सत्यमेव जयते

Indian Telecommunication Security Assurance Requirements (ITSAR)

CELL BROADCAST CENTRE(CBC)

NCCS

Securing Networks

Release Date:
Enforcement Date:

Version: 1.0.0

Security Assurance Standards Facility
National Centre For Communication Security
Department of Telecommunications, Bengaluru-560027

About NCCS

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

Document History

Sl. No	ITSAR Reference	Title	Remarks
1			

Contents

A) Outline

This document specifies the security requirements of Cell Broadcast Centre which is used by Indian TSPs to disseminate ‘one to many’ cell broadcast messages to the receivers (cell phones/mobile handsets that have been configured to receive) within a particular geographical area. These areas may comprise of one or more cells, or may comprise the entire PLMN. The Cell Broadcast service is mainly used at providing location information to customers who have been served by the particular cell site. Indian TSPs also use the Cell Broadcast services for campaigns and providing VAS. The Emergency Alert/Public Warning is one of the established use cases for Cell Broadcast service. In India, National Disaster Monitoring Authority is working on a project which will use Cell Broadcast as one of the channels for sending alerts in an emergency situation.

The objective of this document is to present a comprehensive, country specific security requirements for Cell Broadcast Centre. There are various international standardization bodies/associations like 3GPP, ATIS ETSI etc who have been working on the security aspects related to Cell Broadcasting. The specifications produced by these bodies along with the country specific security requirements are the basis for this document.

This document commences with a concise description of Cell Broadcasting and proceeds to address the common and entity specific security requirements of Cell Broadcast Centre.

B) Scope

This document lays down the security requirements of Cell Broadcast Centre (CBC) deployed in GSM/W-CDMA/LTE/LTE-A networks. This document does not cover the security requirements of interfaces between CBC and the respective RAN nodes of 2G/3G/4G mobile network elements. The requirements specified here are binding on both operators (aka Telecommunication Service Provider- TSP) and Cell Broadcast equipment providers (aka OEMs-Original Equipment Manufacturer).

The regulations regarding Remote Access and Lawful Interceptions are not part of this ITSAR. Similarly, the security features of Public Warning System are not considered here.

C) References

1. 3GPP TS 23 041, Version 11.0.0 Technical realization of Cell Broadcast Service (CBS)
2. 3GPP TS 22.268 Version 11.5.0 Public Warning System Requirements
3. TEC ER No.: TEC/ER/MT/CBC-001/01/APRIL 2018 Cell Broadcast Centre
4. TEC GR 22140:2015 Generic Requirement for Short Message Service Cell Broadcast (SMSCB)
5. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0: "Catalogue of General Security Assurance Requirements".
6. 3GPP TS 44.012 - Short Message Service Cell Broadcast (SMSCB)
7. GSMA- A report on Mobile Networks Public Warning Systems and the rise of Cell Broadcast

D) Definitions and Acronyms

D.1 Definitions

1. 3GPP: The 3rd Generation Partnership Project (3GPP) unites seven communications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC, TSDSI) known as Organizational Partners to develop specifications related to 3GPP technologies.
2. Administration involves keeping track of resources in the networks and how they are assigned so as to meet service quality objectives. It deals with all the “housekeeping” that is necessary to keep things under control.
3. C-interface: Reference Point C is the secure interface between the Govt Alert Gateway and the Cell Broadcast System.
4. Cell: In a wireless communication, cell is the smallest geographical area encompassing the signal range from one Base Station.
5. Cell Broadcast Entity (CBE): It is not owned by the operator and is responsible for originating cell broadcast messages. It is also responsible for all aspects of formatting cell broadcast messages, including the splitting of a cell broadcast message into a number of pages. Cell broadcast messages may originate from a

number of Cell Broadcast Entities (CBEs), which are connected to the Cell Broadcast Centre.

6. Cell Broadcast Centre: It is the heart of the Cell broadcasting system and is located in operator's domain. It may be implemented in redundant configuration. Cell Broadcast Centre provides facility for accepting and storing messages from Cell Broadcast Entities and forwarding these messages to their destination BSCs/RNCs/MMEs of GSM/WCDMA/LTE network at the appropriate time.
7. Cell Broadcast Messages: A Cell Broadcast message consists of a 88 octets of information. The first 6 Octets are used to identify and define the message characteristics, the next 82 are used to carry the message payload itself. This allows for a total number of 93 Characters (GSM 7-bit alphabet) to be used in a single message page, a total message may consist of 15 concatenated pages. Thus, a Cell broadcast message may have the maximum length of 15X93=1395 characters.
8. Common Alerting Protocol (CAP): CAP is an open, non-proprietary digital message format for distributing all types of alerts and notifications to organizations responsible for the dissemination of the emergency notification (e.g. TV/Radio Broadcast companies, network operators) to individuals.

