Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

Charging Function (CHF) of 5G

ITSAR Number: ITSAR111172312

ITSAR Name: NCCS/ITSAR/Core Equipment/5G Sub-systems/Charging Function (CHF) of 5G

Date of Release: 29.12.2023 Version: 1.0.0

Date of Enforcement:

MTCTE के तहत जारी:
Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत
National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

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

Document History

Sr No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Charging Function (CHF) of 5G	ITSAR111172312	1.0.0	29.12.2023	First release

Table of Contents

A) Outline

The objective of this document is to present comprehensive, country-specific security requirements for the Charging Function (CHF), a network function of the 5G Core. The CHF is a part of the Converged Charging System (CCS) of 5G. Convergent charging is an aggregation of online and off-line charging systems to address the new and emerging 5G monetization use cases. The 3GPP charging function (CHF) collects all network and service usage data. CHF functionalities include providing quota management, re-authorization triggers, notifications when the charging domain determines to terminate the charging service, receiving service usage report from NF service consumers and Charging Data Records (CDR) generation for charging events received from Charging Trigger Function (CTF).

The specifications produced by various regional/international standardization bodies/organizations/associations like 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, CHF overview and its functionalities, Logical ubiquitous charging architecture and information flows for 5G systems; service based representation; reference point representation, high level overall charging architecture and information flows, CHF interfaces, coexistence scenarios and interworking with EPC, roaming scenarios and then proceeds to address the common and entity specific security requirements of CHF related to the SBI based interface, Diameter and GTP' based interfaces and secure CDR storage/transfer and security in roaming scenarios.

B) Scope

This document targets on the security requirements of the 5G Core CHF 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

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).

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.

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 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.

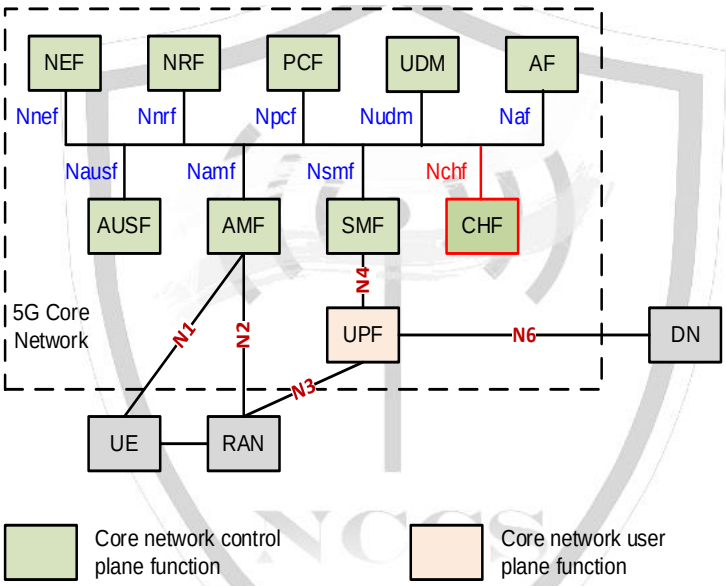

Figure 1: Service based architectural view of 5GS
[Adapted from: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

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 a reference point representation for a few functions of the core network. Point to point reference points are shown between two network functions, for example N40 between CHF and SMF.

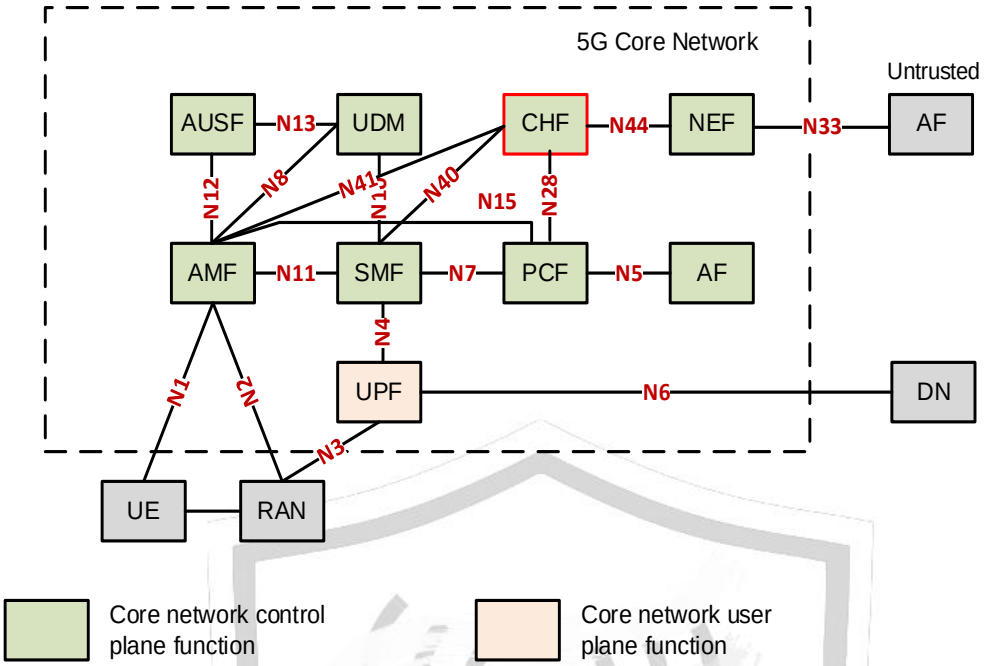

Figure 2: Reference point representation for 5GS
[Adapted from: TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0]

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.

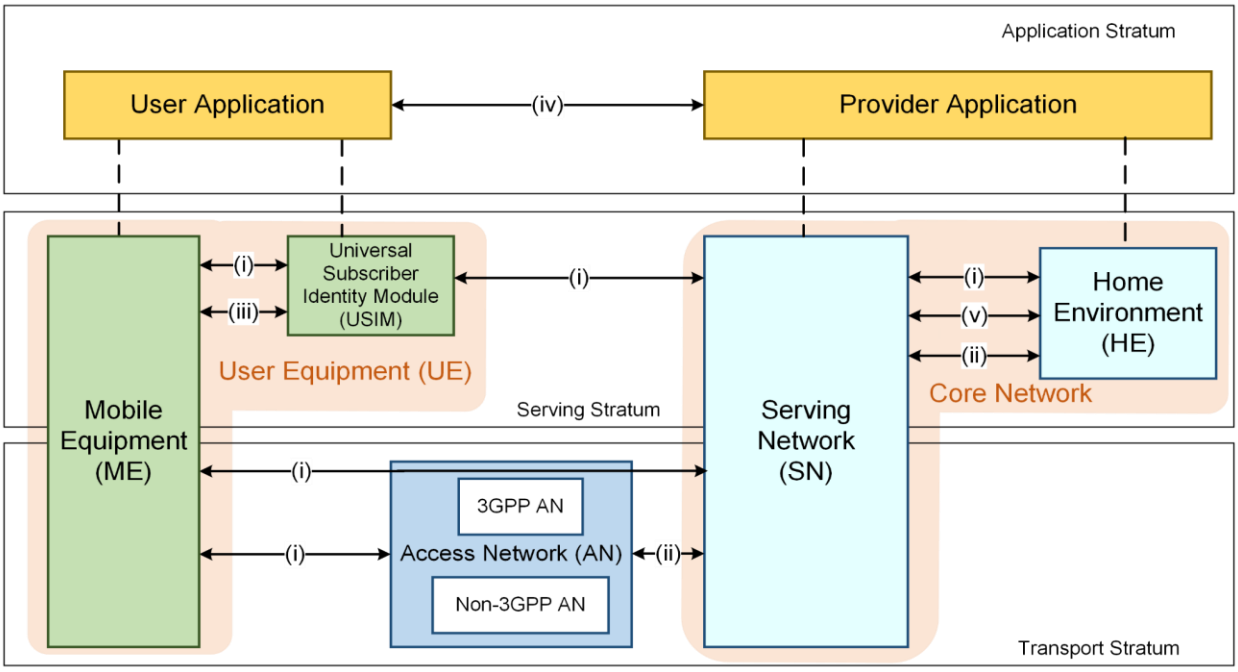

Figure 3: Overview of the security architecture [Adapted from: TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0]

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 Charging Function are covered in the present document. The following sections cover the overview of the CHF along with its security aspects.

