Indian Telecom Security Assurance Requirements

For

Home Subscriber Server (HSS)

Security Assurance Standards (SAS),
National Center for Communications Security, Bengaluru
Department of Telecom, Ministry of Communications
Government of India

PAGE INTENTIONALLY LEFT BLANK

Contents

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. Security Assurance Standards (SAS) division of 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.

Overview:

This document defines the security requirements of Home Subscriber Subsystem abbreviated as HSS, which is an important logical functional entity in the core part of the Evolved Packet System(4G). It is connecting to MME of S6a interface between MME and HSS. It enables transfer of subscription and authentication data for authenticating/authorizing user access between MME and HSS. Diameter protocol over SCTP/IP is used for communication.

Sh: It is an interface between PCRF and HSS. It enables sharing of user subscription data. Diameter protocol over SCTP/IP is used for communication.

HSS Features

- Maintains Database with Subscriber configuration stored ,APN, IMSI, Authentication credentials ,PDN address ,Location information ,Feature-ID (for PCRF) ,Charging Characteristics, Persistent storage in secondary database ,AKA based authentication (key generation and distribution) ,White list of roaming partners (PLMN-ID) ,Multiple Operator support .
- Management interfaces for local/remote management:

Scope

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) specific to the HSS (Home Subscriber Subsystem) , as a core network element in a LTE Network Architecture with a dedicated hardware and dedicated software which includes Operating System as well as application software.

HSS is consists of 1) HSS Client application software [DBMS (Client)] 2) HSS server application software [DBMS (Server)] and 3) Data base (Storage)

Section 1: Access and Authorization

1.1 Management Protocols Mutual Authentication

Requirement:

The protocols used for the HSS management and maintenance shall support mutual authentication mechanisms with replay attacks protection i.e there is mutual authentication of entities for management interfaces on the HSS.

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 HSS management and maintenance.

OEM/TSP shall disable permanently the supported weaker algorithms other than specified in ITSAR Cryptographic control list document.

Note : Any management protocols such as HTTPS over TLS 1.2 (up-to date patched) or TLS 1.3, IP Sec VPN are permitted

[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:

HSS 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.

OEM/TSP shall disable permanently the supported weaker algorithms other than specified in ITSAR Cryptographic control list document

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:

HSS 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.

HSS supports Role Based Access Control (RBAC) at Server level and Data bases level conforming to the globally accepted RBAC standard INCITS 359-2012(R2017), with default support of a minimum of 3 user roles , in particular, for OAM privilege management , for HSS Management and Maintenance, including authorization of the operation for configuration data and software via the HSS console interface.

[Reference: 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/Remote

Requirement:

In-case of Closed environment :

The various user accounts (other than system /admin accounts) on a system shall be protected from misuse. To this end, at least one authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user in closed environment

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.

In-case of Open environment (Internet):

Minimum two of the above Authentication attributes shall be mandatorily combined to protect user accounts (other than system /admin accounts) in an open environment (internet)

1.5 Remote login restrictions for privileged users

Requirement:

Login to HSS as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to HSS remotely i.e remote login access for root/admin/highest privileged users, by default shall be disabled permanently at the time of first installation.

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 HSS.

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

1.6 Authorization Policy

Requirement:

Only Role based authorization is permitted .

Bare minimum RBAC rights are to be assigned for the task to be performed.

[Reference: 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 HSS .

HSS shall also support assignment of specific id for individual accounts per user as configured by the administrator/root user, where a user could be a person, or, for Machine Accounts, an application, or a system.

For HSS, all inactive user accounts shall be locked/permanently disabled.

HSS 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

2.1 Authentication Policy

Requirement:

In-case of closed environment:

For local /Remote access , The various user accounts (other than system /admin accounts) on a HSS shall be protected from misuse. To this end, at least one authentication (Cryptographic keys or Token or Passwords) attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user in closed environment

In-case of Open environment (Internet):

For Local /Remote access, Minimum two of the Authentication attributes (Cryptographic Keys , Token , Passwords) shall be mandatorily combined to protect user accounts (other than system /admin accounts) in an open environment (internet).

[Reference: 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 HSS supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services) LDAP, Windows Login ID , Kerberos, PAM then the communication between HSS 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

OEM/TSP shall disable permanently the supported weaker algorithms other than specified in ITSAR Cryptographic control list 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 a AUTHENTICATION ATTRIBUTE blacklist to prevent vulnerable passwords.

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by HSS.