   CAP messages can be sent in several language and can be targeted to specific geographical areas. CAP contains information such as the nature of the alert (e.g. fire), the severity (e.g. extreme), affected area, broadcast repetition rate and advice/instructions, etc. CAP data is described in terms of XML facilitating its exchange across different formats. CAP format is standardized by OASIS i.e Organization for the Advancement of Structured Information Standard. CAP was also recommended by the International Telecommunication Union (ITU) vide X.1303.
9. Commercial Mobile Alert System (aka, Wireless Emergency Alert): Public Warning System that delivers Warning Notifications provided by Warning Notification Providers to CMAS capable PWS-UEs. CMAS defines the following classes of Warning Notifications: Presidential, Imminent Threat, Public Safety, Child Abduction Emergency, and State/Local WEA Test.
10. Earthquake and Tsunami Warning System: Public Warning System that delivers Warning Notifications specific to Earthquake and Tsunami provided by Warning Notification Providers to the UEs which have the capability of receiving Primary and Secondary Warning Notifications within Notification Areas through the 3GPP network
11. Firmware refers to the programs and data components of an ICT product that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) and cannot be dynamically written or modified during execution. It is said to be hard-wired and a hybrid between hardware and software.
12. Hardware refers to the physical objects, components, circuits and sub-assemblies that are physically and electronically coupled to process programs and data.
13. Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from CBC's local hardware interface.

14. Machine Accounts: These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.
15. Maintenance refers to activities, such as tests, measurements, replacements, adjustments, and repairs, upgrades/updates necessary to restore or maintain a network resource in a specified state so that the resource can perform its required functions. It also involves corrective and preventive proactive measures.
16. MS/UE: These entities receive and display Cell Broadcast messages based on filtering criteria defined by the user with respect to desired categories.
17. NMS: A Network Management System is a network management layer (ITU-T M.3010) operations system.
18. Network Management: It refers to activities, methods, procedures and tools that pertains to operation, administration, maintenance and provision of networked systems (OAMP).
19. Network Operations Centre (NOC): NOC handles the operation and maintenance at network levels. The functions of network operations like fault management/service restoration, configuration management, performance management/traffic management, security management, accounting management, report management and inventory management are administered at NOC. A network will generally have only one NOC. NOC is focused on network management functions such as network monitoring traffic management and signaling management. NOC is also responsible for gathering statistics and generating reports for management, system support, and users.
20. Octet is a 8 bit of data.
21. Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot the problems as soon as possible, ideally before service is affected. In short, it refers to the processes and procedures used to manage and control telecommunications network devices and telecommunications management Network (TMN)-related devices.
22. Operations Support System (OSS) is a server that hosts the implementation of the OSS Application layer in the form of one or more specific OSS applications; the applications might be implemented by Enterprise Java Beans, CORBA objects or Web Services. While eMS and NMS are responsible for managing the network and network resources, OSS supports the operation of network and service management systems.
23. Public Warning System (PWS) is a service offered by authorities to alert the public of an impending emergency situations that are caused by earthquake, tsunami, cyclone, flood, act of terrorism etc. These alerts will help public to prepare better and act in a timely manner to minimize the impact of such disasters. Some countries use this to notify people of a Child Abduction Emergency (e.g., AMBER alert), prison escape etc. The different warning system supported by 3GPP are: ETWS (Rel 8), CMAS (Rel 9), KPAS (Rel 10), EU-ALERT (Rel 11).
24. Provisioning is concerned with configuring resources in the network to support a given service to users. The act of specifying parameters necessary when assigning/de-assigning network resources to/from the control plane or to

invoke/remove services provided by a control plane instance. These parameters are specific to a resource or service request, causing changes to these parameters to only impact a specific resource or service request. Therefore, provisioning is allowed in the initialization and operations phases of control plane lifecycle.

25. Remote Access: The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.
26. Sensitive Data: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
27. Software refers to the programs and data components which are usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution. Two general categories of software are system software and application software.
28. 10/100/1000 Base-T: Ethernet connection method which operates at 10, 100,1000 Mbps and uses twister pair cables. Base here denotes that base band transmission is used.

