.9.2.4]

3.2 Secure Communication on the Diameter Interface

Requirement:

Following security measures shall be adopted for all communications and data transfer through Diameter Interface:

a) To remediate Diameter session vulnerabilities between BSF and the Application Function over Rx, Service Provider shall implement Diameter firewall to filter/block malicious Diameter traffic.

b) The Diameter interface shall be confidentiality, integrity and replay protected.

c) Traffic Protection TLS/DTLS 1.2 and above over TCP/SCTP or NDS/IP shall be implemented for the diameter interfaces between the BSF and the connected entities,

as applicable using the secure cryptographic controls prescribed in Table 1 of the latest document of "ITSAR for Cryptographic Controls".

1) The protection of the Diameter interface shall be supported for NDS/IP as specified in TS 33.210.

2) If (D)TLS is used, implementation and usage shall follow the profile given in clause 6.2 of TS 33.210 and clause 6.1.3a of TS 33.310.

3) A Security Gateway (SEG) shall be used to terminate the NDS/IP IPsec tunnels.

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

Ref [25]: RFC 6733 Diameter based Protocol.

Ref [58]: 3GPP TS 33.210, V17.1.0 (2022-09) Network Domain Security; IP layer security.

Ref [59]: 3GPP TS 33.310, V17.4.0 (2022-09) Network Domain Security; Authentication Framework.

Ref [30]: GSMA FS.19 Diameter Interconnect Security].

3.3 BSF Binding Database related Specific Security Requirements

3.3.1 Removal of Default Accounts in database

Requirement:

All default and anonymous accounts (e.g., test@localhost) that are not intended for normal operation of BSF bindings database shall be deleted.

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

3.3.2 Renaming of root/admin account in the database

Requirement:

The administrative (superuser) account on a BSF bindings database (used for database administration) shall not have a simple/well-known name such as 'root@localhost' in order to avoid exposing a highly privileged account with an easy to guess name.

3.3.3 No default databases in BSF Bindings

Requirement:

Default databases such as test, that are not required for normal operation of BSF binding databases shall be dropped.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.2.3]

3.3.4 Password management and validation policy for Database

Requirement:

BSF binding database shall only accept passwords that comply with the following complexity criteria:

a) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the network product). It shall not be possible setting this absolute minimum length to a lower value by configuration.
b) Comprising at least three of the following categories:
    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. @;!$.)

BSF binding database shall use a default minimum length of 10 characters. The special characters may be categorized in sets according to their Unicode category.

c) Following Password expiration and reuse policy is recommended:
    1) Password expiration: It is recommended to change the passwords annually.
    2) Password reuse restrictions: to prevent old passwords from being chosen again, reuse of last 5 passwords shall be denied.

d) A two-way authentication for the sensitive BSF database protection is highly recommended.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section-4.2.3.4.3.1

Ref [60] CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf].

3.3.5 Restricted access to sensitive Information

Requirement:

Access to sensitive information stored in tables and logs shall be restricted to only authorized accounts. Access to this table shall be restricted to only root/administrator account.

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section-4.2.3.2.3]

3.3.6 Encryption of the BSF Binding Database

Requirement:

The BSF database consists of sensitive data comprising user name, user ID, SUPI, GPSI, IPv4/IPv6 addresses of the UE etc. Hence, it must be protected in storage. BSF database shall be encrypted as applicable, using secure cryptographic controls prescribed in Table1 of the latest document of "ITSAR for Cryptographic Controls".

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.2.3]

3.3.7 BSF Database specific logging

Requirement:

a) Security events related to following database events shall be logged together with a unique reference (e. g. database name, user ID accessing the database) and the exact time the incident occurred.
    i) Database Management Server Login (success or error) events
    ii) Attempted/executed database statements/queries
b) Information available in the logs about authentication attributes shall be masked.
c) BSF shall support real time forwarding of security event logging data to an external system. Secure transport protocols shall be used in accordance with section 2.1.2 of the current document.

d) Log functions should support secure uploading of log files to a central location or to an external system for the BSF database that is logging.