Charging Function (CHF)

The 5G core Charging Function, is a part of the converged charging system (CCS). CCS is an aggregation of online and off-line charging systems, to address the new and emerging 5G monetization use cases. The Converged Charging System (CCS) consists of four distinct modules, the CHF, Account Balance Management Function (ABMF), Charging Gateway Function (CGF) and the Rating Function (RF).

The CHF consists of Online Charging Function (OCF) and Charging Data Function (CDF).

a) Online Charging Function (OCF), provides quota management functionality under Credit-Control terminology.

b) Charging Data Function (CDF), provides Charging Data Records (CDRs) generation functionality for charging events received from the Charging Trigger Function (CTF) or Charging Exposure Function (CEF) via Nchf.

Functionalities of the CHF

CHF functionalities include

a) Providing quota management under Credit-Control terminology,

b) Re-authorization triggers,

c) Notifications when the charging domain determines to terminate the charging service,

d) Receiving service usage report from NF service consumers and CDR generation for charging events received from the Charging Trigger Function (CTF).

Charging Mechanisms

3GPP networks provide functions that implement offline and/or online charging mechanisms on the network domain (e.g. EPC), subsystem (e.g. IMS) and service (e.g. MMS) levels. In order to support these charging mechanisms, the network performs real-time monitoring of resource usage on the above three levels in order to detect the relevant chargeable events.
Examples of network resource usage are a) voice call of a certain duration, b) transport of a certain volume of data, or c) submission of a Multimedia of a certain size. The network resource usage requests may be initiated by the UE (Mobile Originated case) or by the network (Mobile Terminated case).

The three types of charging mechanisms are:

1) **Offline Charging**: In offline charging, the resource usage is reported from the network to the Billing Domain (BD) after the resource usage has occurred.
2) **Online charging:** In online charging, a subscriber account, located in an Online Charging System (OCS) or Converged Charging System (CCS), is queried prior to granting permission to use the requested network resource(s). Offline and online charging may be performed simultaneously and independently for the same chargeable event.
3) **Converged charging:** Converged charging is a process where online and offline charging are combined. The charging information is utilized by CCS in one converged charging service which offers charging with and without quota management, as well as charging information record generation.

Common Charging architecture

An overview of the logical ubiquitous charging architecture and the information flows for converged offline and online charging in service-based interface for 5G systems and Edge Computing enabling sub-systems are depicted in Figures 1 & 2.

Figure 1 provides the overview in service-based representation. The CHF communicates with the AMF, SMF, SMSF, NEF, IP Multimedia Source (IMS) node, 5G Direct Discovery Name Management Function (DDNMF), Edge Enable Server (EES) and PCF over the Nchf service-based interface.

The Nchf Spending Limit control service is exposed by CHF and consumed by the PCF.

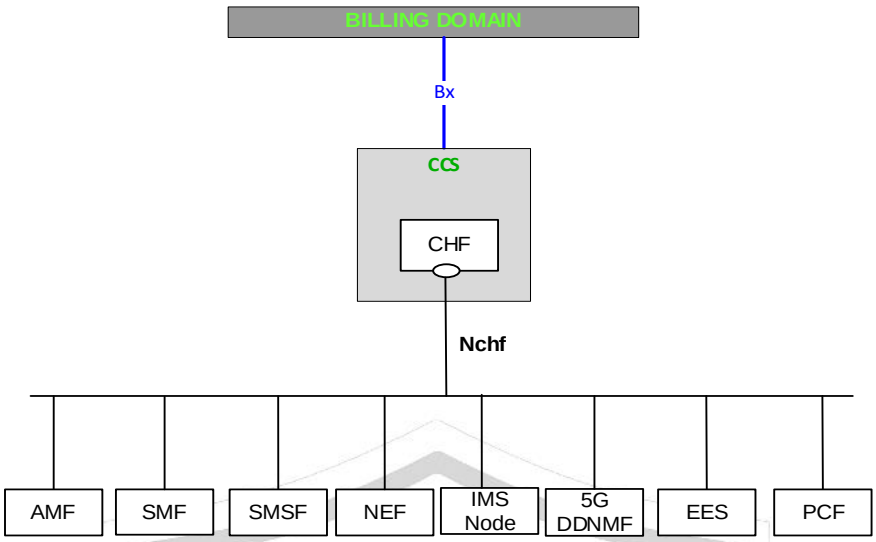

Figure 1: Logical ubiquitous charging architecture and information flows for 5G systems – service-based representation [Reference: Fig:4.2.3.1 TSDSI STD T1.3GPP 32.240-17.8.0 V1.3.0]

Figure 2 provides the charging architecture overview in reference point representation:

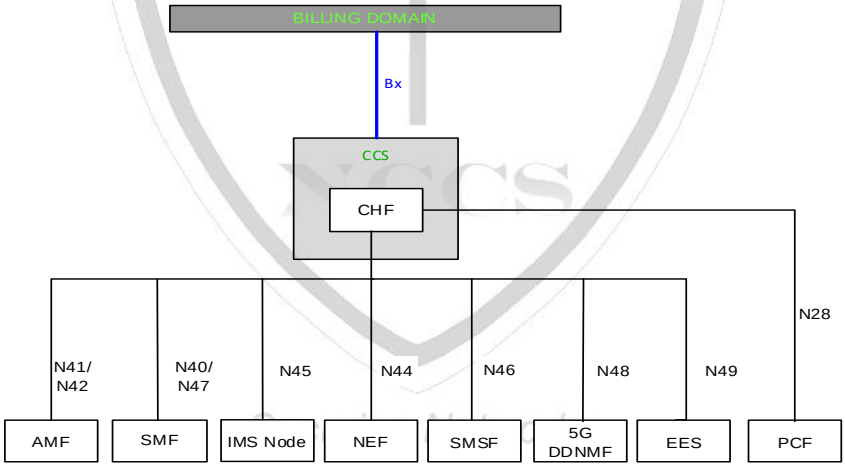

Figure 2: Logical ubiquitous charging architecture and information flows for 5G systems: Reference point representation [Reference: Fig:4.2.3.2 TSDSI STD T1.3GPP 32.240-17.8.0 V1.3.0]

Converged charging functions

An overview of the converged charging architecture used for 5G systems is depicted in Figure 3. It shows the logical charging functions in the network and interfaces between these functions and to the Billing Domain.

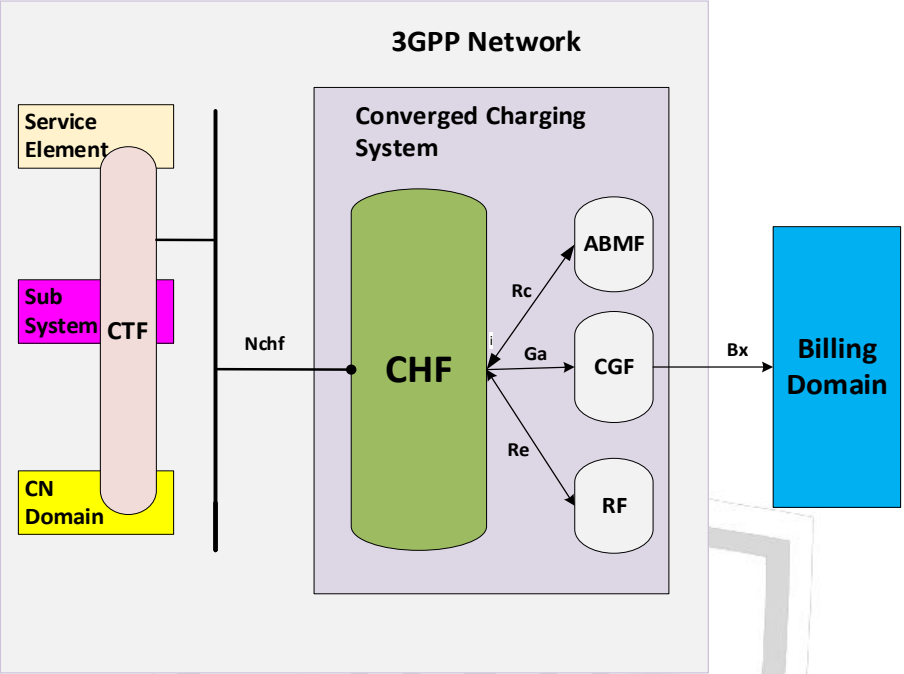

Figure 3: Logical ubiquitous converged charging architecture [Adapted from: Fig: 4.3.3.0.1 TSDSI STD T1.3GPP 32.240-17.8.0 V1.3.0]

Brief working of these functions and reference points is as follows:

1) Charging Trigger Function (CTF): The Charging Trigger Function (CTF) interacts with the CHF of the Converged Charging System using the Nchf interface for consuming CHF services.
    a) The converged charging (Nchf_Converged Charging service) operates:
        i) with quota management (online charging);
        ii) without quota management (offline charging);
    b) offline only charging (Nchf_Offline Only Charging service).