D.2 Acronyms

3GPP: Third Generation Partnership Project

ATIS: Alliance for Telecommunications Industry solutions

BSC: Base Station Controller

BTS: Base Transceiver Station/System

CAP: Common Alerting Protocol

CBC: Cell Broadcast Centre

CBE: Cell Broadcast Entity

CBS: Cell Broadcast Service

CMAS: Commercial Mobile Alert System

CMSP: Commercial Mobile Service Provider

CVSS: Common Vulnerability Scoring System

CWE: Common Weakness Enumeration

CVE: Common Vulnerabilities and Exposures

EAS: Emergency Alert System

ENTEL: Emergency Communications

ETSI: European Telecommunications Standards Institute

ETWS: Earthquake and Tsunami Warning System

EU-Alert: European Union-Alert

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

ITU-T: International Telecommunication Union-Telecommunication Standardization

KPAS: Korean Public Alert System

LCT: Local Craft Terminal

MME: Mobility Management Entity

MS: Mobile Station

OASIS: Organization for the Advancement of Structured Information Standards

PLMN: Public Land Mobile Network

PPDR: Public Protection and Disaster Relief

PSAP: Public Safety Answering Point

PWS: Public Warning System

RNC: Radio Network Controller

TDM: Time Division Multiplexing

TEC: Telecommunication Engineering Centre

UE: User Equipment

VAS: Value Added Service

WEA: Wireless Emergency Alert

E) Conventions

1. Must or shall or required denotes absolute requirement of particular clause of ITSAR.
2. Must not or shall not denotes absolute prohibition of 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 – Introduction

I. Overview: Cell Broadcast is a point to multipoint message distribution service over a wide geographically spread area. These areas may comprise of one or more cells, or may comprise the entire PLMN in a GSM/W-CDMA/LTE/LTE-A networks. The Cell Broadcast messages will be displayed on the mobile handset if the handset is tuned to receive the channel in which the message is being broadcast.

Cell Broadcast message may originate from a number of Cell Broadcast Entities connected to CBC. CBS messages are broadcast cyclically by the cell at a frequency and for a duration, which can be specified. The mobile stations/user equipments within the catchment area of the transmitting BTS/Node B/e-NodeB will be able to receive the broadcast messages, provided that they are switched on and in the idle state.

The CBS messages may be broadcast on two different (basic & extended) channels, which are characterised by different Quality of Service (QoS).

To permit mobiles to selectively display only those messages required by the MS/ UE user, CBS messages are assigned a message class, which categorises the type of information that they contain and the language (Data coding Scheme). The subscriber may be able to select which message classes he/she wishes to have displayed on his/her receiver. A network may be able to remotely activate mobile terminals in order to enable them to receive CBS messages, according to regulatory requirements. The service is asymmetric, as messages originate from Cell Broadcast Entity (CBE) and are received by mobile subscribers but mobile subscribers cannot originate messages. The service facilitates scheduling and repeated transmissions of messages with each message having associated with it a repetition rate and a required number of broadcasts