[Reference: 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 a HSS 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 HSS). It shall not be possible setting this absolute minimum length to a lower value by configuration.

(ii) Password shall mandatorily comprises 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.

If an external 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.

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

When a user is changing a password or entering a new password , HSS/central system checks and ensures that it meets the password requirements.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3]

2.5 Inactive/ Ideal 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 ranging from 2 to 5 minutes.

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

2.6 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.

a) Password change shall be enforced after initial login.
b) Passwords shall be case sensitive
c) The system shall enforce password change based on password management policy.
d) In particular, the system shall enforce password expiry. HSS shall support a configurable period for expiry of passwords.

e) Previously used passwords shall not be allowed upto a certain number (Password History).
f) The number of disallowed previously used passwords shall be Configurable; And its default minimum value shall be 3. This means that the HSS shall store at least the three previously set passwords. The maximum number of passwords that the HSS can store for each user is up to the manufacturer. The never expiring password option shall be disabled permanently
g) When a password is about to expire , a password expiry notification shall be provided to the user.

This requirement shall be met either by HSS itself or in combination with external authentication system.

[Reference: 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: 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.

[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

3.1 Secure Update

Requirement:

HSS (HSS Client application software [DBMS (Client)] 2) HSS server application software [DBMS (Server)) 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.

HSS (HSS Client application software [DBMS (Client)] 2) HSS server application software [DBMS (Server)) 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.

NS : Minor version software upgrade (update) , can done with CLI commands such as YUM , apt-get etc .System will preserve both old version of software packages and New version of Software packages . Its free to customer

3.2 Secure Upgrade

Requirement:

(i) HSS (HSS Client application software [DBMS (Client)] 2) HSS server application software [DBMS (Server)) updates software updates: 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) HSS (HSS Client application software [DBMS (Client)] 2) HSS server application software [DBMS (Server)) software updates shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the HSS shall have a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software upgrade is originated from only these sources.

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

(iv) HSS'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, and modify the list mentioned in bullet (i) above.

[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 and should be augmented with designated TSTL source code review duly supported by furnishing the Software Test Document (STD) generated while developing the HSS.

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 HSS Software, which includes vendor developed code, third party software and open source code libraries used/embedded in the HSS.

(ii)HSS software is free from all known (critical, High, Medium based on CVSS) security vulnerabilities, Security weakness listed in CVE & CWE databses on the date of product release and low severity vulnerabilities shall be addressed at the earliest.

(iii) The binaries for HSS 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 HSS is free from all known malware and backdoors as on the date of product release and shall submit Malware Test Document (MTD) of the HSS to the designated TSTL.

3.5 No unused software packages

Requirement:

Software components or parts of software which are not needed for operation or functionality of the (HSS Client application software [DBMS (Client)] 2) HSS server application software [DBMS (Server)) software shall not be present.

Orphaned software components /packages shall not be present in HSS (DBMS + Data base application)

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

3.6 Insecure Services/protocols Removal

Requirement:

HSS 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.

HSS supporting protocol handlers and services which donot have any known security vulnerabilities shall be disabled by default and can be enabled by operator as per his requirement .

In particular, by default insecure services having known vulnerabilities shall be permanently disabled by the vendor.

[Reference: 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:

HSS 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]

3.8 Secure Time Synchronization

Requirement:

HSS shall provide reliable time and date information provided manually by itself or through NTP/PTP server. HSS shall establish secure communication channel strictly using the secure crypto controls prescribed in the table 1 of ITSAR for cryptographic controls document with the NTP/PTP server.

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

3.9 Restricted reachability of services

Requirement:

The HSS 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.

[Reference: TSDSI STD T1.3GPP 33.117-1 4.2.0 V.1.0.0 Section 4.3.2.2]

3.10 Avoidance of Unspecified Wireless Access

Requirement:

An undertaking shall be given by the vendor as follows:

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

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

3.11 Disable all software based reset options (disable control+alt+delete option)

Requirement:

All the software based reset options e.g., ctrl+alt+delete option which forcibly reboot the HSS system and/or forces the running programs to stop, shall be permanently disabled.

3.12 Lockdown CRON jobs

Requirement:

CRON jobs for carrying out the tasks such as scheduling the backups, monitoring disk space, deleting files and system maintainance activities shall be executed by the privileged user such as administrator only.

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 HSS shall not be present in the HSS's software and/or hardware.

[Reference: 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 HSS shall not contain software and/or hardware components that are no longer supported by Vendor or its 3rd Parties including the open source communities , such as components that have reached end-of-life or end-of-support.