The behavior of the Charging Trigger Function (CTF) embedded in the service element, sub-system component or Core Network element is specified in the respective middle tier charging specifications.

2) The Converged Charging System (CCS): The Converged Charging System (CCS) consists of four distinct modules, namely the CHF, the Account Balance Management Function (ABMF), the Charging Gateway Function (CGF) and the Rating Function (RF). The converged charging system interacts with CTF using Nchf interface and interacts with the BD using Bx interface.

3) Charging Function (CHF): The CHF includes OCF, providing quota management functionality under Credit-Control terminology and CDF providing CDRs generation functionality for charging events received from the CTF or CEF via Nchf.

4) Charging Gateway Function (CGF): The Charging Gateway Function (CGF) forms part of a mobile service providers billing domain, designed to translate CDRs generated by the network into a format suitable for the billing system.

5) Charging Enablement Function (CEF): The Charging Enablement Function (CEF) is a consumer of Nchf charging services, and for the purpose of charging information collection, may consume management services, services exposed by other network functions or both.

6) The Rating Function (RF): The Rating Function (RF) determines the value of the network resource usage (described in the charging event in Annexure I. received by the OCF from the network) on behalf of the OCF. The OCF provides the necessary information, obtained from the charging event, to the RF and receives in return the rating output (monetary or non-monetary units), via the Re reference point. The Rating Function handles ratable instances, such as:

   a) Rating of data volume (e.g., based on charging initiated by an access network entity, i.e., on the bearer level);

   b) Rating of session / connection time (e.g., based on charging initiated by a Session Initiated Protocol (SIP) application, i.e., on the subsystem level);

   c) Rating of service events (e.g., based on charging of web content or Multimedia System (MMS), i.e., on the service level).

7) Account Balance Management Function: The Account Balance Management Function (ABMF) is the location of the subscriber's account balance within the OCS or the CCS.

8) Reference points:
   sRf: The Rf reference point supports interactions between a CTF and a CDF. The following information may flow across this reference point in real-time:
   i) Charging events for offline charging from the CTF to the CDF;
   ii) Acknowledgements for these events from the CDF to the CTF.

The protocol(s) crossing this reference point shall support the following capabilities:

1) Real-time transactions;

2) Stateless mode ("event-based charging") and stateful mode (“session-based charging”) of operation;
3) Provide its own reliability mechanisms, e.g., retransmission of charging events, to run also on unreliable transport.
    a) Ga: The Ga reference point supports interaction between a CDF of CHF and CGF. The following information may flow across this reference point:
        1) CDRs are sent from the CDF to the CGF;
        2) Acknowledgements for these CDRs are returned from the CGF to the CDF.
        3) Redirection of CDRs to another CGF.
        4) Detect communication failures between the communicating peers, using echo messaging.
        5) Advertise to peers about its CDR transfer capability (e.g., after a period of service downtime).
        6) Prevents duplicate CDRs that might arise due to redundancy operations.

The protocol(s) crossing this reference point support the following capabilities:

- Near real-time transactions;
- Send one or more CDRs in a single request message;
- Changeover to secondary destinations (alternate CGFs) in case of the primary CGF not being reachable;
- Provide its own reliability mechanisms, e.g., retransmission of charging events, to run also on unreliable transport.

a) Bx: The Bx reference point supports interactions between a CGF and the BD. The information crossing this reference point is comprised of CDR files. A common, standard file transfer protocol (e.g., File Transfer Access and Management (FTAM), File Transfer Protocol (FTP)) is used, including the transport mechanisms specified for the selected protocol.
b) Re: The Re reference point supports interaction between the OCF of CHF and a Rating Function (RF), in order to determine the value of chargeable events in terms of monetary or non-monetary units.

Rc: The Rc reference point allows the interactions between the OCF of CHF and an Account Balance Management Function (ABMF) in order to access the account of the subscriber on the OCS.

High level Overall Charging Architecture

The overall logical charging architecture is shown in Figure 4.

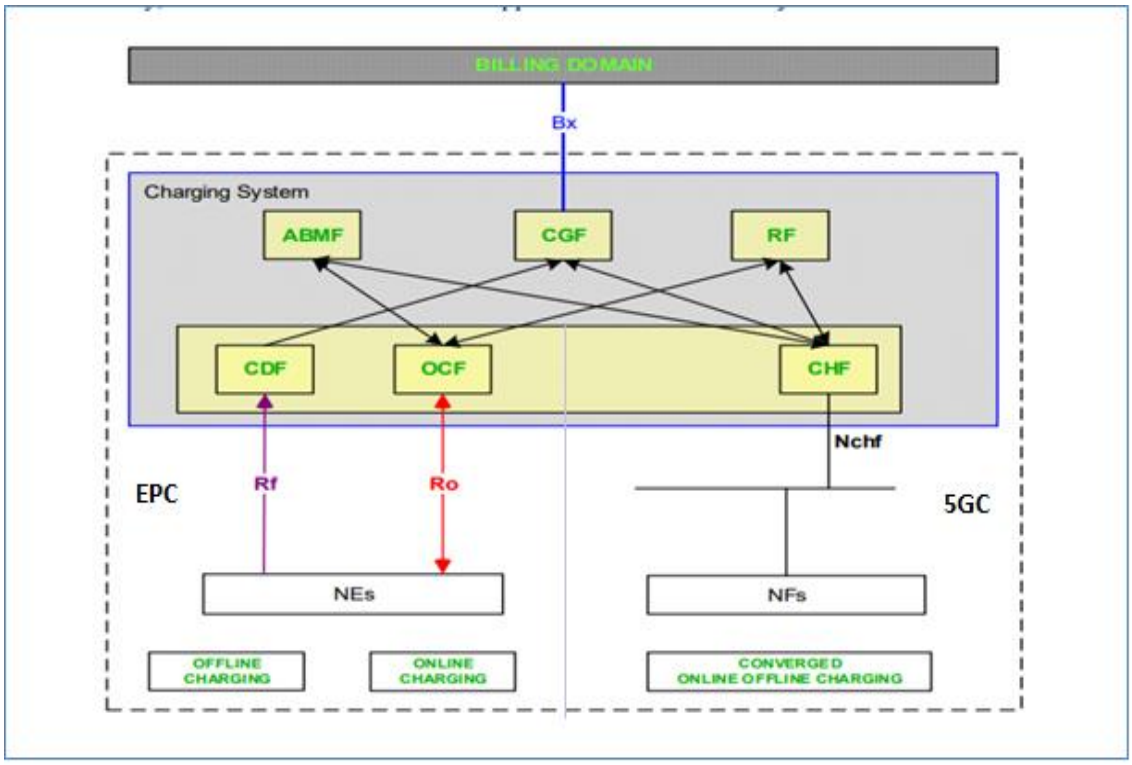

Figure 4: High level overall charging architecture and information flows [Adapted from: Fig. E.2.1.1: TSDSI STD T1.3GPP 32.240-17.8.0 V1.3.0]

The Rf and Ro reference points are applicable to General Packet Radio Service (GPRS), Evolved Packet Core (EPC) or IP Multimedia System (IMS) node Network Elements only.