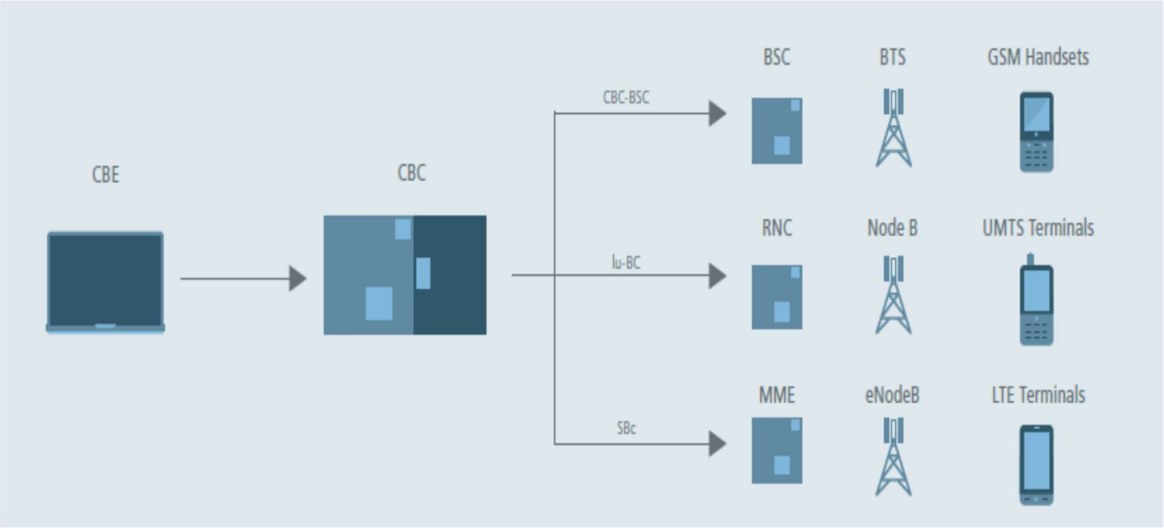
The features of Cell Broadcast are

1) Cell Broadcast messages are location based and will be receivable by even in-roamers.
2) Cell broadcast messages are unidirectional and unacknowledged broadcast where messages are transmitted from network to mobile terminals.
3) Cell Broadcast service does not violate privacy of citizens.
4) Cell Broadcast messages are fast and allows text or binary messages.

Cell Broadcast services are mainly for disseminating alert in case of disasters. In case of M2M messaging, M2M server can send the trigger to M2M device through cell broadcast in an efficient manner that can reduce traffic, and provide for less battery drain. Some operators are using Cell Broadcasting for providing Value Added Services.

II Cell Broadcast System Architecture:

It mainly consists of Cell Broadcast Centre(s), Cell Broadcast entities and RAN of 2G/3G/4G mobile networks. A typical architecture is shown below in Fig 1



a) Cell Broadcast Centre

CBC is the heart of the Cell Boradcast Service architecture. The CBC may be connected to several BSCs/RNCs/MMEs. The CBC may be connected to several CBEs. The CBC shall be responsible for the management of CBS messages including:

- allocation of serial numbers;

- modifying or deleting CBS messages held by the BSC/RNC/eNodeB;

- initiating broadcast by sending fixed length CBS messages to a BSC/RNC/e Node B for each language provided by the cell, and where necessary padding the pages to a length of 82 octets;

- determining the set of cells to which a CBS message should be broadcast, and indicating within the Serial Number the geographical scope of each CBS message;

- determining the time at which a CBS message should commence being broadcast;

- determining the time at which a CBS message should cease being broadcast and subsequently instructing each BSC/RNC/e-Node B node to cease broadcast of the CBS message;

- determining the period at which broadcast of the CBS message should be repeated;

- determining the cell broadcast channel in GSM, on which the CBS message should be broadcast.

- when CBS transmits emergency messages, allocation of "emergency indication" to differentiate it from normal CBS messages, including the "Cell ID/Service Area ID list", "warning type", "warning message". If "warning type" is of 'test', only UEs which are specially designed for testing purposes may display warning message.

The structure of CBC may be divided in the following components:

i. CBC Hardware
ii. Operating System
iii. Relational Database Management
iv. CBC software platform
v. Interfaces

b) Cell Broadcast Entity: Cell broadcast messages originate from a number of Cell Broadcast Entities (CBEs). There can be many CBEs in a CB system.

The CBE functionality shall be as follows:

i. Submit CBM requests: It shall be possible to enter a message and its associated broadcast information (broadcast times, rates etc.) and commit this information to the database.

ii. Query CBM requests: It shall be possible to query any pending or live message requests generated by the CBE. It shall be possible to view the broadcast status of the request, the scheduling information or the success or failure of the broadcast.

iii. Cancel CBM requests: It shall be possible to cancel any pending or live message requests generated by the CBE.

iv. Modify CBM requests: It shall be possible to modify any information pertaining to an existing message request.

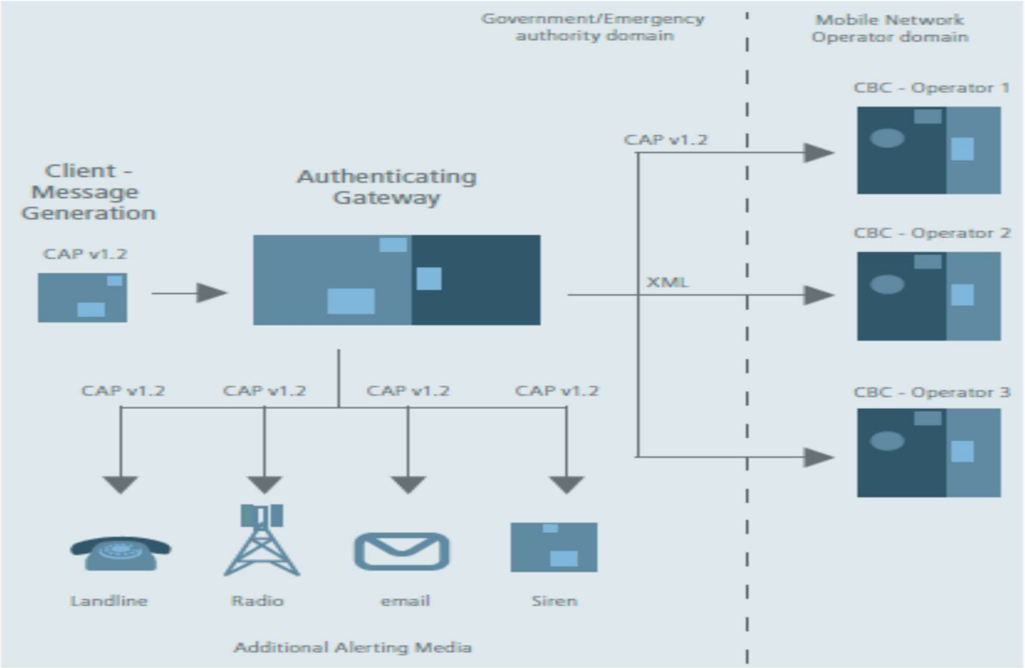
c) Operation, Administration and Management System: Typically CBCs are located at operator premises and are managed by operator.