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section-4.2.3.6]

3.3.8 User privileges

Requirement:

All BSF database server users shall perform only the operations that are permitted to them (as per the privileges assigned to them). For e.g., BSF database service shall support the following privileges:

a) Administrative privileges enable users to manage operation of the database server. These privileges are global because they are not specific to a particular database.
b) Database privileges apply to a database and to all objects within it. These privileges can be granted for specific databases, or globally so that they apply to all databases.
c) Privileges for database objects such as tables, indexes, views, and stored routines can be granted for specific objects within a database, for all objects of a given type within a database (for example, all tables in a database), or globally for all objects of a given type in all databases.

[[Ref [47]:
https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html]

3.3.9 Protection from attacks

Requirement:

a. BSF Sessions Binding Database shall be protected from database injection attacks.
b. Port used by the database service shall not be accessed by unauthorized entities. BSF Bindings database shall use a different port other than the default port for its connections.
c. BSF Sessions Binding Database shall recover securely from correction, loss or damage.
d. BSF Database shall support security mechanisms to protect from DDoS attacks.
e. Database systems shall provide security measures to deal with overload situations which may occur as a 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.

f. Potential protective measures shall include, but not limited, to the following:
    i) Use stored procedures instead of implementing Direct queries
    ii) The number of queries per account per hour may be restricted
    iii) The number of updates an account can issue per hour shall be restricted
    iv) The number of times an account can connect to the server per hour shall be restricted. The number of simultaneous connections to the server by an account (global max_user_connections value is 10).
    v) Validating and encoding all user inputs.
    vi) To mitigate Time of check to time of use attack (TOCTOU), a file shall be locked before the check, as opposed to afterwards so the resource, as checked, is the same as it is when in use.

[Ref [48]: https://owasp.org/www-community/attacks/SQL_Injection#

Ref [4]: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

Ref [54]: https://www.oracle.com/java/technologies/javase/seccodeguide.html.]

3.3.10 Unique Identity

Requirement:

All database accounts shall be uniquely identified (for e.g., username, hostname) by the BSF database server.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.2.4.2.2]

3.3.11 BSF Database Integrity

Requirement:

Systems and mechanisms shall be in place to ensure BSF binding database integrity. Service provider shall provide documentation on specific methods or approaches used to address BSF database integrity.

[Ref [56]: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/.]

3.3.12 BSF Database Availability

Requirement:

Systems and mechanisms shall be in place to ensure availability of BSF database. Service provider shall provide documentation on specific methods or approaches used to address the availability of BSF database.

[Ref [61]: https://docs.oracle.com/cd/B14117_01/server.101/b10726/hadesign.htm#i1006336.]

3.3.13 Secured BSF database backups:

Requirement:

The service provider shall provide mechanisms (such as high availability clusters and big data consistency) for data base backups, integrity and availability.

[Ref [61]: https://docs.oracle.com/cd/B14117_01/server.101/b10726/hadesign.htm#i1006336.]

3.4 Valid AF session

Requirement:

BSF shall be able to generate and send an error response to the AF containing the Experimental-Result-Code Attribute Value Pair (AVP) with the value REQUESTED _SERVICE_NOT_AUTHORIZED (5063) in case there's not a match for AVP values for Rx- AF application identifier and media type.

[Ref [49]: TSDSI STD T1.3GPP 29.214-17.4.0 V1.1.0 Section-4.4; Section-5.5]

Annexure-I (Definitions)

1. **5G Access Network**: An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network [1].
2. **5G System**: 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE [1].
3. **5QI:** 5G QoS Identifier(5QI) is a scalar that is used as a reference to a specific QoS forwarding behavior (e.g., packet loss rate, packet delay budget) to be provided to a 5G QoS Flow.
4. **Application identifier**: An identifier that can be mapped to a specific application traffic detection rule.
5. **Allowed NSSAI**: an NSSAI provided by the serving PLMN during e.g. a registration procedure, indicating the NSSAI allowed by the network for the UE in the serving PLMN for the current registration area.
6. **AUSF**: AUSF is a network function with which SEAF and UDM interact during the authentication of UE [1].
7. **Binding Support Management Service:** A binding support management service is provided by BSF [14].
8. **BSF**: BSF is a network function used for binding an Application Function (AF) request targeting a particular UE to a specific Policy Control Function (PCF) instance [15].
9. **BSF Group:** consists of one or multiple BSF Sets [11].
10. **BSF Group ID:** This refers to one or more BSF instances managing a specific set of SUPIs or GPSIs. A BSF Group consists of one or multiple BSF Sets [11].
11. **BSF Procedures:** BSF procedures concern the storage of binding information in the BSF, the retrieval of binding information from the BSF and the subscription to the notification of PCF registration/deregistration events from the BSF [12].
12. **DDoS**: DDoS is a distributed denial-of-service attack that renders the victim un-usable by the external environment.
13. **DRA**: A Diameter Routing Agent (DRA) is a functional element in a 3G or 4G (such as LTE) network that provides real-time routing capabilities to ensure that messages are routed among the correct elements in a network.
14. **GUTI**: The purpose of the GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity.
15. **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
16. **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
17. **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