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

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 but not allowed to delete or modify the log files.

The Audit log file may contain sensitive information such as text of SQL commands shall be access controlled using file access rights such that only privileged users including the administrator have access to read the log files but not allowed to delete or modify the log files.

Audit log files contents shall be encrypted complied to 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: 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 HSS shall log all important Security events with unique System Reference details as given in the Table below.

Each audit log record shall have at least information pertaining to Record ID , Date/Time stamps, Connection ID , query executed , Host name , IP address , User Name, Command status (success or error) and Command class

EventTypes(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
	Records all account administration activity, i.e.	• Administrator username, • Administered account,

Account administration(Mandatory)	configure, delete, enable, and disable.	• 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 OR where the network device has crashed.	• Action performed (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 (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)
access to personal data (Mandatory)	All use of identification and authentication mechanism	user identity origin of attempt (e.g.IP address) Timestamp Personal data in encrypted text(Optional) outcome of event (Success or failure)
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
		• Username

All activities of the remote user other than Root User (Mandatory)	Records all the activities performed by the remote user on the DUT	• Source (IP address)
		Outcome of event (Success or failure)
		interface type
		Event level (e.g. CRITICAL, MAJOR, MINOR)
		Command/activity performed
		• Timestamp

[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:

(I) (a) The HSS 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 HSS. The communication mechanism between the HSS and the external log server/system should strictly use 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) HSS shall be able to store generated audit data itself, may be with limitations.

(III) HSS shall alert administrator when its security log buffer reaches configured threshold limit .

(IV) In the absence of External system, HSS shall stop its services when its own security event log buffer is full .

[Reference: 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:

HSS 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 " only.

Vendor shall give to TSTL, the list of connected entities with HSS and the method of communications with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing communication by HSS with each entity and any other details required for testing this requirement.

Communication Between HSS-MME (S6a interface), HSS-PCRF (Sh interface), MME –SGSN (S3 interface), SGSN – HLR/AUC (Gr,Gf interface) shall be protected with Cipher and Integrity protection

6.2 Cryptographic Module Security Assurance

Cryptographic module embedded inside the HSS (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 also submit cryptographic algorithm implementation testing document and the test results to designated TSTL for scrutiny.

6.3. Cryptographic Algorithms implementation Security Assurance

Cryptographic algorithms embedded in the crypto module of HSS shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm)

Vendor shall also submit cryptographic algorithm implementation testing document and the test results to designated TSTL for scrutiny.

6.4. Protecting data and information – Confidential System Internal Data

Requirement :

When HSS 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: 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 HSS system that are needed for the functionality shall be protected against manipulation 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.

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 (such as passwords) 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: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "only.

(iv) To prevent password recovery using rainbow tables, do not store the password in plain text instead, choose some string to be used as a salt, and use hash(hash(password)+salt) values

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

6.6 Protection against Copy of Data

Requirement :

HSS shall not create a copy of data in use and data in transit.

Protective measures shall exist against use of available system functions / software residing in HSS to create copy of data for illegal transmission. The software functions, components in the HSS for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

6.7 Protection against Data Exfiltration - Overt Channel

Requirement :

HSS shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit. Establishment of outbound overt channels shall not be allowed and not configured to be used in HSS .

6.8 Protection against Data Exfiltration - Covert Channel

Requirement :

HSS shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.

Establishment of outbound covert channels and tunnels shall not be allowed if they are initiated by / originated automatically from the HSS i.e the HSS shall not have a session or process established/initiated without a configured user or a system user.

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

Section 7: Network Services

7.1 Traffic Separation

Requirement:

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

[Reference: 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:

HSS shall have protection mechanism against known network level and Application level DDoS attacks.

HSS 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 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]

8.2 Excessive Overload Protection

Requirement:

HSS shall act in a predictable way if an overload situation cannot be prevented. HSS 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 HSS 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: 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:

HSS shall respond with error messages, anomalous responses, crash responses when receiving unexpected input request/malformed input request.

Vendors should document the list of protocol stacks supported by HSS for all traffic planes (management, control, data plane and service/application plane) [Reference: 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 HSS , only documented ports on the transport layer respond to requests from outside the system.

Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters like Date & Time stamp, Source IP address, destination Port address etc.

The test for this requirement can be verified by using a suitable port scanning tool.

[Reference: 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 there no known vulnerabilities exist in the HSS at the time of product release.