d) Geographical Information System (GIS): The Geographical Information System gives the geographical nature of the Cell Broadcast System. The GIS provides a powerful means of interpreting and representing data relating to network coverage areas.

III Public Warning System(PWS) : Emergency alert is one of the proven and established use cases of Cell Broadcasting . Cell Broadcasting is an ideal solution for emergency alert due to

1) Over the radio channels, CB messages are carried with the highest priority (3G/4G) or is carried on a dedicated CBCH channel(2G)
2) Alerts can be transmitted in near real time to millions of users.
3) Alerts can be supported in multiple languages
4) It does not require user interaction.
5) Alerts can be sent in unique and dedicated ringtone and specific vibration on a mobile phone.
6) No knowledge of mobile numbers required.
7) CB messages can be received even without SIM card.
8) Cell Broadcast messages can be sent only by an authorized and verified sources.
9) The load on the network is low as the messages are sent once from CBC to cells where it is broadcast repeatedly.

A sample Public Warning System architecture is shown below in Fig 2.



IV Security of Cell Broadcasting Services: The Cell Broadcast messages disseminated to users shall be reliable and from the authorized source only, especially when such messages are of alert nature. As Cell Broadcast Service does not provide any capability for the MS/UE to authenticate that the Alert messages received are from a genuine source, it is possible that malicious Alert messages can be transmitted by a spoofed Base station. Therefore, enough security measures shall be provided in the network to ensure that the source of the message is genuine.

The subsequent chapters address the security requirements of Cell Broadcast Centre (hereinafter referred as CBC).

Chapter 2 – Common Security Requirements

Section 1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:
The protocols used for the CBC management and maintenance shall support mutual authentication mechanisms only.
Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for CBC management and maintenance.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:
CBC management traffic shall be protected strictly using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.4]

2.1.3 Role-Based access control

Requirement:
CBC shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which 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 and what type of operation they can perform i.e. the specific operation command or command group.
CBC supports Role Based Access Control (RBAC) with minimum of 3 user roles, in particular, for OAM privilege management for CBC Management and Maintenance, including authorization of the operation for configuration data and software.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.2]

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
- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed 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 machine accounts where atleast one authentication attribute shall be supported.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

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

[Reference TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. 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/her 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & removal of group accounts

Requirement:

Users shall be identified unambiguously by the CBC.
CBC shall support assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.
CBC shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Sections 4.2.3.4.1.2]

Section 2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:
The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g. password, certificate, token) shall be prevented. For machine-to-machine accounts one authentication attribute will be sufficient. System functions comprise, for example network services (like SSH, 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:
CBC shall support external authentication mechanism such as AAA server (for authentication, authorisation and accounting services) ,then the communication between CBC and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table1 of the latest document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.""

2.2.3 Protection against brute force and dictionary attacks

Requirement:
A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in CBC.
Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.
Various measures or a combination of the following measures can be taken to prevent this:
(a) Using the timer delay (this delay could be the same or increased depending 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 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 CBC. An exception to this requirement is machine accounts.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:
(a) The configuration setting shall be such that a CBC 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 CBC). It shall not be possible setting this absolute minimum length to a lower value by configuration.
(ii) Password shall mandatorily comprise all the following four categories of characters:
- 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. @;!$.)