18. **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
19. **Downlink:** Unidirectional radio link for the transmission of signals from a RAN access point to a UE. Also, in general the direction from Network to UE.
20. **DN Access Identifier** (DNAI)**:** Identifier of a user plane access to one or more DN(s) where applications are deployed.
21. **Identifiable person**: one who can be identified, directly or indirectly, in particular by reference to an identification number, name or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. NOTE: personal data can be gathered from user data and traffic data.
22. **Local access**: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from GNP'/NE's local hardware interface.
23. **Local Area Data Network**: a Data Network (DN) that is accessible by the UE only in specific locations, that provides connectivity to a specific DNN, and whose availability is provided to the UE.
24. **Local Break Out (LBO):** Roaming scenario for a PDU Session where the PDU Session Anchor and its controlling SMF are located in the serving PLMN (VPLMN).
25. **Local logical interface**: It is an interface that can be used only via physical connection to the Generic Network Product (GNP). That is, the connection requires physical access to the GNP. The entire protocol stack is considered to be part of the local logical interface. The entire protocol stack and the physical parts of the interface can be used by local connections. Local Logical Interfaces also include the local hardware interfaces and the Local Maintenance Terminal interface (LMT) of the GNP used for its maintenance through a console. i.e. Local logical interfaces include Operations, Administration and Maintenance (OAM) local console, LMT (Local Maintenance Terminal) interface and GNP local hardware interfaces. Attaching to a Local interface may cause execution of complex internal procedures in the GNP like loading USB device drivers, enumeration of attached devices, mounting file systems etc.
26. **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.
27. **Medium Access Control**: A sub-layer of radio interface layer 2 providing unacknowledged data transfer service on logical channels and access to transport channels.
28. **Mobility**: The ability for the user to communicate whilst moving independent of location.

29. **Mobility Registration update:** UE re-registration when entering a new Tracking Area (TA) outside the TA Identifier (TAI) List as specified in [3GPP TS 23.501, V1.5.0 (2017-11).
30. **Network Element**: A discrete telecommunications entity which can be managed over a specific interface e.g. the RNC.
31. **NG-RAN**: It is the radio access network introduced for accessing 5G.
32. **Node B**: A logical node responsible for radio transmission / reception in one or more cells to/from the User Equipment. Terminates the Iub interface towards the RNC.
33. **Non-Access Stratum**: Protocols between UE and the core network that are not terminated in the RAN.
34. **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.
35. **Packet:** An information unit identified by a label at layer 3 of the OSI reference model.
36. **A network protocol data unit (NPDU)**: Personal data: any information relating to an identified or identifiable natural person ('data subject').
    NOTE: personal data can be gathered from user data and traffic data.
37. **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 LMN. 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 types 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.
38. **PLMN Operator**: Public Land Mobile Network operator. The entity which offers telecommunications services over an air interface.
39. **Protocol Data Unit:** In the reference model for Open System Interconnect (OSI), a unit of data specified in an (N)-protocol layer and consisting of (N)-protocol control information and possibly (N)-user data.
40. **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.
41. **QoS profile**: a QoS profile comprises a number of QoS parameters. A QoS profile is associated with each QoS session. The QoS profile defines the performance expectations placed on the bearer network.