The Nchf interface is applicable to 5G Core Network Functions only.

When the target charging system (i.e. 5G CCS or EPC OCS/OFCS) needs to support termination of a reference point or interface from the opposite type of core network (i.e. Ro/Rf or Nchf) implementations need to include interworking between the HTTP used by Service Based Interface and the Diameter protocol.

CHF- Roaming Scenario

In case of roaming scenario, wholesale charging for 5G data connectivity is provided by the visited Mobile Network Operator (MNO) to the home Mobile Network Operator, in local breakout case. Charging information is generated in the home MNO for retail purposes.

The following two figures, Figure 5 & 6 depict the roaming 5G data connectivity scenario in service-based representation and reference point representation:

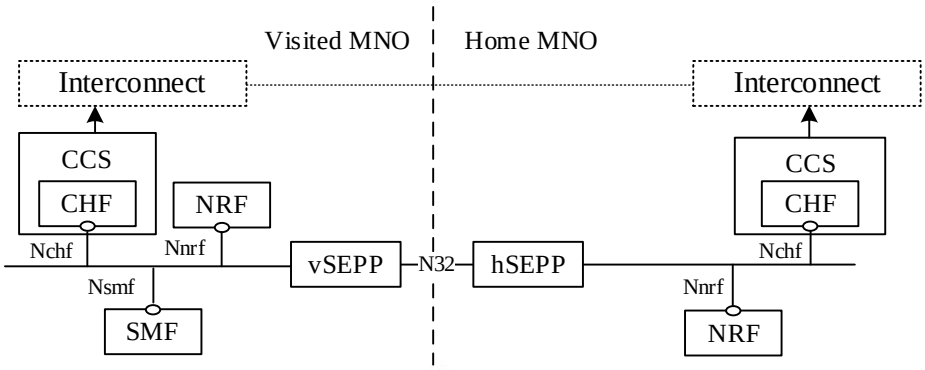

Figure 5: Roaming 5G data connectivity scenario in service-based interface representation: [Reference: 3GPP TS 28.827 V1.9.0 (2023-05) Release 17, "Study on 5G charging for additional roaming scenarios and actors"]

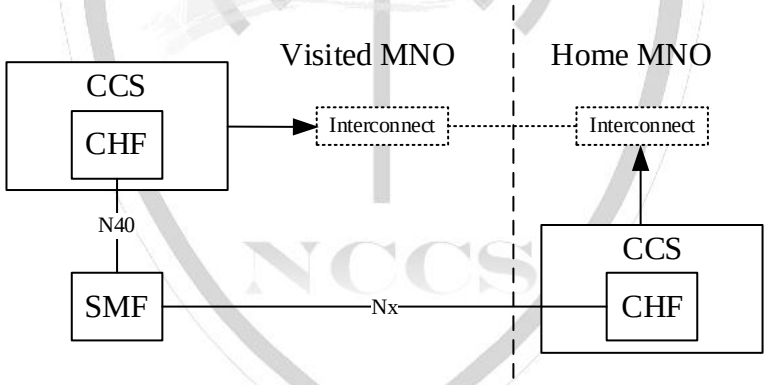

Figure 6. Roaming 5G data connectivity scenario in reference point representation: [Reference: 3GPP TS 28.827 V1.9.0 (2023-05) Release 17, "Study on 5G charging for additional roaming scenarios and actors "]

CHF Security Aspects

The Charging Function is a part of the Converged Charging System (CCS) in the Control Plane of the 5G Core Network. The security requirements of CHF are:

GTP Prime (GTP') based Interface related:

The CHF transfers Charging Data Records over the GTP' based Ga interface to the Charging Gateway Function (CGF). For protection of information between the CHF and CGF, secure communication between the two NFs needs to be ensured.

Diameter Interface related:

The diameter interface is vulnerable to threats and Distributed Denial of Service (DDoS attacks), which need to be addressed. CHF uses the diameter interfaces Rc and Re.

i) Rc Interface is used between CHF and the Account Balance Management Function (ABMF).
ii) Re interface is used between CHF and the Rating Function (Rating Function) involving transfer of resource usage data and monetary/non-monetary units.

Secure exchange of data/tariff/UE credentials are of utmost importance.

Preservation of charging data record files:

The CHF generates Charging Data Records consisting of sensitive UE data, personal privacy records and vital credentials with monetary value. Secure Storage/Transfer of information/data/CDRs is essential.

Chapter 2 - Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Authentication for Product Management and Maintenance interfaces

Requirement:

CHF shall support mutual authentication of entities on management interfaces, the authentication mechanism can rely on the management protocols used for the interface or other means.
Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecom Security Assurance Requirements (ITSAR) for Cryptographic Controls shall only be used for 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:

CHF management traffic (information exchanged during interactions with operations, administration and Management (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 Role-based access control policy

Requirement:

CHF 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 operations, 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 CHF 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

2.1.4 User authentication - Local/Remote

Requirement:

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

Authentication attributes include

a) Cryptographic keys
b) Token
c) Passwords

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

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

2.1.5 Remote login restrictions for privileged users

Requirement:

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

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

[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 CHF.

CHF 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.

CHF 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 2.2: 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 CHF supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services), then the communication between CHF and the external authentication entity shall be protected using the authentication and elated 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 CHF. 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 CHF. 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 CHF 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 CHF). 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 CHF.

(e) When a user is changing a password or entering a new password, the CHF /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 CHF shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. CHF 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 CHF shall store at least the three previously set passwords. The maximum number of passwords that the CHF 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.
CHF 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 CHF.
The minimum password age shall be set as one day i.e. recycling or flipping of passwords to immediate return to favourite 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-4.2.3.4.3.2

Ref [17]: 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. CHF 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 [17]: CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf]

Section 2.3: Software Security

2.3.1 Secure Update

Requirement:

(a) Software package integrity shall be validated during the software update stage.
(b) CHF 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 CHF 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) CHF 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 CHF 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 CHF software which includes OEM developed code, third party software and opensource code libraries used/embedded in the CHF.
    ii) The CHF 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 CHF 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 CHF is free from all known malware and backdoors as on the date of offer of the CHF to designated TSTL, for testing and shall submit their internal Malware Test Document (MTD) of the CHF 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 CHF shall not be present/configured.
Orphaned software components/packages shall not be present in the CHF.
OEM shall provide the list of software that are necessary for CHF's operation.
In addition, OEM shall furnish an undertaking as "CHF does not contain software that is not used in the functionality of the CHF."

[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:

CHF 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 CHF 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.

- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Telnet

- rlogin, Rate Control Protocol (RCP), Remote Shell Protocol (RSH)
- HTTP
- Simple Network Management Protocol (SNMP) v1 and v2
- SSHv1
- Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- Bootstrap Protocol (BOOTP) server
- Discovery protocols (Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP))
- IP Identification Service (Identd)
- Packet Assembler/Disassembler (PAD)
- 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 CHF 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 CHF 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 CHF shall establish a secure communication channel through standard interface with the Network Time Protocol (NTP) / Precision Time Protocol (PTP) server as per appropriate TEC ER (Essential Requirement) document.

CHF 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 CHF 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 CHF 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 CHF 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. Secured Shell (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 CHF'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 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e. the software and hardware functions which are not needed for operation or functionality of the CHF shall be permanently deactivated. Permanently means that they shall not be reactivated again after a CHF 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 CHF 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 CHF.
EXAMPLE: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the CHF.

[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. Applicable only when GVNP Type3 product can be used.

2.4.2 No unsupported components

Requirement:

OEM shall ensure that the CHF 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. Applicable only when GVNP Type3 product can be used.