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 CBC.
e) When a user is changing a password or entering a new password, CBC /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).
Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.1]

2.2.5 Inactive Session Timeout

Requirement:
An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.
CBC shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement, normally set between 2 to 5 minutes.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:
If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his/her password at any time. When an external centralized system for user authentication is used it is possible to implement this function on this system.
Password change shall be enforced after initial login.
CBC shall enforce password change based on password management policy.
In particular, the system shall enforce password expiry. CBC shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed upto a certain number (Password History).
The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its minimum value shall be 3. This means that the CBC shall store at least the three previously set passwords. The maximum number of passwords that the CBC 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.

CBC to have in-built mechanism to support this requirement.

If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.

And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the CBC.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.2]

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 "*".

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:
Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.3]

Section 3: Software Security

2.3.1 Secure Update

Requirement:
For software updates, CBC shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

To this end, the CBC has a list of public keys or certificates of authorised software sources and uses the keys to verify that the software update is originated from only these sources.

2.3.2 Secure Upgrade Requirement:

Requirement:

(a) CBC Software package integrity shall be validated in the installation /upgrade stage.

(b) CBC shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only. To this end, the CBC shall have a list of public keys or certificates of authorised software sources and uses the keys to verify that the software update is originated from only these sources.

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

(d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in (b) above

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:
a) OEM shall follow the best security practices including secure coding for software development. Source code shall be made available either at 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 CBC Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the CBC.

(ii) CBC software shall be free from CWE top 25 and OWASP top10 security weaknesses on the date of offer of product to the designated TTSL for testing. For other security weaknesses, OEM shall give mitigation plan.

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

2.3.4 Known Malware and backdoor Check

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

2.3.5 No unused software

Requirement:
Software components or parts of software ~~packages~~ which are not needed for operation or functionality of the CBC shall not be present.
Orphaned software components /packages shall not be present in CBC.
OEM shall provide the list of software that are necessary for CBC's operation.
In addition, OEM shall furnish an undertaking as
"CBC does not contain Software that is not used in the functionality of CBC"

[Reference: TSDSI STD T1.3GPP 33.117 -14.2.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:
CBC shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. CBC shall not support following services

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH

- HTTP
- SNMPv1 and v2
- SSHv1
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD
- 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 CBC and their purpose needs to be provided by the OEM as prerequisite for the test case. OEM shall submit "Communication Matrix" clearly showing the services and ports used.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:
CBC shall boot only from memory devices intended for this purpose.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:
CBC shall provide reliable time and date information provided through NTP/PTP server.
CBC shall establish secure communication channel with the NTP/PTP server.
CBC shall establish secure communication channel strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) "with NTP/PTP server.
CBC shall generate audit logs for all changes to time settings.

2.3.9 Restricted reachability of services

Requirement:
The CBC shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers.
Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the

management plane for separation of management traffic from user traffic.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.2]

2.3.10 Self Testing

Requirement:
CBC shall perform self-tests (integrity of the firmware and software as well as correct operation of cryptographic Module as per security requirement area of "self-test" of FIPS-140-2 or Later version etc.,) to identify failures in its security mechanisms during i) power on ii) when the Administrator Instructs III) Periodic, with period configurable and iv) at the time of restart.

Section 4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:
Unused functions i.e the software and hardware functions which are not needed for operation or functionality of the CBC shall be deactivated in the CBC's software and/or hardware.
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 CBC.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:
OEM to ensure that the CBC shall not contain software and hardware components that are no longer supported by OEM or its 3rd Parties including the open-source communities, such as components that have reached end-of-life or end-of-support.

An undertaking in this regard shall be given by OEM.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.5]

2.4.3 Avoidance of unspecified mode of Access

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

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

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement:
The security event log shall be access controlled (file access rights) such that only privilege users including the administrator have access to read the log files. The only

allowed operations on security event log are archiving/saving and viewing.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0. section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:
The CBC shall log all important Security events with unique System Reference details as given in the Table below.
CBC shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity and the outcome (success or failure) of the event. Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

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

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

		Outcome of event (Success or failure)
		Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	Attempt to initiate manual update, initiation of update, completion of update	User identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	Old value of time
		New value of time
		Timestamp
		origin of attempt to change time (e.g.IP address)
		Subject identity
		Outcome of event (Success or failure)
		User identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session.	User identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)

authorised remote administrators (Optional)		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Audit data changes (Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure)
		Subject identity
		User identity
		origin of attempt to change time (e.g.IP address)
		Details of data deleted or modified
Port Scan attempts	Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters	Date
		Time Stamp
		Source IP address
		Destination Port address
User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
		Origin of attempt (IP address)
		Outcome of event (Success or failure)
		Timestamp