42. **QoS session**: Lifetime of PDP context. The period between the opening and closing of a network connection whose characteristics are defined by a QoS profile. Multiple QoS sessions may exist, each with a different QoS profile.
43. **Quality of Service**: 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;
    - service operability performance;
    - service accessibility performance;
    - service retainability performance;
    - service integrity performance; and
    - other factors specific to each service.
44. **Radio link**: A "radio link" is a logical association between single User Equipment and a single RAN access point. Its physical realization comprises one or more radio bearer transmissions.
45. **Radio Resource Control**: A sublayer of radio interface Layer 3 existing in the control plane only which provides information transfer service to the non-access stratum. RRC is responsible for controlling the configuration of radio interface Layers 1 and 2.
46. **Registered PLMN** (RPLMN): This is the PLMN on which the UE has performed a location registration successfully.
47. **Registration Area**: A (NAS) registration area is an area in which the UE may roam without a need to perform location registration, which is a NAS procedure.
48. **Remote Access**: The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.
49. **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]
50. **Serving Network:** The serving network provides the user with access to the services of home environment.[51]

Annexure-II (Acronyms)

5GC	-	5G Core Network
5GMM	-	5GS Mobility Management
5GS	-	5G System
5GSM	-	5G Session Management
AF	-	Application Function
AKA	-	Authentication and Key Agreement
AKA'	-	AKA Prime
AKMA	-	Authentication and Key Management for Applications
ARP	-	Address Resolution Protocol/Allocation and Retention Priority
ARPF	-	Authentication Credential Repository and Processing Function
AS	-	Access Stratum
ATSSS	-	Access Traffic Steering, Switching, Splitting
AUSF	-	Authentication Server Function
AUTS	-	Authentication failure message with synchronization failure
AVP	-	Attribute Value Pairs
BSF	-	Binding Support Function
CHF	-	Charging Function
CIoT	-	Cellular Internet of things
CLI	-	Command Line Interface
CM	-	Connection Management
CP	-	Control Plane
CVE	-	Common Vulnerabilities and Exposures
CWE	-	Common Weakness Enumeration
CVSS	-	Common Vulnerability Scoring System
DCCF	-	Data Collection Coordination Function
DDoS	-	Distributed Denial of Service
DL	-	Downlink
DN	-	Data Network
DNN	-	Data Network Name
DRA	-	Diameter Routing Agent
DTLS	-	Datagram Transport Layer Security
EAP	-	Extensible Authentication Protocol
EASDF	-	Edge Application Server Discovery Function
EPC	-	Evolved Packet Core
EPS	-	Evolved Packet System
gNB	-	5G Next Generation base station
GNP	-	Generalized Network Product

GTP-C	-	GPRS Tunneling Protocol-Control Plane
GTP-U	-	GPRS Tunneling Protocol-User Plane
GUI	-	Graphical User Interface
GUTI	-	Globally Unique Temporary Identifier
GVNP	-	Generalized Virtual Network Product
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
ICMP	-	Internet Control Message Protocol
IE	-	Information Element
IMS	-	IP Multimedia Subsystem
IMPI	-	IMS Private Identity
IMPU	-	IMS Public Identity
IP	-	Internet Protocol
IPUPS	-	Inter-PLMN User Plane Security
IPX	-	IP exchange
ISO	-	International Standardization Organization
ISO-OSI	-	ISO-Open System Interconnection
JSON	-	JavaScript Object Notation
JWS	-	JSON Web Signature
JWT	-	JSON Web Token
LBO	-	Local Breakout
LMF	-	Location Management Function
MA PDU	-	Multiple Access PDU
ML	-	Machine Learning
N3IWF	-	Non-3GPP Interworking Function
NAS	-	Non-Access Stratum
NEF	-	Network Exposure Function
NF	-	Network Function
NG	-	Next Generation
ng-eNB	-	Next Generation e-NodeB
NG-RAN	-	Next Generation Radio Access Network
NRF	-	Network Repository Function
NVD	-	National Vulnerability Database
NWDAF	-	Network Data Analytics Function
NW-TT	-	Network -side TSN Translator
O&M	-	Operations and Maintenance
OAM	-	Operations Administration Maintenance
OEM	-	Original Equipment Manufacturer
OS	-	Operating System
PCF	-	Policy Control Function