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

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

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

Section 2.5: User Audit

2.5.1 Audit trail storage and protection

Requirement:

The security event log shall be access controlled (file access rights), such 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 CHF shall log all important Security events with unique System Reference details as given in the table below:
CHF shall record within each audit record at least information pertaining to date and time of the event, type of event, subject identity, protocol, service or program used for access, source and destination IP addresses & ports and the outcome (success or failure) of the event.

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

Sl No	Event Types (Mandatory or Optional)	Description	Event data to be logged
1	Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the CHF.	Username
			Source (IP address) if remote access
			Outcome of event (Success or failure)
			Timestamp
2	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
3	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
4	Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space,	Value exceeded
			Value reached
			(Here suitable threshold values shall be defined depending on the individual system.)

		CPU load over a longer period have exceeded their	Outcome of event (Success or failure)
			Timestamp
5	Configuration change (Mandatory)	Changes to configuration of the CHF.	Change made
			Timestamp
			Outcome of event (Success or failure)
			Username
6	Reboot/shutdown/crash (Mandatory)	This event records any action on the network device/CHF that forces a reboot or shutdown OR where the network device/CHF has crashed.	Action performed (boot, reboot, shutdown, etc.)
			Username (for intentional actions)
			Outcome of event (Success or failure)
			Timestamp
7	Interface status change (Mandatory)	Change to the status of interfaces on the network device/CHF (e.g. shutdown)	Interface name and type
			Status (shutdown, down, missing link, etc.)
			Outcome of event (Success or failure)
			Timestamp
8	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
9	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
10	Services (Optional)	Starting and Stopping of Services (if applicable)	Service Identity
			Activity performed (start, stop, etc.)
			Timestamp
			Outcome of event (Success or failure)
11	X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
			Reason for failure
			Subject identity

			Type of event
12	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
13	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
14	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
15	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)
16	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
17	User Login and Logoff (Mandatory)	All use of Identification and	User identity
			Origin of attempt (IP address)

		authentication mechanisms.	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) CHF shall support (near real time) 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 CHF.
c) CHF 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. 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 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:

CHF 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 CHF and the method of secure communication, 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 CHF (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 CHF (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 [20]: 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 CHF shall be in compliance with the respective latest 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 CHF is in compliance with the respective latest FIPS standards (for the specific crypto algorithm embedded inside the CHF)."

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

a) When CHF 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 CHF 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 CHF 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, CHF 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 CHF to create a copy of data for illegal transmission.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**

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

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) CHF shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound covert channels and tunnels such as Domain Name System (DNS) Tunnel, HTTPS Tunnel, Internet Control Message Protocol (ICMP) Tunnel, Transport Layer Security (TLS), Secure Sockets Layer (SSL), Secured Shell (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 CHF.
c) Session logs shall be generated for establishment of any session initiated by either user or CHF system.

2.6.9 System Robustness against Unexpected Input

Requirement:

During transmission of data to a system, it is necessary to validate input to the CHF, before processing. This includes all data which is sent to the system. Examples of these are user input, inputs from CHF's NF consumers viz. PCF, SMF, NEF, SMSF, IMS node, DDNMF and

EES, 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:

CHF shall support mechanisms for taking backup of sensitive data, configuration, and log files and their restoration. An effective backup and restoration strategy shall be in place and documented.

Ref [16]: "Security Guidance for 5G Cloud Infrastructure", Data Protection by NSA & CISA, Part III]

2.6.11 Secure deletion of sensitive data

Requirement:

CHF shall support secure deletion of sensitive data by authorized users in such a manner that it cannot be recovered through any forensic means.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level Requirement

Requirement:

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

In particular the CHF 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) CHF 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 CHF 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 [11]: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection – Anti-Spoofing

Requirement:

CHF 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 2.8: Attack Prevention Mechanisms

2.8.1 Overload Situations

Requirement:

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

CHF 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 may 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 CHF shall act in a predictable way if an overload situation cannot be prevented. CHF 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 CHF 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 CHF'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:

CHF 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 CHF. 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.

2.8.4 GTP-C Filtering (when 5GC is interworking with EPC)

Requirement:

The following capability is conditionally required:

a) For each message of a GTP-C-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.

At least the following actions should be supported when the check is satisfied:

- Discard: the matching message is discarded.
- Accept: the matching message is accepted.
- 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.

b) This requirement is conditional in the following sense: It is required that at least one of the following two statements holds:

- CHF supports the capability described above, and this is stated in the product documentation.

- The CHF's documentation states that the capability is not supported and that the CHF needs to be deployed together with a separate entity that provides the capability described above.

[Ref [3]: TSDSI STD T1.3GPP 33.117--17.1.0 V.1.1.0-Section 4.2.6.2.3]

Section 2.9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of CHF 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 CHF, 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 by TSTL at the time of testing 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 [9]: https://nvd.nist.gov/vuln-metrics/cvss
Ref [19]: Reference Architecture]

Section 2.10: 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 CHF 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 CHF.

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.

CHF 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 CHF 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:

CHF 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 CHF 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 CHF 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 CHF 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 CHF, 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 CHF 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 CHF 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, CHF 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 and privileged users.

2.10.13 Restrictions on Soft-Restart

Requirement:

The CHF 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 2.11: Web Servers

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

2.11.1 HTTPS

Requirement:

The communication between CHF Web client and the CHF 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 CHF.
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 CHF 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 CHF 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 CHF 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 CHF 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 CHF 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 CHF 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 CHF 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 CHF 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 CHF 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 CHF 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 CHF 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 CHF's web server's document directory.
In particular, the CHF 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 CHF 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 CHF 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 CHF 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) CHF shall not accept session identifiers from GET/POST variables.
12) CHF 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 2.12: 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 CHF 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 CHF'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 Information element (IE) e.g. QoS setup parameters, user identifiers, 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.

[1. Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section-4.3.6.4
2. Ref[60]: 3GPP TS 29.501 V17.1.0, 5G system; Principles and Guidelines for Services Definition; Stage 3 , Section 6.2]

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 Network Slice Instance (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 base 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 [15]: 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 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 CHF. The CHF shall never use the eval function to evaluate JSON data to prevent client-side JSON injections. CHF shall sanitize all data before serializing it to JSON, to prevent server-side JSON injections.

[Ref [21]: ENISA THREAT LANDSCAPE FOR 5G NETWORKS, December 2020]

Section 2.13: Other Security Requirements

2.13.1 Remote Diagnostic Procedure – Verification

Requirement:

If the CHF 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:

- User id
- Time stamp
- Interface type
- Event Type.
- Command/activity performed
- Result type (e.g., SUCCESS, FAILURE).
- IP Address of remote machine

Ref[61]: GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack section 2.2.7.7

2.13.2 No System Password Recovery

Requirement:

No provision shall exist for the CHF System / Root password recovery.

2.13.3 Secure System Software Revocation

Requirement:

Once the CHF 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 CHF shall support a well-established control mechanism for rolling back to previous software image.

2.13.4 Software Integrity Check- Installation

Requirement:

CHF 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 CHF 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 CHF 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 CHF 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 [13]: RFC 7515 JSON Web Signature (JWS)
Ref [14]: 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 CHF, it shall be possible to isolate CHF at network and/or compute/storage level. Such provisions shall be documented.

[Ref [18]: ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section-4.1.3]

Chapter 3 - Specific Security Requirements

3.1 Secure Communication over the GTP Prime (GTP') based Interface, Ga

Requirement:

For secure communication between the CHF and the Charging Gateway Function (CGF) over the Ga interface, the following shall apply:

1) The GTP' interface shall be confidentiality, integrity, and replay protected.
2) For the protection of the GTP' interface, Network Domain Security/Internet Protocol (NDS/IP) shall be used as specified in 3GPP TS 33.210.

[Ref [2]: TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0, Security architecture and procedures for 5G system: Section 9.9.
Ref [48]: TSDSI STD T1.3GPP TS 33.210, V17.1.0 Network Domain Security; IP layer security: Section 5.1, Section 5.3.1 and Section 5.4.
Ref [56]: RFC-4303: "IP Encapsulating Security Payload (ESP)", S. Kent, BBN Technologies, December 2005.
Ref [57]: IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"].