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:
(a) (i) The CBC shall support forwarding of security event logging data to an external system by push or pull mechanism.
(ii) Log functions should support secure uploading of log files to a central location or to a system external for the CBC.
(b) CBC shall be able to store the generated audit data itself may be with limitations.
(c) CBC shall alert administrator when its security log buffer reaches configured threshold limit.
(d) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), CBC shall have mechanism to store audit data locally. CBC

shall have sufficient memory (minimum 100 MB) allocated for this purpose. The OEM to submit justification document for sufficiency of local storage requirement.
(e) Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.6.2]

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:
CBC shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

OEM shall submit to TSTL, the list of the connected entities with CBC and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing the 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 CBC (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 CBC (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".

OEM shall also submit cryptographic module testing document and the detailed self / Lab test report along with test results for scrutiny

CBC shall support the minimum security level of 2 as defined in FIPS 140-2.

2.6.3. Cryptographic Algorithms implementation Security Assurance

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

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

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithm implemented inside the Crypto module of CBC is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the CBC)"

OEM shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results for scrutiny.

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:
a) When CBC 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.
b) Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.2.]

2.6.5. Protecting data and information in storage

Requirement:
a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted.
b) Sensitive files of CBC system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.

c)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 in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.
(iii)Stored files in the CBC: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:
a) Without authentication, CBC 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 CBC to create copy of data for illegal transmission.
c) The software functions, components in the CBC for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement:
a) CBC shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound overt channels such as HTTPS, IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the CBC.
Session logs shall be generated for establishment of any session initiated by either user or CBC.

---

2. 6.8 Protection against Data Exfiltration - Covert Channel

Requirement:
a) CBC 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 DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the CBC.
c) Session logs shall be generated for establishment of any session initiated by either user or CBC system.

Section 7: Network Services

2.7.1 Traffic Separation

Requirement:
CBC shall support physical or logical separation of Operation & Management traffic and control plane traffic. See RFC 3871 for further information.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.5.1].

2.7.2 Traffic Protection –Anti-Spoofing

Requirement:
CBC 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.3.1.1]

Section 8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

Requirement:
CBC shall have protection mechanism against Network level and Application-level DDoS attacks.

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

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.3.1]

2. 8.2 Excessive Overload Protection

Requirement:
CBC shall act in a predictable way if an overload situation cannot be prevented. CBC shall be built in this way that it can react on an overload situation in a controlled way.
However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that CBC cannot reach an undefined and thus potentially insecure, state. In an extreme case, CBC shall continue to work in degraded mode with less traffic handling capacity but without loss of system security functions.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.3.3]

2. 8.3 Filtering IP options

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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.4.1.1.3]

Section 9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.4]

2.9.2 Port Scanning

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:
It shall be ensured that no known critical/high/medium (as per CVE-IDs of NIST-NVD) vulnerabilities (as on date of offer of CBC to the designated TTSL for testing) shall exist in the CBC. For low/uncategorized (as per CVE-IDs of NIST-NVD) category vulnerabilities remediation plan is to be provided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

Section 10: Operating System

2.10.1 Growing Content Handling

Requirement:
a) Growing or dynamic content shall not influence system functions.
b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop CBC from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:
Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the CBC.
CBC shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	129	Echo Reply	Optional (i.e.as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	128	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	Neighbour Solicitation	Permitted	Permitted
N/A	136	Neighbour Advertisement	Permitted	N/A

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:
Each system account in CBC shall have a unique identification with appropriate non-repudiation controls.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.2.2]

2.10.5 OS Hardening

Requirement:
Appropriate OS hardening procedures including security measures required to ensure the kernel miniaturization etc. shall be implemented in CBC.

Kernel based network functions not needed for the operation of the CBC shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.2]

2.10.6 No automatic launch of removable media

Requirement:
CBC shall not automatically launch any application when removable media device is connected.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.3]

2.10.7 Protection from buffer overflows

Requirement:
CBC 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 the OEM.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in CBC 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.6]

2.10.9 File-system Authorization privileges

Requirement:
CBC 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.7]

2.10.10 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, ~~TTE~~ CBC shall have feature to restrict Scripts / Batch-processes / Macros usage among various users. It shall be possible to administratively configure scheduled tasks usage i.e Cron-Job usage (permit / deny) among various users like Normal users, privileged users.

2.10.11 Restrictions on Soft-Restart

Requirement:
CBC 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.