PDR	-	Packet Detection Rule
PDU	-	Protocol Data Unit
PFCP	-	Packet Forwarding Control Protocol
PFD	-	Packet Flow Descriptor
PLMN	-	Public Land Mobile Network
PRINS	-	Protocol for N32 Interconnect Security
PSA	-	PDU Session Anchor
QoS	-	Quality of Service
RAM	-	Random Access Memory
RAN	-	Radio Access Network
RAT	-	Radio Access Technology
RES	-	Response
REST	-	Representational State Transfer
RFC	-	Request For Comments
RM	-	Registration Management
RRC	-	Radio Resource Control
S-NSSAI	-	Single - Network Slice Selection Assistance Information
SBI	-	Service Based Interfaces
SCP	-	Service Communication Proxy
SDF	-	Service Data Flow
SEAF	-	Security Anchor Function
SEPP	-	Security Edge Protection Proxy
SIDF	-	Subscription Identifier De-Concealing Function
SMF	-	Session Management Function
SNPN	-	Stand Alone Non-Public Network
SSC	-	Session and Service Continuity
SUCI	-	Subscription Concealed Identifier
SUPI	-	Subscription Permanent Identifier
TA	-	Tracking Area
TNGF	-	Trusted Non-3GPP Gateway Function
TSCTSF	-	Time Sensitivity Communication and Time Synchronization Function
TSC	-	Time Sensitive Communication
TSN	-	Time Sensitive Networking
TSTL	-	Telecom Security Testing Laboratory
UDM	-	Unified Data Management
UDR	-	Unified Data Repository
UE	-	User Equipment
UL	-	Uplink
UPF	-	User Plane Function
URI	-	Uniform Resource Identifier

URL	-	Uniform Resource Locator
URLLC	-	Ultra Reliable Low Latency Communication
URSP	-	UE Route Selection Policy
VN	-	Virtual Network
WLAN	-	Wireless Local Area Network

Annexure-III (References)

1. TSDSI STD T1.3GPP 23.501-17.4.0 V1.0.0 “System architecture for the 5G System 5GS)”
2. TSDSI STD T1.3GPP 33.501-17.4.0 V1.0.0 “Security Architecture and procedures for 5G System”
3. TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0 “Catalogue of General Security Assurance Requirements”
4. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html.
5. https://owasp.org/www-project-top-ten/.
6. https://owasp.org/www-project-api-security/.
7. RFC 8915 - Network Time Security for the Network Time Protocol (NTP).
8. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.
9. https://nvd.nist.gov/vuln-metrics/cvss
10. 3GPP TS 23.501 V1.5.0 (2017-11) Release 15; First existence of BSF specification; “System architecture for the 5G System (5GS)”.
11. 3GPP TS 23.501 Ver 17.5.0 (2022-07), Support for framed routing, NF services provided by BSF, “System architecture for the 5G System (5GS)”.
12. 3GPP TS 29.513 Ver 17.0.0, (2020-09), covering BSF; BSF procedures; Binding Information creation; “Policy and Charging Control signalling flows and QoS parameter mapping”.
13. 3GPP TS 29.512 Ver 16.5.0, 5G System; “Binding Support Management Service”
14. 3GPP TS 29.521 V17.0.0 (2021-03) 5G System; “Binding Support Management Service”.
15. 3GPP TS 23.503 V16.12.0 (2022-06); “Policy and charging control framework for the 5G System (5GS)”.
16. 3GPP TS 29.201 V17.0.0 (2021-12) “Representational State Transfer (REST) reference point between Application Function (AF) and Protocol Converter (PC)”
17. 3GPP TS 23.502 Ver 16.7.0 (2021-01)
18. 3GPP TS 23.501 V18.1.0 (2023-03)
19. 3GPP TS 23.501 V18.1.0 (2023-03)
20. 3GPP TS 29.211 V6.4.0 (2007-06) “Rx Interface and Rx/Gx signalling flows”.
21. 3GPP TS 23.228 V6.16.0 (2007-03), “IP Multimedia Subsystem (IMS)”.
22. ETSI TS 129 211 V6.2.0 (2005-09), ” Rx Interface and Rx/Gx signaling flows”.
23. TSDSI RPT T1.3GPP 33.926-14.0.0 V1.0.0”, “Security Assurance Specification”, (SCAS)\threats and critical assets in 3GPP network product classes.
24. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
25. IETF-RFC 6733, Diameter Base Protocol, Erricson Research Centre, Nokia Research Centre, V. Fazardo Ed, Oct 2012.
26. RFC 7540 Hypertext Transfer Protocol Version 2 (HTTP/2).
27. RFC 7515 JSON Web Signature (JWS).
28. RFC 7519 JSON Web Token (JWT).