3.2 Secure Communication over the Diameter based interfaces, Rc and Re.

Requirement:

Following security measures shall be adopted for all communications and data transfers over the Diameter Interfaces, viz. Rc interface between the CHF and Account Balance Management Function (ABMF) and Re interface between the CHF and Rating Function (RF): -

1. The Diameter interface shall be confidentiality, integrity, and replay protected.
2. Traffic Protection TLS/DTLS 1.2 and above over TCP/SCTP or NDS/IP shall be supported for the diameter interfaces between the CHF and the connected entities, as applicable using the secure cryptographic controls prescribed in Table 1 of the latest document of "ITSAR for Cryptographic Controls".
3. The protection of the Diameter interface shall be supported for NDS/IP as specified in TS 33.210.
4. If (D)TLS is used, implementation and usage shall follow the profiles given in TS 33.210 and TS 33.310.

[Ref [2]: TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0- Security architecture and procedures for 5G system: Section 9.9.

Ref [12]: IETF RFC 6733 Diameter based Protocol: Section 13.
Ref [48]: TSDSI STD T1.3GPP TS 33.210, V17.1.0: Network Domain Security; IP layer security: Section 5.3.1(IPsec), Section 6.2 ((D)TLS).
Ref [49]: TSDSI STD T1. 3GPP 33.310 -17.3.0 V1.1.0 Network Domain Security; Authentication Framework: Section 6.2.1b (IKEv2/IPsec), Section 6.1.3a((D(TLS)).
Ref [56]: RFC-4303: "IP Encapsulating Security Payload (ESP)", S. Kent, BBN Technologies, December 2005.
Ref [57]: IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"]

Section 3.3: Charging Data Records related Specific Security Requirements

3.3.1 Charging Data Record File Integrity

Requirement:

Systems and mechanisms shall be in place to ensure CHF database integrity. Documentation on specific methods or approaches used to address the CHF database integrity shall be provided.

[Ref [46]: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/]

3.3.2 Charging Data Records Availability

Requirement:
Systems and mechanisms shall be in place to ensure the availability of the Charging Data Record files generated by CHF. Documentation on the specific methods or approaches used to address the availability of the Charging Data Records shall be provided.

[Ref [50]: https://docs.oracle.com/cd/B14117_01/server.101/b10726/hadesign.htm#i1006336.]

3.3.3 Secured backups of Charging Data Records

Requirement:

The mechanisms (such as high availability clusters) for CDR backups and restoration shall be supported.

[Ref [50]: https://docs.oracle.com/cd/B14117_01/server.101/b10726/hadesign.htm#i1006336.]

3.3.4 CDR file Protection

Requirement:

For protection against file manipulations secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" shall be used.

[[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0 "Catalogue of General Security Assurance Requirements": Section-4.2.3.2.3]

Annexure-I

Definitions

1. **2G- / 3G-:** prefixes 2G- and 3G- refer to functionality that supports only GSM or UMTS, respectively, e.g. 2G-SGSN refers only to the GSM functionality of an SGSN.
2. **5G Access Network**: An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network [1].
3. **5G Core Network**: The core network specified in the present document. It connects to a 5G Access Network.
4. **5G System**: 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE [1].
5. **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.
6. **Accounting:** process of apportioning charges between the Home Environment, Serving Network and Subscriber.
7. **Accounting Meter Record:** record containing one or more counters employed to register the usage of resources en masse. Includes simple event counters and/ or cumulative call second counters.
8. **Advice of Charge (AoC):** Real-time display of the network utilization charges incurred by the Mobile Station The charges are displayed in the form of charging units. If a unit price is stored by the MS, then the display may also include the equivalent charge in the home currency.
9. **Additional actor**: This is a retailer or a wholesaler of mobile services but does not own licensed radio spectrum, an additional actor that is a retailer is often referred to as Mobile Virtual Network Operator (MVNO).
10. **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.
11. **AoC service:** Combination of one or more services, both basic and supplementary, together with a number of other charging relevant parameters to define a customized service for the purpose of advice of charge.
12. **Application Identifier**: An Identifier that can be mapped to a specific application traffic detection rule.
13. **Application Based Charging (ABC):** Ability to perform charging on an application basis for network usage based upon application detection. billing: function whereby CDRs generated by the charging function(s) are transformed into bills requiring

payment.

14. **AUSF**: AUSF is a network function with which SEAF and UDM interact during the authentication of UE [1].
15. **Billing Domain:** part of the operator network, which is outside the core network, which receives and processes CDR files from the core network charging functions. It includes functions that can provide billing mediation and billing or other (e.g. statistical) end applications.
16. **Billing and Charging Evolution:** The process is driven by new formats like Usage Data Report, Billing Statement Report and Detailed Data Record which together build a robust framework for seamless revenue assurance. The process is a simplified and flexible optional settlement method, tailor made for future wholesale roaming settlement needs of operators
17. **Call:** a logical association between several users (this could be connection oriented or connection less).
18. **Camped on a cell:** The UE is in idle mode and has completed the cell selection/reselection process and has chosen a cell. The UE monitors system information and (in most cases) paging information. Note that the services may be limited, and that the PLMN may not be aware of the existence of the UE within the chosen cell.
19. **Capability Class:** A piece of information which indicates general 3GPP System mobile station characteristics (e.g., supported radio interfaces) for the interest of the network.
20. **Carrier:** The modulated waveform conveying the E-UTRA, UTRA or GSM/EDGE physical channels
21. **Carrier frequency:** Centre frequency of the cell.
22. **Card session:** A link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card.
23. **CAC (Connection Admission Control):** A set of measures taken by the network to balance between the QoS requirements of new connections request and the current network utilisation without affecting the grade of service of existing/already established connections.
24. **CAMEL**: network feature that provides the mechanisms to support operator specific services even when roaming outside HPLMN.
25. **CAMEL Subscription Information**: identifies a subscriber as having CAMEL services.
26. **Channel edge:** The lowest and highest frequency of the carrier, separated by the channel bandwidth.
27. **Channel bandwidth:** The RF bandwidth supporting a single RF carrier with the transmission bandwidth configured in the uplink or downlink of a cell. The channel

bandwidth is measured in MHz and is used as a reference for transmitter and receiver RF requirements.

28. **Charged Party:** A user involved in a chargeable event who has to pay parts or the whole charges of the chargeable event, or a third party paying the charges caused by one or all users involved in the chargeable event, or a network operator.
29. **Charging**: function within the telecommunications network and the associated OCS/BD components whereby information related to a chargeable event is collected, formatted, transferred and evaluated in order to make it possible to determine usage for which the charged party may be billed (offline charging) or the subscriber's account balance may be debited (online charging).
30. **Charging Data Record (CDR):** A formatted collection of information about a chargeable event (e.g. time of call set-up, duration of the call, amount of data transferred, etc) for use in billing and accounting. For each party to be charged for parts of or all charges of a chargeable event a separate CDR shall be generated, i.e more than one CDR may be generated for a single chargeable event, e.g. because of its long duration, or because more than one charged party is to be charged.
31. **Chargeable Event:** An activity utilising telecommunications network infrastructure and related services for user-to-user communication (e.g., a single call, a data communication session or a short message), or for user to network communication (e.g., service profile administration), or for inter-network communication (e.g., transferring calls, signalling, or short messages), or for mobility (e.g., roaming or inter-system handover), which the network operator wants to charge for. The cost of a chargeable event may cover the cost of sending, transporting, delivery and storage. The cost of call related signalling may also be included.
32. **Charging Event**: set of charging information forwarded by the CTF towards the CDF (offline charging) or towards the OCS (online charging). Each charging event matches exactly one chargeable event.
33. **Charged party:** user involved in a chargeable event that has to pay parts or the whole charges of the chargeable event, or a third party paying the charges caused by one or all users involved in the chargeable event, or a network operator.
34. **CHF Group ID**: This refers to one or more CHF instances managing a specific set of SUPIs.
35. **Charging Session**: The association between the CHF (NF Service Producer) that provides the charging service and NF service consumer.
36. **Cipher key:** A code used in conjunction with a security algorithm to encode and decode user and/or signalling data.
37. **Circuit Switched Domain**: domain within GSM / UMTS in which information is transferred in circuit switched mode.