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

The test for this requirement can be verified by using a suitable Vulnerability scanning tool.

[Reference: 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 HSS 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 HSS 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]

10.2 Handling of ICMP

Requirement:

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

HSS 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

HSS 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: 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:

HSS 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]

10.4 System account identification

Requirement:

Each system account in HSS 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]

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 HSS

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

[Reference: 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:

HSS 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]

10.7 Protection from buffer overflows

Requirement:

HSS shall support mechanisms for buffer overflow protection.

[Reference: 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 HSS in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

[Reference: 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:

HSS 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]

Section 11: Web Servers

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

11.1 HTTPS

Requirement:

OEM/TSP shall disable permanently the supported weaker algorithms other than specified in ITSAR Cryptographic control list document

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: 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 HSS webserver (for both successful as well as failed attempts) shall be logged by HSS.

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]

11.3 HTTPS input validation

Requirement:

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

HSS 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]

11.4 No system privileges

Requirement:

No HSS 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]

11.5 No unused HTTPS methods

Requirement:

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

[Reference: 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 HSS 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]

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]

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]

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]

11.10 Access rights for web server configuration

Requirement:

Access rights for HSS 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]

11.11 No default content

Requirement:

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

[Reference: 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: 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 HSS 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]

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

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

[Reference: 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 HSS operation shall be deleted.
[Reference: 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 HSS web server's document directory.

In particular, the HSS 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]

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

12.1 No Password reset

Requirement:

In the event of HSS system password reset with appropriate authentication and access control , the entire configuration of the HSS shall be irretrievably deleted .

No provision shall exists for HSS system password reset by attacker

12.2 Secure System Software Revocation

Requirement:

Once the HSS 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.

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

12.3 Software Integrity Check – Installation

Requirement:

HSS 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.

12.4 Software Integrity Check – Boot

Requirement:

The HSS 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 document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 " to the expected reference value.

HSS shall support the possibility to verify software image integrity at boot time, detecting, for example, software image tampering and/or unauthorized software image updates.

12.5 Unused Physical and Logical Interfaces Disabling

Requirement:

HSS 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 disabled.

12.6 No Default Profile

Requirement: Predefined or default user accounts in HSS shall be deleted or disabled.

12.7 Security Algorithm Modification

Requirement:

It shall not be possible to modify security algorithms supported by HSS

It shall not be possible to modify security algorithms supported by HSS through unauthorized access, e.g. to perform a downgrade attack by deceiving the nodes to use a weaker algorithm

Section 13: Database specific security requirements

13.1 No default accounts

Requirement:

All Default (any test accounts) and anonymous accounts (for eg: "@'localhost') that are not intended for normal operation of HSS database shall be deleted.

13.2 Renaming of root account

Requirement:

HSS database by default comes with root account like ‘root'@'localhost’ that is used for administrative purposes. This account has all privileges, is a system account, and can perform any operation. HSS database shall support renaming of the root account to something else (choice of OEM) to avoid exposing a highly privileged account with a well-known name. Such “root” account shall be renamed.

13.3 No default database

Requirement:

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

13.4 Unique identity

Requirement:

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

13.5 Non-disclosure of sensitive information

Requirement:

Sensitive information like passwords shall be masked while entering on the terminal and in the entries in command line history related to password (set, modify).

13.6 Password management and validation policy

Requirement:

HSS database shall support the following password-management capabilities and password validation policy,

a. Password expiration, to require passwords to be changed periodically. (default password lifetime) – for every 60 days

b. Password reuse restrictions, to prevent old passwords from being chosen again. (password_history and password_reuse_interval) – reuse of last 3 passwords is restricted within 180 days

c. Password verification, password changes (replace and reset) must specify the current password (PASSWORD REQUIRE)

d. Dual passwords, to enable clients to connect using either a primary or secondary password. - shall be disabled

e. Password generation by root/administrator account for other accounts shall be random (default length of 20 characters)

f. Connection to HSS database shall be refused from the accounts that are in locked state.

13.7 Restricted access to sensitive information

Requirement:

Access to sensitive information stored in tables and logs shall be restricted to only authorised accounts. For eg., MySQL stores passwords for user accounts in the mysql.user system table. Access to this table shall be restricted to only root account.

