सत्यमेव जयते

Indian Telecom Security Assurance Requirements

For

Home Subscriber Server (HSS)

NCCS / ITSAR / CORE / 4G-HSS

NCCS

Securing Networks

Release Date: 25/03/2022 Version: 1.0.0

Date of Enforcement:

National Centre for Communication Security (NCCS), Bengaluru
Department of Telecommunications
Ministry of Communications
Government of India

Abstract

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:

© NCCS 2022

Table of Contents

NCCS
Securing Networks

© NCCS 2022

NCCS
Securing Networks

NCCS
Securing Networks

© NCCS 2022

Securing Networks

Scope of Work

This document contains Indian Telecom Security Assurance Requirements (ITSAR) specific to the Home Subscriber Server (HSS) , a 4G core network element.

NCCS
Securing Networks

© NCCS 2022

Common Security Requirements (CSR)

Section 1: Access and Authorization

1.1 Management Protocols Mutual Authentication

Modified Security Requirement:

The protocols used for the HSS (Home Subscriber Server) management and maintenance shall support mutual authentication mechanisms only

Secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" shall be used for HSS 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:

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

NCCS
Securing Networks

[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

© NCCS 2022

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) with 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.

[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:

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 user name, 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 (single authentication attribute in case of machine account) for protecting the all accounts from misuse.

Securing Networks

Machine Accounts: These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.

Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from HSS 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.1]

© NCCS 2022

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.

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 HSS

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

1.6 Authorization Policy

NCCS
Securing Networks

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: 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

© NCCS 2022

Requirement:

Users shall be identified unambiguously by the HSS.

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

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]

NCCS
Securing Networks

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 in case of user accounts (e.g. password, certificate, token) and single authentication attribute in case of machine account, 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: 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

© NCCS 2022

Requirement:

If the HSS supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services) 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 latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”

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 HSS.

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

NCCS
Securing Networks

2.4 Enforce Strong Password

Requirement:

(a) The configuration setting shall be such that an 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 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.

HSS 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 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. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).

Securing Networks

[Reference: 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.

© NCCS 2022

HSS shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement, normally set between 2 to 5 minutes.

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

2.6 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. HSS shall support a configurable period for expiry of passwords.

Previously used passwords shall not be allowed upto a certain number (password history).

NCCS
Securing Networks

The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its 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.

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.

© NCCS 2022

HSS 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 HSS

[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]

Securing Networks

2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the vendor provides instructions on how to manually change it.

© NCCS 2022

[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:

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

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

3.2 Secure Upgrade

Requirement:

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

(ii) HSS shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls as prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.. To this end, the HSS 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) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in point 2.

© NCCS 2022

[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) OEM shall follow security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).

b) Also OEM shall submit the undertaking as below:

(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the HSS software, which includes vendor developed code, third party software and open source code libraries used/embedded in the HSS.

(ii)The HSS software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of HSS to designated TSTL for testing. For other security weaknesses, OEM shall give mitigation plan.

(iii) The binaries for HSS and upgrades/updates thereafter generated from the source code are free from CWE top 25 & OWASP top 10 security weaknesses.

NCCS
Securing Networks

3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that HSS is free from all known malware and backdoors as on the date of offer of HSS to designated TSTL for 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 HSS shall not be present.

© NCCS 2022

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

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

OEM shall furnish an undertaking as “HSS does not contain Software that is not used in the functionality of HSS”

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

3.6 Unnecessary Services 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 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

Securing Networks

© NCCS 2022

-	MOP

Full documentation of required protocols and services (Communication matrix) of the Network product and their purpose needs to be provided by the OEM as prerequisite for the test case

[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 by itself or through NTP/PTP server.

HSS shall provide reliable time and date information provided through NTP/PTP server. HSS shall establish secure communication channel with the NTP/PTP server.

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

NCCS
Securing Networks

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

© NCCS 2022

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.

Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.

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

3.10 Self Testing

Requirement:

HSS 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.

NCCS
Securing Networks

Section 4: System Secure Execution Environment

4.1 No unused functions

Requirement:

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

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

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

© NCCS 2022

4.2 No unsupported components

Requirement:

OEM to ensure that the HSS shall not contain software and 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.5]

4.3 Avoidance of Unspecified Mode of Access

Requirement:

HSS shall not contain any mode of access (e.g.,wireless) mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM 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]

NCCS Securing Networks

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.

© NCCS 2022

[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.

HSS 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

© NCCS 2022

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)

© NCCS 2022

		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,	user identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)

	Termination of an interactive session	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:

© NCCS 2022

(I) (a) The HSS shall support forwarding 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.

(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 (due to loss of connectivity or due to node failure or due to any other reasons), HSS shall have mechanism to store audit data locally. HSS shall have sufficient memory (minimum 100 MB) allocated for this purpose. OEM to submit justification document for sufficiency of local storage requirement.

Secure Log export shall comply the Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

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

Securing Networks

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 latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

6.2 Cryptographic Module Security Assurance

© NCCS 2022

Requirement:

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.

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

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

Requirement:

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

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

NCCS
Securing Networks

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

OEM 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:

© NCCS 2022

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.

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 Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

(ii) Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

(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 latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

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.