38. **Closed group:** A group with a predefined set of members. Only defined members may participate in a closed group.
39. **Closed Subscriber Group (CSG):** A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells).
40. **Coverage area:** Area over which a 3GPP System service is provided with the service probability above a certain threshold.
41. **Coverage area (of a mobile cellular system):** An area where mobile cellular services are provided by that mobile cellular system to the level required of that system.
42. **Credit-Control**: mechanism which directly interacts in real-time with an account and controls or monitors the charges, related to the service usage. Credit-Control is a process of: checking if credit is available, credit reservation, deduction of credit from the end user account when service is completed and refunding of reserved credit not used.
43. **CSG cell**: A cell, part of the PLMN, broadcasting a specific CSG Identity. A CSG cell is accessible by the members of the closed subscriber's group for that CSG Identity. All the CSG cells sharing the same identity are identifiable as a single group.
44. **CSG Identity (CSGID)**: An identity broadcast by a CSG cell or cells and used by the UE to facilitate access for authorised members of the associated Closed Subscriber Group.
45. **CSG Indicator**: An indication transmitted on the broadcast channel of the CSG cell that allows the UE to identify such a CSG cell.
46. **CSG manager**: A CSG manager can, under the operator's supervision, add, remove and view the list of CSG members.
47. **Domain**: part of a communication network that provides resources using a certain bearer technology.
48. **FTAM**: File Transfer Access and Management is an OSI application Layer 7 protocol that standardizes how files are accessed and managed in a distributed network file system. It outlines and combines standards for file transfer and remote access to open files into a single protocol.
49. **Gateway UE:** a UE, which acts as a gateway providing access to and from the 3GPP network for one or more non-3GPP devices that are connected to the gateway UE.
50. **GPRS:** packet switched bearer and radio services for GSM and UMTS systems.
51. **Hard Handover:** Hard handover is a category of handover procedures where all the old radio links in the UE are abandoned before the new radio links are established.
52. **Heterogeneous Network:** a 3GPP access network consisting of multiple cells with different characteristics (e.g., for the case of E-UTRA: a variety of e-NodeBs, Home e-NodeBs, e-UTRA Relays).

53. **HE-VASP:** Home Environment Value Added Service Provider. This is a VASP that has an agreement with the Home Environment to provide services. The Home Environment provides services to the user in a managed way, possibly by collaborating with HE-VASPs, but this is transparent to the user. The same service could be provided by more than one HE-VASP and each HE-VASP can provide more than one service.
54. **HNB Name**: The HNB Name is a broadcast string in free text format that provides a human readable name for the Home NodeB/eNodeB.
55. **Home Environment:** responsible for overall provision and control of the Personal Service Environment of its subscribers.
56. **Home Mobile Network Operator** (home MNO): This is an operator of PLMN where the MCC and MNC of the PLMN identity is same as the MCC and MNC of the UE's SUPI, also referred to as HPLMN.
57. **Home PLMN:** This is a PLMN where the MCC and MNC of the PLMN identity match the MCC and MNC of the IMSI. Matching criteria are defined in TS 23.122.
58. **Integrity:** (in the context of security) The avoidance of unauthorised modification of information.
59. **Inter PLMN handover:** Handover between different PLMNs, ie having different MCC-MNC.
60. **International Mobile Station Equipment Identity (IMEI):** An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the PLMN and shall be unconditionally implemented by the MS manufacturer.
61. **International mobile user number (IMUN):** The International Mobile User Number is a dialable number allocated to a 3GPP System user.
62. **Intra PLMN handover:** Handover within the same network, i.e. having the same MCC-MNC regardless of radio access system.
63. **IP-Connectivity Access Network (IP-CAN):** The collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities**.** An example of an "**IP-Connectivity Access Network**" is **GPRS**.
64. **Local Charging Zone (LCZ):** A logical grouping of a number of cells, where a special tariff applies for a select group of users. A network may have a number of LCZs. A LCZ does not necessarily need to be aligned with an LA or RA, i.e. the border of LCZ may not be the border of an LA or RA.
65. **Multipoint:** A value of the service attribute "communication configuration", which denotes that the communication involves more than two network terminations (source: ITU-T I.113).
66. **Multimedia service:** Services that handle several types of media such as audio and video in a synchronised way from the user's point of view. A multimedia service may

involve multiple parties, multiple connections, and the addition or deletion of resources and users within a single communication.

67. **NF service**: a functionality exposed by a NF through a service-based interface and consumed by other authorized NFs.
68. **NF service operation**: An elementary unit a NF service is composed of.
69. **Personal Service Environment:** contains personalised information defining how subscribed services are provided and presented towards the user. Each subscriber of the Home Environment has her own Personal Service Environment. The Personal Service Environment is defined in terms of one or more User Profiles.
70. **Prepay service:** A prepay service allows a subscriber to pay in advance for the use of specific services, the prepay account may be updated each time the subscriber uses the services related to that account.
71. **Quota management (Roaming):** V-CHF checks if the units requested by NF is sufficient based on the available number of units that has been granted by H-CHF. If the account has sufficient funds, V-CHF performs the corresponding unit reservations.
72. **Real time:** Time, typically in a number of seconds, to perform the on-line mechanism used for fraud control and cost control.
73. **Reduced Partial CDR (RPC):** partial CDRs that only provide mandatory fields and information regarding changes in the session parameters relative to the previous partial CDR. For example, location information is not repeated in these CDRs if the subscriber did not change its location.
74. **Service based interface**: It represents how a set of services is provided/exposed by a given NF.
75. **Session:** logical connection between parties involved in a packet switched based communication This term is used for IP connections rather than the term "call" that is normally used for a connection over conventional (circuit switched) systems.
76. **Settlement:** payment of amounts resulting from the accounting process.
77. **Successful call:** connection that reaches the communication or data transfer phase e.g. the "answered" state for speech connections. All other connection attempts are regarded as unsuccessful.
78. **Tariff:** set of parameters defining the network utilization charges for the use of a particular bearer / session / service.
79. **Transit:** interconnection scenarios in multi operator environments where one or more transit operators are between the originating and terminating operator.
80. **User Equipment (UE)**: device allowing a user access to network services. For the purpose of 3GPP specifications the interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains, the domains being separated by reference points. Currently defined domains are the USIM and ME Domains. The ME Domain can further be subdivided into several

components showing the connectivity between multiple functional groups. These groups can be implemented in one or more hardware devices. An example of such connectivity is the TE – MT interface. Further, an occurrence of a User Equipment is an MS for GSM as defined in TS 24.002.

81. **Visited Mobile Network Operator** (visited MNO): This is an operator of PLMN where the MCC and MNC of the PLMN identity is different from the MCC and MNC of the UE's SUPI, also referred to as VPLMN.

