Indian Telecom Security Assurance Requirements

Common Security Requirements

for

Private Automatic Branch Exchange (PABX)

DRAFT FOR APPROVAL

Release Date: Version: 1.0.0

Date of Enforcement:

Security Assurance Standards Facility (SASF) Division
National Centre for Communication Security (NCCS), Bengaluru
Department of Telecommunications
Ministry of Communications
Government of India

Document Name	ITSAR for Private Automatic Branch Exchange (PABX)		
Doc. No.	Version	Release date	Enforcement date
ITSAR-PABX-XXXX	1.0.0	XX-XXX-XXXX	XX-XXX-XXXX

Table of Contents

Scope

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) for **Private Automatic Branch Exchange (PABX)**.

Section 1: Access and Authorization

1.1 Management Protocols Mutual Authentication

Requirement:

The protocols used for the PABX management and maintenance shall support mutual authentication mechanisms only.

Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” shall only be used for PABX management and maintenance.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.4.1]

1.2 Management Traffic Protection

Requirement:

PABX management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.2.4]

1.3 Role-Based access control

Requirement:

PABX 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.

PABX supports Role Based Access Control (RBAC) with minimum of 3 user roles, in particular, for OAM privilege management, for PABX Management and Maintenance, including authorization of the operation for configuration data and software via the PABX console interface.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.6.2]

1.4 User Authentication – Local and 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 the all accounts from misuse.

Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from NE local hardware interface.

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.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.2.1]

1.5 Remote login restrictions for privileged users

Requirement:

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

This remote root user access restriction is also applicable to application softwares / tools such as TeamViewer, desktop sharing etc which provide remote access to the PABX.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.6]

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.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.6.1]

1.7 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the PABX.

PABX shall support assignment of individual accounts per user, where a user could be a person, or, for machine accounts, an application, or a system.

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

[Reference: 1) 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

2.1 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. 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.1.1]

2.2 Authentication Support – External

Requirement:

If the PABX supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services) then the communication between PABX 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 document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

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. 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:

(i) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
(ii) 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.
(iii) Using an AUTHENTICATION ATTRIBUTE blacklist to prevent vulnerable passwords.
(iv) 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 PABX. An exception to this requirement is machine accounts.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.3]

2.4 Enforce Strong Password

Requirement:

The configuration setting shall be such that an PABX 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 PABX). 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. @;!$.)

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.

PABX shall have in-built mechanism to support this requirement, further 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 subclause.

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

When a user is changing a password or entering a new password, PABX/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.).

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.4.3.1]

2.5 Inactive Session Timeout

Requirement:

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

PABX 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.5.2]

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 is possible to redirect or implement this function on this system.

Password change shall be enforced after initial login.

The system shall enforce password change based on password management policy.

In particular, the system shall enforce password expiry. PABX 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:

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

PABX 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 PABX.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.2]

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.4]

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, vendor 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 vendor provides instructions on how to manually change it.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.2.3]

Section 3: Software Security

3.1 Secure Update

Requirement:

PABX's system software updates shall be carried out strictly using the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

PABX shall allow updates only if code signing certificate is valid and not time expired.

Software update integrity shall be verified strictly using the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

3.2 Secure Upgrade

Requirement:

(i) PABX Software package integrity shall be validated in the installation and upgrade stages strictly using the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

(ii) PABX shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the PABX shall have a list of public keys or certificates of

authorised software sources, and uses the keys to verify that the software upgrade is originated from only these sources.

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

(iv) PABX's software upgrades shall be carried out strictly using the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

(v) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.5]

3.3 Source code security assurance

Requirement:

a) Vendor should follow best security practices including secure coding for software development. Source code shall be offered to designated TSTL for source code review. It may be supported by furnishing the Software Test Document (STD).

b) Also Vendor 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 NE software, which includes vendor developed code, third party software and open source code libraries used/embedded in the NE.

(ii) The NE software is free from all known security vulnerabilities, security weaknesses listed in the CVE and CWE databases as on the date of offer of NE to designated TSTL for testing.

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

3.4 Known Malware and backdoor Check

Requirement:

Vendor shall submit an undertaking stating that PABX is free from all known malware and backdoors as on the date of testing and shall submit Malware test document (MTD).

3.5 No unused software

Requirement:

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

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

Vendor shall provide the list of software that are necessary for its operation.

[Reference: 1) TSDSI STD T1.3GPP 33.117 -14.2.0 V.1.0.0 Section 4.3.2.3]

3.6 Unnecessary Services Removal

Requirement:

PABX 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. PABX Shall not support following services. Any other protocols, services that are vulnerable are also to be permanently disabled.

- 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

Full documentation of required protocols and services of the Network product and their purpose needs to be provided by the vendor as prerequisite for the test case.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.1]

3.7 Restricting System Boot Source

Requirement:

PABX shall boot only from memory devices intended for this purpose.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.2]

3.8 Secure Time Synchronization

Requirement:

NE shall provide reliable time and date information provided by itself or through NTP/PTP server.

NE shall establish secure communication channel with the NTP/PTP server.

NE shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” with NTP/PTP server.