© NCCS 2022

[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 :

Without authentication, HSS shall not create a copy of data in use or 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 / data in transit. Establishment of outbound overt channels such as, HTTPS IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network product.

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

Securing Networks

6.8 Protection against Data Exfiltration - Covert Channel

Requirement :

HSS shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network Product.

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

© NCCS 2022

Section 7: Network Services

7.1 Traffic Filtering – Network Level

Requirement:

HSS shall provide a mechanism to filter incoming IP packets on any IP interface

In particular the Network product shall provide a mechanism:

(i) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.

(ii) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:

- Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
- Accept: the matching message is accepted.
- Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

(iii) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.

(iv) To filter on the basis of the value(s) of any portion of the protocol header.

(v) To reset the accounting.

(vi) The Network product shall provide a mechanism to disable/enable each defined rule.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.6.2.1]

7.2 Traffic Separation

© NCCS 2022

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].

7.3 Traffic Protection – Anti-Spoofing

Requirement:

Systems shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

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

NCCS
Securing Networks

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.

© NCCS 2022

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 (as applicable to HSS) 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: 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]

8.3 Filtering IP Options

Requirement:

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

NCCS
Securing Networks

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

Section 9: Vulnerability Testing Requirements

9.1 Fuzzing – Network and Application Level

Requirement:

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

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

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.

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

Securing Networks

9.3 Vulnerability Scanning

Requirement:

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

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

Section 10: Operating System

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.

© NCCS 2022

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]

NCCS
Securing Networks

© NCCS 2022

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. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by the OEM.

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

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

© NCCS 2022

escalation or extended access permissions due to the contents of the mounted file systems.

OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g. USB drive, CD ROM etc.) for data transfer.

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

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]

10.10 Restrictions on running Scripts / Batch-processes

Requirement:

HSS shall have feature to restrict Scripts / Batch-processes / Macros usage among various users. It shall be administratively configurable to permit or deny the use. E.g. It is possible to administratively configure scheduled tasks usage (permit / deny) among various users like Normal users, privileged users.

10.11 Restrictions on Soft-Restart

Securing Networks

Requirement:

HSS shall restrict software-based system restart options usage among various users. The software reset / restart either through command or use of key-combinations like CTRL+ALT+DEL is not available to normal users for prevention of unintended / malicious trigger of system reset / restart.

Section 11: Web Servers

This entire section of the security requirements is applicable if the HSS 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 latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

[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

Securing Networks

[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.

Securing Networks

[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.

© NCCS 2022

[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]

NCCS Securing Networks

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.

© NCCS 2022

[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]

NCCS Securing Networks

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 OEM.

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

© NCCS 2022

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]

NCCS Securing Networks

Section 12: Other Security requirements

12.1. Remote Diagnostic Procedure – Verification

Requirement:

If the HSS is providing Remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user.

All activities performed by the remote user are to be logged with the following parameters:

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

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

12.2 No system/root Password recovery

Requirement:

No provision shall exist for HSS system / Root password recovery.

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

Securing Networks

12.3 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.

© NCCS 2022

12.4 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 latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

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

12.5 Software Integrity Check – Boot

Requirement:

The HSS 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 latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” to the expected reference value.

NCCS
Securing Networks

12.6 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 so that they remain inactive even in the event of a reboot.

12.7 No Default Profile

Requirement:

No pre-defined user accounts other than one Highest privilege (Admin / Root) user account would be available.

12.8 Security Algorithm Modification

Requirement:

It shall not be possible to modify security algorithms supported by HSS without admin / root credentials. Bidding-down beyond prescribed security / cryptographic algorithms by means of negotiation by communicating entities is not permitted.

HSS Specific Security Requirements (SSR)

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.

NCCS
Securing Networks

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.

© NCCS 2022

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).

NCCS
Securing Networks

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

© NCCS 2022

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.

NCCS Securing Networks

b. Encryption methods shall comply Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”. shall only be used for HSS management and maintenance

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

© NCCS 2022

13.9 Secure logs (database specific)

Requirement:

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

b) Information available in the logs about authentication attributes shall be masked/hashed.

c) 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.

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

- DBMS (Sever) Login (success or error) events
- Attempted/Executed database statements/queries

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,

NCCS Securing Networks

• 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.

© NCCS 2022

13.11 Protection from attacks

Requirement:

a) Data base shall be protected from database injection attacks.

b) Port used by the database service shall not be accessed by unauthorised entities. 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 and their transmission.

© NCCS 2022

13.13 Secure transmission of database information

Data shall not be transmitted in plain (unencrypted) text. HSS – database application shall necessarily deploy TLS / DTLS (refer to Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”. to communicate with other nodes.

13.14 Traffic Protection

TLS/DTLS shall be implemented for the diameter protocol interfaces eg. Sh, Gr, etc between the HSS and the connected/connecting entities and by strictly using the Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

For the interfaces that carry other than diameter traffic shall be protected with the IPsec and by strictly using the Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

Securing Networks

© NCCS 2022

Annexure -I

Acronyms

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
HSS	Home Subscriber Server
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

NCCS
Securing Networks

© NCCS 2022

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

Securing Networks

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

NCCS
Securing Networks

© NCCS 2022

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

NCCS
Securing Networks

Annexure -II

List of undertakings to be furnished by the OEM 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)

NCCS
Securing Networks

© NCCS 2022