29. RFC 6749 Oauth 2.0 [IETF] October 2012, The OAuth 2.1 Authorization Framework, 2023.
30. GSMA FS.19, “Diameter Interconnect Security”.
31. GSMA FS.11, “SS7 Interconnect Security Monitoring and Firewall Guidelines
32. “Security Guidance for 5G Cloud Infrastructure” by NSA & CISA https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf]
33. https://www.broadforward.com/binding-support-function-bsf/
34. https://www.nokia.com/networks/core-networks/cloud-signaling-director/-bsf
35. https://www.ericsson.com/en/blog/2019/10/you-need-a-robust-signaling-solution-in-5g-too/bsf.
36. https://www.amazon.in/5G Wireless-Comprehensive-Introduction-William-Stallings/dp/0136767141.
37. https://www.linkedin.com/pulse/introduction-5g-core-service-based-architecture-sba-marin ivezic?trk=read_related_article-card_title-BSF.
38. http://www.dba-oracle.com/t_password_security.htm.
39. https://ieeexplore.ieee.org/document/9952199/ A Security Assessment of HTTP/2 Usage in 5G Service Based Architecture, N. Wehbe, H. Almandine, M. Pourzandi, E. Bou-Harb, and C.i Assi, 15th November, 2022.
40. Diameter-2018-eng.pdf (gsma.com), Diameter Vulnerabilities Exposure Report, 2018.
41. ENISA-Signaling Security in Telecom SS7/Diameter/5G EU level assessment of the current situation MARCH 2018.
42. National Informatic Centre (NIC) guidelines on Cybersecurity. https://guidelines.india.gov.in/guidelines/#cybersecurityGuidelines
43. Controller General of Defence Accounts, Govt. of India, “Information Security Policy Version 1”, https://cgda.nic.in/circulars/1SecurityPolicy%20version%201.0.pdf.
44. ENISA THREAT LANDSCAPE FOR 5G NETWORKS, December 2020.
45. ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section 4.1.3]
46. https://www.nokia.com/networks/asservice/saas/securitywp/?did=D000000051 82&gclid=EAIaIQobChMIgJPpwv_wIV1HJ9Ch062grIEAAYASAAEgIWavD_BwE, Demystifying SaaS and public cloud security with Google cloud, Amazon AWS, Microsoft Azure and Nokia, White Paper, 2022.
47. https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html]
48. https://owasp.org/www-community/attacks/SQL_Injection#
49. TSDSI STD T1.3GPP 29.214-17.4.0 V1.1.0, “Policy and Charging Control over Rx reference point”.

50. ENISA Recommendation “Standardization in support of the cybersecurity certification”, Dec 2019.
51. 3GPP TR 21.905 V17.1.0 (2021-12) “Vocabulary for 3GPP Specifications.
52. http://www.dba-oracle.com/t_password_security.htm.
53. https://www.techtarget.com/searchsecurity/answer/How-to-mitigate-the-risk-of-a-TOCTTOU-attack.
54. https://www.oracle.com/java/technologies/javase/seccodeguide.html.
55. TSDSI STD T1.3GPP 33.106-14.1.0 V1.0.0, Technical Standard, Lawful interception requirements.
56. https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/.
57. https://www.techtarget.com/searchoracle/tip/The-basics-of-Oracle-database-availability#:~.
58. 3GPP TS 33.210, Version 17.1.0, (2022-09) “Network Domain Security (NDS); IP network layer security”.
59. 3GPP TS 33.310, Version 17.4.0, (2022-09) “Network Domain Security (NDS), Authentication Framework (AF)”.
60. CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf.
61. https://docs.oracle.com/cd/B14117_01/server.101/b10726/hadesign.htm#i1006336.
62. GSM Association Non-confidential Official Document NG.133,” Cloud Infrastructure Reference Architecture”, managed by OpenStack;version 1.0, 22 February, 2022.