13.8 Secure storage

Requirement:

a. Data (databases, tables, contents of tables) of HSS database shall be stored in an encrypted manner.

b. Data shall not be transmitted in plain (unencrypted) text over the Internet.

c. Encryption methods shall comply 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 HSS management and maintenance

13.9 Secure logs

Requirement:

a) Log files shall be stored in an encrypted manner. Encryption methods shall comply Secure cryptographic controls prescribed in Table1 of the document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "

b) Sensitive information available in the logs such as passwords shall be masked/hashed.

c) Contents of audit log files shall be encrypted as it contains sensitive information, such as the text of SQL statements.

d) Audit log files should be written to a directory accessible only to the HSS database server and to users with a legitimate reason to view the log.

e) Log shall be generated by HSS specific to the database for the events

- DBMS (Sever) Login (success or error) events
- Executed SQL statements
- Create table , Drop Table and Modify the table
- Modify Table at Row Level
- Modify Table at Column Level
- Deleting Data from Tables
- Successful and Unsuccessful deletion of Rows from Tables
- Activities in related with updating the tables

13.10 User privileges

Requirement:

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

• Administrative privileges enable users to manage operation of the database server. These privileges are global because they are not specific to a particular database.

• Database privileges apply to a database and to all objects within it. These privileges can be granted for specific databases, or globally so that they apply to all databases.

• Privileges for database objects such as tables, indexes, views, and stored routines can be granted for specific objects within a database, for all objects of a given type within a database (for example, all tables in a database), or globally for all objects of a given type in all databases.

13.11 Protection from attacks

Requirement:

a) Data base shall be protected from SQL injection attacks & No SQL injection attacks

b) Default Port (in case of Mysql: 3306) should not be accessed by External attackers. Such port shall be blocked on Firewall /Router. HSS database shall use a different port other than default port for its connections.

c) Database shall recover securely from correction, loss, damage.

d) Database shall support security mechanisms to protect from DDoS attacks.

Data base system 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 shall include, but not limited , to the following:

- Use stored procedures instead of implementing Direct queries
- The number of queries an account can issue per hour
- The number of updates an account can issue per hour
- The number of times an account can connect to the server per hour
- The number of simultaneous connections to the server by an account (global max_user_connections value is 10)

13.12 Secure Back ups

HSS shall support secure mechanisms for taking back up of Data base files , configuration files, log files

ABBREVIATIONS

AAA Server	Authentication, Authorization, and Accounting Server
ACL	Access Control Lists
AES	Advanced Encryption Standard
CERT	Computer emergency response teams
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDOS	Distributed Denial of Service
NE	Network Element
EMS	Element management System
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPSec VPN	Internet Protocol Security Virtual Private Network
MC/DC	Modified Condition / Decision Coverage
MD5	Message Digest Algorithm
MISRA	Motor Industry Software Reliability Association
NIST	National Institute of Standards and Technology
NMS	Network management System
NTP	Network Time Protocol
OMC	Operation and maintenance Console
OS	Operating System
OSPF	Open Shortest Path First
PTP	Precision Time protocol
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SFTP	Secure File Transfer Protocol

SHA	Secure hash Algorithm
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
TLS VPN	Transport Layer Security Virtual Private Network
URPF	Unicast Reverse Path Forwarding
AES	Advanced Encryption Standard
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AN	Access Network
AS	Access Stratum
AUTN	Authentication token
AV	Authentication Vector
ASME	Access Security Management Entity
DoS	Denial of Service
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
eNB	Evolved Node-B
EPC	Evolved Packet Core
EPS	Evolved Packet System
EPS-AV	EPS authentication vector
E-UTRAN	Evolved UTRAN
GUTI	Globally Unique Temporary Identity
HE	Home Environment
HSS	Home Subscriber Server
IK	Integrity Key

IKE	Internet Key Exchange
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
KDF	Key Derivation Function
KSI	Key Set Identifier
MAC	Message Authentication Code
ME	Mobile Equipment
MME	Mobility Management Entity
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
NAS	Non Access Stratum
NCCS	National Centre For Communication Security
NTP	Network Time Protocol
OS	Operating System
PLMN	Public Land Mobile Network
PRNG	Pseudo Random Number Generator
PTP	Precision Time Protocol
RAND	RANDom number
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SN	Serving Network
SN id	Serving Network identity
SQN	Sequence Number
SRVCC	Single Radio Voice Call Continuity
S-TMSI	S-Temporary Mobile Subscriber Identity
TAI	Tracking Area Identity
TAU	Tracking Area Update
UE	User Equipment

UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UP	User Plane
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
XRES	Expected Response

Annexure A

LIST OF UNDERTAKINGS TO BE FURNISHED BY THE VENDOR FOR HSS 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)