Section 11: Web Servers

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

2.11.1 HTTPS

Requirement:
The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) ” only.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:
Access to the CBC webserver (for both successful as well as failed attempts) shall be logged by CBC.
The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.2.1]

2.11.3 HTTPS input validation

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:
No CBC web server processes shall run with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:
HTTPS methods that are not required for CBC operation shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:
All optional add-ons and components of the web server shall be deactivated if they are not required for CBC operation.
In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.4]

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

Requirement:
If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:
Access rights for CBC web server configuration files shall only be granted to the owner of

the web server process or to a user with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]

2.11.11 No default content

Requirement:
Default content that is provided with the standard installation of the CBC web server shall be removed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9]

2.11.12 No directory listings

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:
User-defined error pages and Error messages shall not include version information and other internal information about the CBC web server and the modules/add-ons used.
Default error pages of the CBC web server shall be replaced by error pages defined by the OEM.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:
File type or script-mappings that are not required for CBC operation shall be deleted.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the CBC web server's document directory.
In particular, the CBC web server shall not be able to access files which are not meant to

be delivered.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:
If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]

Section 12: Other Security requirements

2.12.1 Remote Diagnostic Procedure – Verification

Requirement:

If the CBC 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:

1. User id
2. Time stamp
3. Interface type
4. Event level (e.g. CRITICAL, MAJOR, MINOR)
5. Command/activity performed and
6. Result type (e.g. SUCCESS, FAILURE).
7. IP Address of remote machine

2.12.2 No System/Root Password Recovery

Requirement:
No provision shall exist for CBC System / Root password recovery.

2.12.3 Secure System Software Revocation

Requirement:
Once the CBC software image is legally updated/upgraded with New Software Image, it should 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.
CBC shall support a well-established control mechanism for rolling back to previous software image.

2.12.4 Software Integrity Check –Installation

Requirement:
CBC shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

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

2.12.5 Software Integrity Check – Boot

Requirement:
The CBC 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 Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

2.12. 6 Unused Physical and Logical Interfaces Disabling

Requirement:
CBC 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.

2.12.7 No Default Profile

Requirement:
Predefined or default user accounts in CBC shall be deleted or disabled.
No pre-defined user accounts other than Admin / Root user account would be available.

2.12.8 Security Algorithm/Protocol Downgrade attack

Requirement:
It shall not be possible to downgrade security algorithms/protocols supported by CBC to those not listed in Table 1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0"

Chapter 3 Specific Security Requirements

3.1 The hardware over which CBC is running shall be free of known vulnerability at the date of offer of product for testing to the designated TTSL.

3.2 CBC system shall be highly reliable, scalable and fully available without single point of failure.

3.3 CBC shall support M2M message update to M2M devices using cell broadcast as bearer.

3.4 CBE-CBSC interface shall be fully redundant and secured with IP Sec VPN. It shall be possible for both CBE and CBC to mutually authenticate with each other through digital certificates.

3.5 When the CBE-CBC link is idle beyond the configured time period, the connection shall be terminated automatically and reinitiated when required.

3.6 The IP addresses of CBEs shall be whitelisted in CBC.

3.7 It shall be possible to prevent spam messages being transmitted.

3.8 CBC shall support an end-to-end testing to check the message delivery to the cell, without actually broadcasting

3.9 CBC architecture shall support site level and geographic level redundancy. The data replication between geo redundant sites shall by fully synchronized.

3.10 CBC shall support backup and restore procedures for full and incremental backups.

3.11 CBC shall support the auto cell discovery mechanism as aided by RAN

3.12 CBC-GIS interface shall be well defined and it should be possible to map geo-coordinates with the corresponding cells seamlessly.

3.13 The databases used in CBC shall be fully secured.

3.14 CBC shall be protected by Firewall and IDS/IPS.

3.15 CBC shall meet the functional requirements that will aid in the implementation of Public Warning System security (as and when specified and mandated).

Appendix

List of Submissions

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and backdoor Check (against test case 2.3.4)
3. Communication Matrix (against test case 2.3.6)
4. No unsupported components (against test case 2.4.2)
5. Avoidance of Unspecified Wireless Access (against test case 2.4.3)
6. Secure Log Export -Sufficiency of local storage (against test case 2.5.3 IV)
7. Cryptographic Based Secure Communication (against test case 2.6.1)
8. Cryptographic Module Security Assurance (against test case2.6.2)
9. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)
10. Hardware - Absence of known vulnerability/security weakness (against test case 3.1.2)

-End of Document-