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

3.9 Restricted reachability of services

Requirement:

The PABX 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.2]

3.10 Self Testing

Requirement:

PABX 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 Administrator Instructs iii) Periodic, with period configurable.

Section 4: System Secure Execution Environment

4.1 No unused functions

Requirement:

Unused functions i.e. the software and/or hardware functions which are not needed for operation or functionality of the PABX shall not be present in the PABX’s software and/or hardware.

List of the used functions of the Networks s software and hardware as given by the vendor shall match the list of used software and hardware functions that are necessary for the operation of the PABX.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.4]

4.2 No unsupported components

Requirement:

Vendor to ensure that the PABX shall not contain software and/or hardware components that are no longer supported by vendor or its third parties including the open-source communities, such as components that have reached end-of-life or end-of-support.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.5]

4.3 Avoidance of Unspecified Wireless Access

Requirement:

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

An undertaking shall be given by the vendor as follows:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.6.1]

Section 5: User Audit

5.1 Audit trail storage and protection

Requirement:

The security event log shall be access controlled using file access rights such that only privilege users including the administrator have access to read the log files. The rights to delete or modify the log files are to be restricted, a trail of delete or modify activities may be logged in separate log file.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]

5.2 Audit Event Generation

Requirement:

The PABX shall log all important security events with unique System Reference details as given in the Table below.

PABX 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 DUT	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, enable, and disable.	Administrator username,
		Administered account,
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded,
		Value reached
		(Here suitable threshold values shall be defined depending on the individual system.)
		Outcome of event (Success or failure)
		Timestamp
Configuration change (Mandatory)	Changes to configuration of the 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 that forces a reboot or shutdown	Action performed (reboot, shutdown, etc.)
		Username (for intentional actions)

	OR where the network device has crashed.	Outcome of event (Success or failure)
		Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the network device (e.g. shutdown)	Interface name and type
		Status (shutdown, 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)
User login (Mandatory)	All use of identification and authentication mechanism	user identity
		origin of attempt (e.g. IP address)
		Timestamp
		outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	attempt to initiate manual update, initiation of update, completion of update	user identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	old value of time
		new value of time

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.6.1;
2) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.5]

5.3 Secure Log Export

Requirement:

Document Name	ITSAR for Private Automatic Branch Exchange (PABX)		
Doc. No.	Version	Release date	Enforcement date
ITSAR-PABX-XXXX	1.0.0	XX-XXX-XXXX	XX-XXX-XXXX

(i) (a) The PABX shall support forward of security event logging data to an external system by push or pull mechanism.
(b) Log functions should support secure uploading of log files to a central location or to a system external for the PABX.

(ii) PABX shall be able to store generated audit data itself, may be with limitations.

(iii) PABX shall alert administrator when its security log buffer reaches configured threshold limit.

(iv) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), PABX shall have mechanism to store audit data locally. PABX shall have sufficient memory (minimum 100 MB) allocated for this purpose. vendor to submit justification document for sufficiency of local storage requirement.

(v) Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.6.2]

Section 6: Data Protection

6.1 Cryptographic Based Secure Communication with connecting entities

Requirements:

PABX shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0".

6.2 Cryptographic Module Security Assurance

An undertaking is to be submitted by the vendor mentioning that "Cryptographic module embedded inside the PABX (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."

Vendor shall submit cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny.

6.3 Cryptographic Algorithms implementation Security Assurance

An undertaking is to be submitted by the vendor mentioning that “Cryptographic algorithms embedded in the crypto module of PABX shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm).”

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

6.4 Protecting data and information – Confidential System Internal Data

Requirement:

When PABX 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 to users and administrators.

Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.2]

6.5 Protecting data and information in storage

Requirement:

For Sensitive data in storage (persistent or temporary), read access rights shall be restricted. Files of NE system that are needed for the functionality shall be protected against manipulation.

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, encrypt it by implementation-specific means, strictly using the cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0”

(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 document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0”.

(iii) Stored files: Files having sensitive data shall be protected against manipulation strictly using checksum or cryptographic methods as defined in NCCS approved Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0”.

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.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3]

Section 7: Network Services

7.1 Traffic Separation

Requirement:

PABX shall support physical and/or logical separation of Operation & Maintenance traffic and control plane traffic. See RFC 3871 [3] for further information.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.5.1].

Section 8: Attack Prevention Mechanisms

8.1 Network Level and application-level DDoS

Requirement:

PABX shall have protection mechanism against known network level and application-level DDoS attacks.

PABX 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, but not limited, to the following:

- 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 a 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.1]

8.2 Excessive Overload Protection

Requirement:

PABX shall act in a predictable way if an overload situation cannot be prevented. PABX 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 PABX cannot reach an undefined and thus potentially insecure state. In an extreme case, a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.3]

Section 9: Vulnerability Testing Requirements

9.1 Fuzzing – Network and Application Level

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.4.4]

9.2 Port Scanning

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.4.2]

9.3 Vulnerability Scanning

Requirement:

It shall be ensured that no known vulnerabilities (as on date of offer of PABX to designated TSTL for testing) shall exist in the PABX.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

Section 10: Operating System

10.1 Growing Content Handling

Requirements:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.1.1]

10.2 Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for PABX operation shall be disabled on the PABX.

PABX 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

PABX 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	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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.1.2]

10.3 Authenticated Privilege Escalation only

Requirement:

PABX 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.2.1]

10.4 System account identification

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.2.2]

10.5 OS Hardening

Requirement:

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in PABX.

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

[Reference: 1)1 TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.2]

10.6 No automatic launch of removable media

Requirement:

PABX shall not automatically launch any application when removable media device is connected.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.3]

10.7 Protection from buffer overflows

Requirement:

PABX 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 vendor.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.5]

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 NE 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: 1)1 TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.6]

10.9 File-system Authorization privileges

Requirement:

PABX 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.7]

Section 11: Web Servers

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

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 document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.5.1]

11.2 Webserver logging

Requirement:

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

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.5.2.1]

11.3 HTTPS input validation

Requirement:

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

PABX 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.5.4]

11.4 No system privileges

Requirement:

No PABX web server processes shall run with system privileges.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.2]

11.5 No unused HTTPS methods

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.3]

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 PABX operation.

In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.4]

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.5]

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.6]

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.7]

11.10 Access rights for web server configuration

Requirement:

Access rights for PABX web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.8]

11.11 No default content

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.9]

11.12 No directory listings

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.10]

11.13 Web server information in HTTPS headers

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.11]

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 PABX web server and the modules/add-ons used.

Default error pages of the PABX web server shall be replaced by error pages defined by the vendor.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.12]

11.15 Minimized file type mappings

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.13]

11.16 Restricted file access

Requirement:

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

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.14]

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.15]

Section 12: Other Security requirements

12.1. Remote Diagnostic Procedure – Verification

Requirement:

If the PABX 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).

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.6]

12.2 No Password Recovery

Requirement:

In the event of system password reset (e.g.: Through press of Hard-reset button), the entire configuration of the PABX shall be irretrievably deleted.

No provision shall exist for PABX system password recovery.

12.3 Secure System Software Revocation

Requirement:

Once the PABX 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.

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

12.4 Software Integrity Check – Installation

Requirement:

PABX shall validate the software package integrity before the installation/upgrade stage strictly using the secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

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

12.5 Software Integrity Check – Boot

Requirement:

The PABX shall verify the integrity of software component(s) at boot time by comparing the result of a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” to the expected reference value.

12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

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

Physical and logical accessible interfaces which are not under use shall be permanently disabled so that they remain inactive even in the event of a reboot.

12.7 No Default Profile

Requirement:

Predefined or default user accounts in PABX shall be deleted or disabled.

12.8 Security Algorithm Modification

Requirement:

It shall not be possible to modify security algorithms supported by PABX.

12.9 Management Interface Isolation

Requirement:

PABX shall support management software usage/critical command execution only through a dedicated management interface.

12.10 External Alert Generation

Requirement:

PABX shall support configuring the thresholds for system parameter values such as memory, hard disk space, CPU load and it shall generate an external alert when these system parameter values exceed their defined thresholds.

12.11 Secure VPN connection

Requirement:

PABX shall establish VPN connections with its peers strictly using the secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

Section 13: Specific Security Requirements

13.1 Voice and Data Traffic Protection

Requirement:

Voice and Data traffic between the PABX and the connected/connecting entities shall be protected in PABX strictly using the secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

13.2 Signalling Traffic Protection

Requirement:

Signalling traffic between the PABX and the connected/connecting entities shall be protected strictly using the secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

13.3 CDR (Call Detail Record) Protection

Requirement:

CDR (Call Detail Record) data of PABX system shall be protected against manipulation/tampering strictly using the Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” with appropriate non-repudiation controls.

Read access rights to CDR data shall be restricted and shall be allowed only for authorized users.

13.4 CLI (Calling Line Identification) Protection

Requirement:

It shall not be possible to modify the CLI in PABX. In addition, the applicant/ manufacturer/licensee shall give undertaking that there is no software available in their system for providing such function/service.

13.5 Maintenance-Out-of-Service (MOS)

Requirement:

When a line is placed under MOS while it is in operation, the PABX shall terminate both its signalling and voice channel connections with the user terminal/instrument.

ABBREVIATIONS

AAA Server	Authentication, Authorization, and Accounting Server
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDOS	Distributed Denial of Service
DoS	Denial of Service
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
MAC	Message Authentication Code
NCCS	National Centre For Communication Security
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System

PTP	Precision Time protocol
SFTP	Secure File Transfer Protocol
SHA	Secure hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network

Annexure-A

LIST OF UNDERTAKINGS TO BE FURNISHED BY THE VENDOR FOR PABX SECURITY TESTING

1. Source Code Security Assurance (against test case 3.3)
2. Known Malware and backdoor Check (against test case 3.4)
3. Avoidance of Unspecified Wireless Access (against test case 3.10)
4. Cryptographic Module Security Assurance (against test case 6.2)
5. Cryptographic Algorithms implementation Security Assurance (against test case 6.3)
6. Undertaking that no software available in the system allowing modification of CLI (against test case 13.4)