Annexure-II

Acronyms

3G	-	3rd Generation
3GPP	-	3rd Generation Partnership Project
5GC	-	5G Core Network
5GS	-	5G System
AAA	-	Authentication, Authorization and Accounting
ABMF	-	Account Balance Management Function
AF	-	Application Function
AMF	-	Access and Mobility Management Function
AOC	-	Advice of Charge
API	-	Application Program Interfaces
APN	-	Access Point Name
AS	-	Application Server
BCE	-	Billing and Charging Evolution
BD	-	Billing Domain
BGCF	-	Breakout Gateway Control Function
BS	-	Bearer Services
BSC	-	Base Station Controller
BSS	-	Base Station Subsystem
BTS	-	Base Transceiver Station
CAMEL	-	Customized Applications for Mobile network Enhanced Logic
CAP	-	CAMEL Application Part
CCS	-	Converged Charging System
CDF	-	Charging Data Function
CDR	-	Charging Data Record
CG	-	Charging Gateway
CGF	-	Charging Gateway Function
CHF	-	Charging Function
CN	-	Core Network
CP	-	Control Plane
CS	-	Circuit Switched
CSCF	-	Call Session Control Function (I-Interrogating; E-Emergency; P-Proxy; and S-Serving)
DNAI	-	Data Network Access Identifier of a user plane access to one or more DN(s) where applications are deployed.
IPUPS	-	Inter PLMN User Plane Security

I-SMF	-	Intermediate SMF
I-UPF	-	Intermediate UPF
OCF	-	Online Charging Function
OCS	-	Online Charging System
OMR	-	Optimal Media Routing
PCEF	-	Policy and Charging Enforcement Function
PCF	-	Policy Control Function
PCRF	-	Policy and Charging Rules Function
PFD	-	Packet Flow Description
PDR	-	Packet Detection Rule
RF	-	Rating Function
SA	-	3GPP TSG Service and System Aspects
SCCP	-	Signaling Connection Control Part
SCEF	-	Service Capability Exposure Function
SCF	-	Service Control Function
SCS	-	Services Capability Server
SCUR	-	Session Charging with Unit Reservation
SGSN	-	Serving GPRS Support Node
SIM	-	Subscriber Identity Module
SMS	-	Short Message Service
SMF	-	Session Management Function
SSF	-	Service Switching Function
TAP	-	Transferred Account Procedure
TDF	-	Traffic Detection Function
TR	-	Technical Report
TRF	-	Transit and Roaming Function
TS	-	Technical Specification
TWAG	-	Trusted WLAN Access Gateway
UE	-	User Equipment
UMTS	-	Universal Mobile Telecommunications System
UPF	-	User Plane Function
USIM	-	Universal SIM
VAS	-	Value Added Service
VLR	-	Visitor Location Register
VMSC	-	Visited MSC
VPLMN	-	Visited PLMN
WLAN	-	Wireless LAN

Annexure-III

List of Submissions

List of Undertakings to be furnished by the OEMs for CHF Security Testing

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and backdoor Check (against test case 2.3.4)
3. No unused Software (against test case 2.3.5)
4. No Unsupported Components (against test case 2.4.2)
5. Avoidance of Unspecified Wireless Access (against test case 2.4.3)
6. Cryptographic Module Security Assurance (against test case 2.6.2)
7. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)

Annexure IV

References

1) TSDSI STD T1.3GPP 23.501-17.6.0 V1.2.0 “System architecture for the 5G System 5GS)”.
2) TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0, “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) RFC 7540 Hypertext Transfer Protocol Version 2 (HTTP/2).
11) RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
12) IETF-RFC 6733, Diameter Base Protocol, Ericsson Research Centre, Nokia Research Centre, V. Fajardo Ed, Oct 2012.
13) RFC 7515 JSON Web Signature (JWS).
14) RFC 7519 JSON Web Token (JWT).
15) RFC 6749 OAuth 2.0 [IETF] October 2012, The OAuth 2.1 Authorization Framework, 2023.
16) “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.
17) CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf.
18) ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section 4.1.3].
19) GSMA NG 133 Cloud Infrastructure Reference Architecture.
20) ENISA Recommendation “Standardization in support of the cybersecurity certification”, Dec 2019.
21) ENISA THREAT LANDSCAPE FOR 5G NETWORKS, December 2020.
22) 3GPP TS 29.513 Ver 17.0.0, (2020-09), “Policy and Charging Control signalling flows and QoS parameter mapping”.
23) TSDSI STD T1.3GPP 32.240-17.8.0 V1.3.0, Telecommunication management; Charging management; Charging architecture and principles.
24) 3GPP TS 22.115 V17.1.0 (2022-06); Release 17; Charging and Billing.

25) TSDSI STD T1.3GPP 32.290-17.6.0 V1.2.0, 5G; Telecommunication management; Charging management; 5G system; Services, operations and procedures of charging using Service Based Interface (SBI).
26) 3GPP TS 29.201 V17.0.0 (2021-12) "Representational State Transfer (REST) reference point between Application Function (AF) and Protocol Converter (PC)".
27) 3GPP TS 23.502 - 17.5.0 V1.1.0 (2021-01)," procedures for the 5G System (5GS)".
28) 3GPP TS 29.211 V6.4.0 (2007-06) "Rx Interface and Rx/Gx signalling flows".
29) 3GPP TS 23.228 V6.16.0 (2007-03), "IP Multimedia Subsystem (IMS)".
30) 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.
31) GSMA FS.19, "Diameter Interconnect Security".
32) GSMA FS.11, "SS7 Interconnect Security Monitoring and Firewall Guidelines.
33) 3GPP TS 32.296 V17.0.0 (2022-03); Online Charging System (OCS): Applications and interfaces.
34) TSDSI STD T1.3GPP 43.020-14.3.0 V1.0.0; Security Related Network Functions : GPRS
35) ETSI TS 132 295 V8.0.0 (2009-01) Telecommunication management; Charging management; Charging Data Record (CDR) transfer.
36) "5G Wireless-Comprehensive-Introduction", William Stallings, Pearson Education, 2021.
37) 3GPP TS 32.291 version 16.7.0, Release 16, 5G; Telecommunication management; Charging management; 5G system, charging service; Stage 3 (3GPP TS 32.291 version 16.7.0 Release 16).
38) N. Wehbe, H. Almandine, M. Pourzandi, E. Bou-Harb and C. Assi, "A Security Assessment of HTTP/2 Usage in 5G Service Based Architecture, IEEE Communications Magazine, Vol 61, January 2023.
39) Diameter-2018-eng.pdf (gsma.com), Diameter Vulnerabilities Exposure Report, 2018.
40) National Informatic Centre (NIC) guidelines on Cybersecurity. https://guidelines india.gov.in/guidelines/#cybersecurityGuidelines.
41) https://www.nokia.com/networks/asservice/saas/securitywp/?did=D00000005182 &gclid=EAIaIQobChMIgJPpwv_wIV1HJ9Ch062grIEAAYASAAEgIWavD_BwE, Demystifying SaaS and public cloud security with Google cloud, Amazon AWS, Microsoft Azure and Nokia, White Paper, 2022.
42) https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html]
43) 3GPP TR 21.905 V17.1.0 (2021-12) "Vocabulary for 3GPP Specifications".
44) https://www.techtarget.com/searchsecurity/answer/How-to-mitigate-the-risk-of-a-TOCTTOU-attack.
45) https://www.oracle.com/java/technologies/javase/seccodeguide.html.
46) https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/.

47) https://www.techtarget.com/searchoracle/tip/The-basics-of-Oracle-database-availability#:~.
48) TSDSI STD T1.3GPP 33.210-17.1.0 V1.1.0: Network Domain Security (NDS); IP network layer security 3GPP TS 33.210 V17.1.0.
49) TSDSI STD T1. 3GPP 33.310, Version 17.3.0, V1.1.0 "Network Domain Security (NDS), Authentication Framework (AF)".
50) https://docs.oracle.com/cd/B14117_01/server.101/b10726/hadesign.htm#i1006336
51) TSDSI STD T1.3GPP 41.061-4.0.0 V1.0.0; GPRS ciphering algorithm requirements.
52) GSM Association Non-confidential Official Document OPG.02 - Operator Platform Telco Edge Requirement Operator Platform Telco Edge Requirements Version 2.0 14 April 2022.
53) FS-20 GPRS Tunnelling Protocol security, "https://www.gsma.com › security › resources › fs-20-g".
54) https://www.manageengine.com/data-security/what-is/data-in-motion.html? Source what-is.
55) https://www.techtarget.com/searchcontentmanagement/tip/7-common-file-sharing-security -risks.
56) RFC-4303: "IP Encapsulating Security Payload (ESP)", S. Kent, BBN Technologies, December 2005.
57) IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"].
58) "https://www.cisecurity.org>uploads", CIS Controls Measures and Metrics for Version 7.
59) 3GPP TS 28.827 V1.9.0 (2023-05) Release 17, "Study on 5G charging for additional roaming scenarios and actors "
60) 3GPP TS 29.501 V17.1.0, 5G system; Principles and Guidelines for Services Definition; Stage 3.
61) GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack