NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB), CABINET DIVISION

PAKISTAN SECURITY STANDARD FOR CRYPTOGRAPHIC & INFORMATION TECHNOLOGY SECURITY DEVICES

Cryptographic Security Guide Book

(Public Domain)

PAKISTAN STANDARDS AND QUALITY CONTROL AUTHORITY (PSQCA)
Standards Development Centre, PSQCA Complex, Gulistan-e-Jauher, Karachi

ICS: 35.020;35.030

PAKISTAN SECURITY STANDARD FOR CRYPTOGRAPHIC & INFORMATION TECHNOLOGY SECURITY DEVICES

Cryptographic Security Guide Book

(Public Domain)

DOCUMENT CODE INDEX	**:**	**PSS-GB-CRYPTOSEC-V1.0**
DOCUMENT TYPE	**:**	**PUBLIC**
CLASSIFICATION	**:**	**PUBLIC**
DATE OF ISSUE	**:**	**14 JUNE 2023**
ISSUING AUTHORITY	**:**	**PSQCA (PS: 5544-2021 -** ICS: 35.020;35.030**)**

PAKISTAN STANDARDS AND QUALITY CONTROL AUTHORITY (PSQCA)
Standards Development Centre, PSQCA Complex, Gulistan-e-Jauher, Karachi

Pakistan Security Standard for Cryptographic & IT Security Devices

Announcing the Standard for

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC & IT SECURITY DEVICES

This Pakistan Security Standard was adopted by the Pakistan Standards & Quality Control Authority Standards Development Centre on recommendation of National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, on 09-11-2021 after draft finalization and approval by National Standards Committee (NSC) for Information Technology. In the preparation of this standard the views of Cyber Security Specialists, Experts from Academia, Product Developers, Product Vendors, Testing Authorities, Regulatory Authorities and User Organizations have been taken into consideration.

1. Name of Standard. This standard may be called the **'**Pakistan Security Standard (PSS) for Cryptographic & IT Security (ITSec) Devices'. This standard consists of PSS-GB-CRYPTOSEC and PSS-GB-ITSEC.

2. Category of Standard. Information Security**,** Cryptography, Computer Security, IT Security, Network Security, Application Security, Cyber Security.

3. Explanation. PSS Guidebooks delineate guidelines for ensuring mandatory security and technical requirements that shall be satisfied by Cryptographic & ITSec Equipment (CE) and Cryptographic Algorithms or Primitives (CP) for sectors requiring such security systems to protect sensitive information in computer, telecommunication or cyber systems. The standard provides four increasing, qualitative levels of overall security; Level 1 (Low), Level 2 (Basic), Level 3 (Medium), and Level 4 (High); for the equipment comprising CE, CP and Supported Systems i.e. Key Management System and Network Management System; referred to as Crypto Equipment & Primitives (CEP) throughout PSS. These levels are intended to cover wide range of potential applications and environments in which a CE, CP or CEP may be employed.

PSS ITSec Guidebook outline guidelines for ensuring mandatory security and technical requirements that shall be satisfied by ITSec products and services. Till such time that a separate 'National IT Security Certification Scheme' is developed in line with Common Criteria (CC) Evaluation Methodology and promulgated, PSS will also serve as ITSec evaluation standard.

Vendors, developers and sponsors of Cryptographic & ITSec products shall request product or services evaluation from NTISB which will assign responsibility to any accredited laboratory for

evaluation of Cryptographic & ITSec products. Pakistan National Accreditation Council (PNAC) accredited Cryptographic & ITSec testing laboratories shall perform CEP compliance/ conformance testing after receiving vendors/ sponsors requests through NTISB. This standard supersedes TM-27, *Procedure for Introduction of a New Crypto Machine and Speech Secrecy Equipment in Pakistan*, in its entirety.

4. Approving Authority. Government of Pakistan.

5. Maintaining Agency. National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, Government of Pakistan.

6. Applicability. Consumer electronics or IT systems or solutions that do not claim the provision of security functionality are excluded from PSS certification**.** List of items covered under PSS is as below:-

a. **Cryptographic**. Such articles that claim provision of confidentiality, integrity, authentication, availability and/ or non-repudiation to users, networks or systems such as all kinds of cryptographic encryptors, hardware security modules, key generation, management or distribution systems, cryptographic tokens or systems for secure access or user authentication, cryptographic algorithms or protocols or operations, cryptography based communication or web applications, secure Virtual Private Networks or other such solutions.
b. **IT Security**. Such articles that claim provision of specific cyber security functions such as all kinds of firewalls, network routers, high capacity switch, intrusion detection & prevention, endpoint security, secure access control systems, security information management, security information and event management, secure operating systems, secure applications, secure database management, anti-denial of service, anti-virus, anti-spyware, anti-theft, anti-malware or any other such solution.

7. Applications. NTISB shall validate Cryptographic & ITSec equipment to PSS. Products validated as conforming to PSS shall be accepted and preferred by the government organizations and departments for protection of sensitive information till such time that PSS becomes mandatory. The goal of PSS is to promote use of validated Cryptographic & ITSec products and services and provide critical sectors with a security metric to use in such procurements. This standard **shall also** be used in designing and implementing cryptographic and ITSec products and services that government organizations and critical sectors either operate or are operated for them. After analyzing guidebooks, vendors and developers of security solutions will request NTISB for provision of restricted release documents that contain additional information. The adoption and use of this standard is also encouraged for private and commercial sector organizations. Cryptography-based

security systems may be utilized in various computer, telecommunication, and cyber security applications (e.g., authentication, authorization, access control, data at rest and motion, personal identification, IP networks and fixed telecom network communications, wireless communication i.e. radio, mobile, satellite etc.) that may be used in various operating environments (e.g., centralized or distributed environments, remote access scenarios and hostile environments etc.). The cryptographic functions for data secrecy, data integrity, personal identification, digital signatures and management of cryptographic keys etc. are based on factors that are specific to the application and operating environment. Users of critical sectors shall select equipment or services of a level of security appropriate for the organizational requirements commensurating to application and environment in which the equipment or service will be utilized or provided. Developers of local industry will acquire PSS guidance from NTISB for designing security equipment and services for local as well as export markets. Vendors or sponsors of security equipment will approach NTISB for conduct of security strength testing through Evaluation Labs that will assure users regarding achieved security level against vendor or developer claims.

8. Interpretation. Questions concerning the content and specifications of this standard shall be addressed to: Secretary, NTISB, Cabinet Division, Islamabad (www.cabinet.gov.pk).

9. Qualifications. The security requirements specified in this standard are approved by Pakistan Standards and Quality Control Authority (PSQCA) which are based upon information provided by various sectors such as Public, Private, Academia, Industry and International Standards from NIST, ISO/ IEC and Common Criteria etc. The requirements are designed to aid in protecting sensitive data and services against attacks by adversarial entities e.g. insiders, hackers, hacktivists, unauthorized entities, economic and non-aligned competitors etc. While the security requirements specified in this standard are intended to maintain the security provided by a Cryptographic & ITSec product, conformance to this standard is not sufficient to ensure that a particular product is secure. User of a Cryptographic & ITSec product is responsible for its secure configuration, operation, maintenance and ensuring that the security provided by a product is sufficient and acceptable to the owner of the information that is being protected. Any residual risk is acknowledged and accepted by the responsible authority in each organization along with the enforcement responsibility of NTISB recommendations.

New or revised requirements may be needed to meet technological and economic changes with scientific and cryptographic evolution. This standard shall be reviewed, revised and updated after every 3 years or as and when required on the instructions of NTISB who will designate a Review Committee from stakeholders**.** PSS will retain relevance in implementation of information, IT and cyber security aspects of national policies on use of cyber, cloud, broadband, data protection and

other such policies as and when these are promulgated. All users will obtain latest version from PSQCA, NTISB and provide required information and data in accordance with the provisions of latest PSS publications. For guidance on subjects not covered by PSS, respective standard/ guideline/ best practice of US NIST, Common Criteria, OWASP, SANS, ISO/ IEC, ILAC etc. may be referred.

10. Implementation Schedule. This standard will become mandatory in 5x years' time frame (with effect from **1st June 2028**). However, its earlier adoption is recommended and sectors requiring immediate adoption for deployment may undertake appropriate actions at their level with consultation of respective regulators and/ or PPRA. As PSS security requirements are in line with International security standards, relevant product certifications such as US NIST FIPS 140-2 and/ or Common Criteria etc. may be produced by vendors and accepted till such time that PSS certification becomes mandatory for critical sectors. NTISB shall devise business model and strategic plan to facilitate and encourage establishment of Cryptographic & ITSec Evaluation labs for PSS based testing in public, private and academia sectors. Till such time (which shall not exceed 2 years) that labs get accreditation under National Accreditation Standard for Crypto & ITSec Evaluation Labs (NASCEL), decision for employing existing infrastructure and facilities in public sector rests with NTISB. Before the standard becomes mandatory, sectors requiring security of information & systems shall develop phase-out and procurement plans to comply with PSS requirements. NTISB shall maintain validated product list on NTISB website and devise a controlled mechanism for Vendors and Developers for restricted release of additional technical documents depending upon type, configuration and operational environment of the security solution. Organizations may purchase any of the products on the NTISB validated product list as per their environment, operational and information security requirements. Use of such equipment will however be subject to conformance to the security requirements, applicability of the security profile of the equipment or service and NTISB guidance.

Sr No	**Sector**	**Timelines**		
		PSS Compliance (Product Conformance to PSS)		**PSS Certification** (Product Evaluation as per PSS)
		New Procurement	Existing Operational Products	
a	**Government** (Federal, Provincial, Ministries, Regulatory bodies, Education, Health, LEAs, Energy sector, Railways, Critical Organizations such as CAA, NADRA, Immigration, Ehsaas, etc.)	• International Certifications (FIPS, CC, etc.) may be acceptable as per sector regulator/ user organization security requirement till PSS	• Phase-Out Plan to be developed before PSS becomes mandatory. • Product Phase out may be implemented as per sensitivity of	Mandatory after **5x years**

<table>
<tr><th rowspan="2">Sr No</th><th rowspan="2">Sector</th><th colspan="3">Timelines</th></tr>
<tr><th colspan="2">PSS Compliance
(Product Conformance to PSS)</th><th>PSS Certification
(Product Evaluation as per PSS)</th></tr>
<tr><th></th><th></th><th>New Procurement</th><th>Existing Operational Products</th><th></th></tr>
<tr><td>b</td><td>Defense
(Services including all related organizations)</td><td rowspan="4">becomes mandatory or as per priority set by respective sector regulator.

• Must be PSS Compliant after 5x years.

• Interoperability with existing systems to be ensured.</td><td rowspan="3">organization and information alongwith financial implications.</td><td rowspan="4"></td></tr>
<tr><td>c</td><td>Semi-Government or Autonomous bodies</td></tr>
<tr><td>d</td><td>Telecom & ISPs
(including mobile, data and fixed telephony service providers)</td></tr>
<tr><td>e</td><td>Banking and Financial</td></tr>
<tr><td>f</td><td>Private & Industrial Sectors</td><td></td><td>If dealing with Personal Identifiable Information (PII), Intellectual Property (IP), sensitive projects, sensitive data or related to critical infra etc, Phase-Out Plan to be developed before PSS becomes mandatory after 5x years or as per respective sector regulator priority.</td></tr>
</table>

Table - PSS Implementation Schedule

11. Where to obtain copies of this Standard. This publication is available at NTISB and PSQCA websites. Other computer security publications issued by NTISB are also available at NTISB website.

12. List of Authors, Contributors, Reviewers & Approval Committees

S/N	Name	Information	
PSS AUTHORS PANEL			
1.	Dr Nassar Ikram	dr_nassar_ikram@yahoo.com	National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, Pakistan +92-051-9208054 +92-051-9207930 pss-devpanel@cabinet.gov.pk
2.	Dr Nadeem Sial	nadeem@commoncriteria.gov.pk	
3.	Kashif Rahim	kashif@commoncriteria.gov.pk	
4.	Dr Asad Khan Sadozai	mabu.maaz@gmail.com	
5.	Muhammad Umair Tariq	m.omair.tarik@gmail.com	
6.	Uroosa Kiran	uroosakiran@gmail.com	
7.	Muhammad Amir	muhammad.aamir.tariq@gmail.com	
8.	Ali Afzal Awan	aaa.phdis@students.mcs.edu.pk	
9.	Raja Zeeshan Haider	rhaider.phdismcs@student.nust.edu.pk	
PSS REVIEWING PANEL			
1.	Mansoor Sehgal	Secretary, NTISB	
2.	Dr Baber Aslam	ababer@mcs.edu.pk	
3.	Syed Junaid Imam	Member IT, MoIT&T	
4.	Dr Muhmmad Tayyab Ali	MCS, NUST, Islamabad	

S/N	Name	Information	
5.	Sharjeel Zareen		
6.	Dr Liaqat Ali Khan	Air University, Islamabad	
7.	Dr Muhammad Qasim Saeed		
8.	Khalid Habib	Bahria University, Islamabad	
9.	Dr Mureed Hussain	National Engineering & Scientific Commission (NESCOM)	
10.	Dr Sheraz Ahmed		
11.	Dr Safdar Shaheen		
12.	Dr Mehreen Afzal	Director Security & GRC, pkCERT, MoIT&T	
13.	Abdul Rehan Khan	Department of Communication Security (DCS)	
14.	Ghazenfer Abbas	Pakistan Telecommunication Authority (PTA)	
15.	Dr Maajid Khan	Institute of Space Technologies (IST), Islamabad	
16.	Mohsin Ali	Inbox Business Tech (Pvt) Ltd	
17.	Mahir Mohsin Sheikh	Trillium Information Security Systems	
18.	Ismat Gul Khattak	DG, Pakistan National Accreditation Council (PNAC)	
19.	Azhar Khan	Director, Pakistan National Accreditation Council (PNAC)	
PSS STAKEHOLDERS PANEL			
1.	Shazia Shah	National Telecom Corporation (NTC)	
2.	Irfan Rafi		
3.	Faisal Ayub	National Database and Registration Authority (NADRA)	
4.	Muhammad Sibtain	Department of Communication Security (DCS)	
5.	Aalishan Akhter	Ministry of Information Technology and Telecommunication (MoIT&T)	
6.	Muhammad Imran	Frequency Allocation Board (FAB)	
7.	Muhammad Ilyas	Ministry of Interior (MoI)	
8.	Zafar Mehboob		
9.	Dr Saeed ur Rehman	Pakistan Standards and Quality Control Authority (PSQCA)	
10.	Dr Muhammad Wasif Nisar		
11.	Abdul Ghaffar Niazi		
12.	Wahab Feroze	Ministry of Science and Technology (MoST)	
13.	Dr Shoukat Ali	Pakistan Software Export Board (PSEB)	
14.	Imran Nazir	National Information Technology Board (NITB)	
15.	Usman Ghani	Ministry of Industries Pakistan (MoIP)	
16.	Abid Hussain Kalwar		
17.	Ali Murtaza	State Bank of Pakistan (SBP)	
18.	Faisal Anwar	United Bank Limited (UBL)	
19.	Waqas Mehmood	Higher Education Commission (HEC)	
PSQCA APPROVING PANEL			
1.	Meritorious Prof Dr S.M. Aqil Burney	Chairman	Head of Actuarial Science and Risk Management (IOBM), UoK, Karachi, aqil.burney@iobm.edu.pk
2.	Muhammad Asif Riaz	V Chairman	ENSTA Tech Digital Array, Private Limited, Karachi,
PSQCA APPROVING PANEL MEMBERS			
1.	Dr Syed Irfan Nabi	Assistant Professor, Institute of Business Administration (IBA) , Karachi	
2.	Iqbal Ahmad Jamal	Chairman (ICT-TC1), PIBAS Pakistan, Pvt Limited	
3.	Ishfaque Ahmed Khanzada	Chairman (ICT-TC6), Head of ICT Infra & Network, University of Karachi	
4.	Asif Rafiq	Senior Lecturer, DHA Suffa University, Karachi	
5.	Tariq Umer	Chairman (ICT-TC3), Assistant Professor COMSATS University, Lahore	
6.	Dr Humera Tariq	Chairman (ICT-TC5), Associate Professor, University of Karachi	
7.	Rana Shahzad Qasir	Chairman (ICT-TC5), Cyber Crime, Federal Investigation Agency (FIA) Karachi	
8.	Muhammad Tayyab Chaudhry	Chairman (ICT-TC7), Assistant Professor, COMSATS University, Lahore	
9.	Dr Abdul Razzaque	Chairman (ICT-TC7) Associate Professor, MCS, NUST	
10.	Dr. Muhammad Akram Iftikhar	Chairman (ICT-TC-2) Assistant Professor, COMSATS University	
11.	Imran Nazir	Assistant Secretary, NTISB	
12.	Kamran Rasheed	Deputy Secretary, NTISB	
13.	Kashif Rahim	Director, NTISB	
14.	Muhammad Umair Tariq	Director Technical Development Centre, pkCERT, MoIT&T	
15.	Uroosa Kiran	Deputy Director, NTISB	
16.	Anjum Parveen	Deputy Director (IT & ICT), Secretary to the Committee NSC/TC , Standards Development Centre, PSQCA , Karachi	

Table - PSS Authors, Reviewing & Approving Panels

FOREWORD

1. This Pakistan Standard was adopted by the authority of the Board of Directors for Pakistan Standards and Quality Control Authority after approval by the Technical Committee for "Information technology - Information Security, Cyber Security and Privacy protection ICT-TC3" had been approved and endorsed by the IT & ICT National Standards Committee on 09-11-2021.
2. This Pakistan Standard is formulated based on information provided by varied sectors such as public, private, academia, industry and International Standards from NIST, ISO/ IEC and Common Criteria etc. Standard named it as "Pakistan Security Standard for Cryptographic & ITSec Devices- PSS Guide Book" and "Pakistan Security Standard for Cryptographic & ITSec Devices- ITSec Guide Book". As per technical committee it was deemed suitable to adopt it.
3. This Pakistan Standard is formulated based on information provided by varied sectors such as public, private, academia, industry and International Standards from NIST, ISO/ IEC and Common Criteria etc. "Pakistan Security Standard for Cryptographic & ITSec Devices" and its use hereby acknowledged with thanks.
4. This standard is subject to periodical review in order to keep pace with the development in industry. Any suggestions for improvement shall be recorded and placed before the revising committee in due course.
5. This standard is intended chiefly to cover the technical provisions relating to this standard and it does not include all the necessary provisions of a Contract.
6. Scheme Publication PSS-GB-CRYPTOSec and PSS-GB-ITSec provides insight into PSS and procedural guidelines for Vendors, Developers and Sponsors (VDS) on evaluation, development and validation of COMSEC products. It will also help standardize indigenous development of information security (INFOSEC) products, components, services and procedures in Pakistan in line with modern trends. Also, will prepare and facilitate understanding of responsibilities during design and development stages as well as before conduct of evaluation, during the evaluation process and subsequent formalities for culmination of evaluation process.

In the event of any questions concerning this publication or for further information, please consult NTISB at given address.	
Address:	Secretary National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, Pakistan
Telephone:	+92-051-9208054; FAX +92-051-9207930
Email	pss@cabinet.gov.pk; pss@ntisb.gov.pk

AMENDMENT RECORD

Amendments to this document will be published as and when required.

Date	Version	Details of Affected Sections

ABBREVIATIONS

AS	Assertion
AVL	Accredited and Validated Lab
BC	Block Cipher
CC	Common Criteria (for Information Technology Security Evaluation)
CE	Cryptographic Equipment
CEVaL	Cryptographic Evaluation & Validation Lab
CEP	Cryptographic Equipment and Cryptographic Primitives
COMSEC	Communication Security
CP	Cryptographic Primitives
EAAPP	Evaluation Application, Acceptance and Preparation Process
ECAC	Electronic Certification Accreditation Council
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESM	Evaluation Startup Meeting
ETL	EMI/ EMC/ Environmental Testing Laboratory
EVP	Evaluation and Validation Process
EWP	Evaluation Work Plan
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
INFOSEC	Information Security
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
IVR	Implementation Verification Requirements
LSM	Latin Square Matrix
NDA	Non-Disclosure Agreement
NTISB	National Telecommunication and Information Technology Security Board
NVLAP	National Voluntary Lab Accreditation Procedure (US FIPS NVLAP)
PNAC	Pakistan National Accreditation Council
PED	PSS Evaluation Documentation
PNDA	PSS Non-Disclosure Agreement
PSS	Pakistan Security Standard for Cryptographic & ITSec Devices
PSSIS	PSS Implementation Scheme
SDM	Scope Defining Meeting
SSER-DP	Security Strength Evaluation Report by NTISB-PSSIS to Developer
SSER-Int	Internal Security Strength Evaluation Report by EL
SSER-SP	Security Strength Evaluation Report by NTISB-PSSIS to Sponsor
VDS	Vendor/ Developer/ Sponsor
VWP	Validation Work Plan

REFERENCES

Following documents were studied prior drafting this document. Some of the contents or ideas have been taken from referred documents.

1. **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program (CMVP):** National Institute of Standards and Technology Communications Security Establishment, January 27, 2010

2. **UKSP 01:** UK IT Security Evaluation and Certification Scheme Description of the Scheme, Issue 6.3, December 2009

3. **UKSP 03:** UK IT Security Evaluation and Certification Scheme Sponsor's Guide, Issue 2.2, December 2009

4. **Publication #1: Organization, Management and Concept of Operations**, US Common Criteria Evaluation and Validation Scheme, Version 2.0, September 8, 2008

5. **CCEVS 05:** Common Criteria Evaluation and Validation Scheme Guidance To Sponsors, Issue 2.0, September 2008

For dated or edition-specified references, subsequent amendments (excluding errata) to, or revisions of, any of these publications do not apply. However, parties who are users of this procedure are encouraged to investigate possibility of applying most recent editions. For undated references or references whose editions are not specified, latest editions shall apply.

DOCUMENT ORGANIZATION AND SCOPE

This document gives an insight into PSS and describes in detail roles of Vendor, Developer and Sponsor (VDS) in evaluation process. It consists of 5x chapters with supporting annexures. ***Chapter 1*** describes evaluation, scope, composition, structure and security levels of PSS. ***Chapter 2*** describes roles of VDS and evaluation/ validation process. ***Chapter 3*** provides information related to Crypto & ITSec Equipment and Primitives (CEP) re-validation. ***Chapter 4*** provides guidance to developer/ vendor for preparing PSS Evaluation Documentation (PED), while ***Chapter 5*** provides guidelines to developer/ vendor for export of cryptographic and ITSec equipment.

Table of Contents

List of Figures

List of Table

Chapter 1
Introduction

1.1 Background

Ubiquitous use of Information Technology (IT) necessitates use of Information Security (INFOSEC) products for protection of underlying data and information before, during and after communication. For the purpose, Cryptographic and IT Security (ITSec) equipment employing cryptographic algorithms are key components and form backbone in overall security of information and communication systems. At the same time, confidence and assurance in use of such products is essential; especially when such products are used in sensitive communication systems. To establish such confidence, INFOSEC products are subjected to security strength evaluation where a communication, IT and cryptographic equipment is meticulously evaluated to find **the weakest link** in overall communication system which may lead to **information compromise**. INFOSEC equipment and algorithms are therefore evaluated according to a set of security, functional, technical, and performance requirements as per operational environment where such devices operate.

1.2 Contemporary International Models

Various countries have evolved INFOSEC evaluation strategies by putting in place stringent security assessment standards. US Federal Information Processing Standards **FIPS 140-2** for Cryptographic Modules and EU's **Common Criteria** (CC) for ITSec are two most widely referred standards worldwide for commercial Communication Security (COMSEC) products. These publicly available standards state general requirements for a product but separately specify requirements for cryptographic algorithms albeit referring to national standards. Certification/ evaluation of a product is compulsory prior procurement and use by any government or defense organization in these regions. Additionally, each country has developed some specific standards for COMSEC products for use in government and military domains that are not publicly available such as NATO STANAG and US MIL-STD standards.

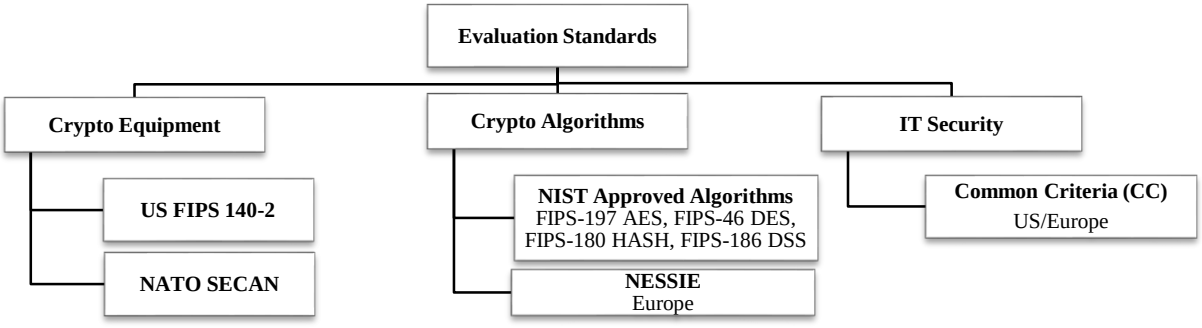

Figure 1.1: International COMSEC Evaluation Standards

1.3 TM-27 Evaluation Model

NTISB, Cabinet Division, being the **national regulator** for cryptographic and information technology affairs, conducts security evaluations to benchmark cryptographic strength, identify backdoors and grade security classification of COMSEC products. Previously, such evaluations were conducted through an arrangement of multi-campus evaluation facilities under Technical Memorandum – 27 (Procedure for Introduction of a New Crypto Machine and Speech Secrecy Equipment in Pakistan), which was promulgated in 1994. Besides being generic and outdated, TM-27 failed to provide standardized criteria for device evaluation as well as development guidelines for indigenous COMSEC developers. Consequently, COMSEC devices remained under evaluation for extended periods of time without final outcomes.

1.4 PSS Evaluation Model

To resolve complexities experienced in evaluations under TM-27, NTISB developed **Pakistan** **S**ecurity **S**tandard for Cryptographic & ITSec Equipment (PSS). PSS establishes baseline requirements that must be met for Cryptographic and ITSec Equipment (CE) as well as Cryptographic Primitives (CP i.e. algorithms, security protocols, security mechanisms and supporting systems) to be used in Pakistan. PSS not only lists **criteria for Evaluation Labs** (EL) to evaluate COMSEC products but also **defines benchmarks for indigenous developers** and vendors for designing their products as per distinct security requirements of local and foreign markets. Additionally, PSS defines administrative and technical requirements as well as guidelines for public and private sector technical labs that request NTISB for accreditation for conduct of COMSEC evaluations. Such **A**ccredited and **V**alidated **L**abs (AVL) will undertake COMSEC evaluations as per requirements and procedures stipulated in PSS. **N**ational **A**ccreditation **S**tandard for **C**rypto and ITSec **E**valuation **L**abs (NASCEL) is in line with ISO-17025 and US FIPS NVLAP procedures for COMSEC lab accreditation.

1.4.1 Principal Participants

Principal participants of PSS evaluation framework are as below:-

1) **NTISB**. The regulatory and governing body of Government of Pakistan to establish management and procedural framework for Cryptographic Equipment and Primitives (CEP) evaluations within Pakistan. Framework includes establishment of approved techniques, procedures and accreditation of labs for conduct of evaluations while maintaining confidentiality, integrity and impartiality of the process. NTISB Board provides top level direction, assigns tasks, setting and reviewing policies and monitoring overall INFOSEC landscape. Policies are set

following extensive interaction with organizations and stakeholders. Responsibility for NTISB working resides with Secretary NTISB with oversight provided by NTISB Executive Committee. Broadly, in the context of PSS, NTISB functions will include Product Certification and Lab Accreditation. TEC for product certification and ATC for lab accreditation are chaired by Chairman NTISB Board i.e. Secretary Cabinet Division with Secretary NTISB as convener. TEC is a technical committee responsible for governing overall evaluation and certification process. Whereas, ATC will spearhead accreditation of evaluation labs, in line with Pakistan National Accreditation Council (PNAC) being the apex Accreditation Body (AB) of Pakistan.

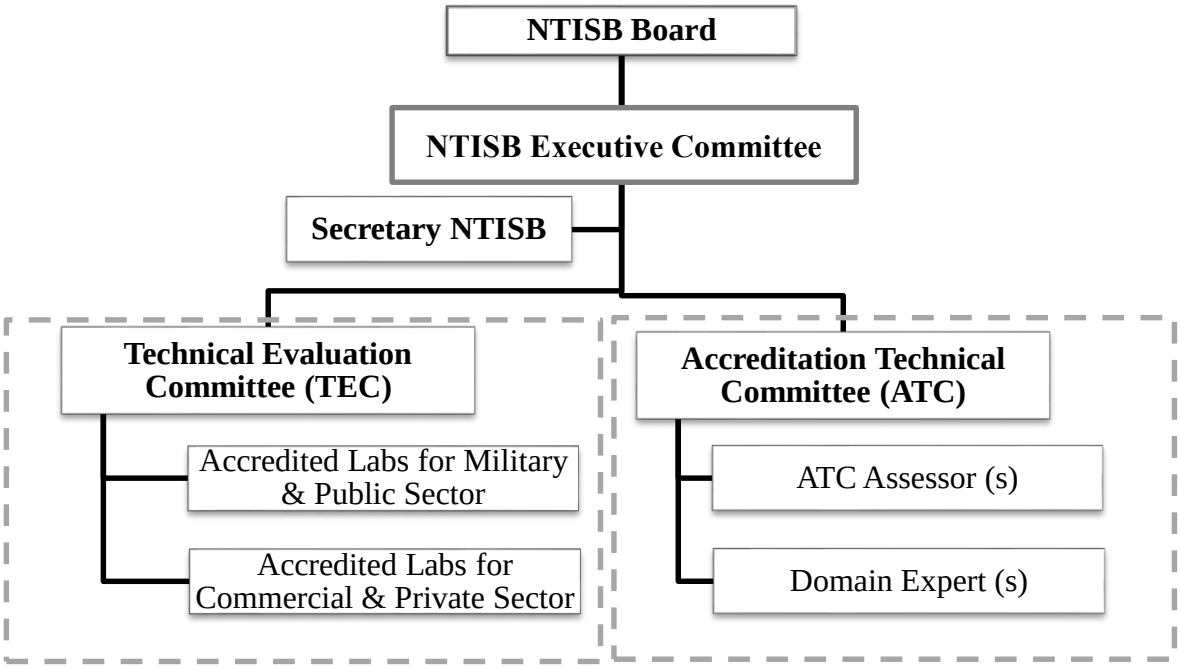

Figure 1.2: NTISB Structure

2) **Evaluation Labs (ELs)**
   a) **Cryptographic Evaluation and Validation Lab (CEVaL)**. Evaluation Lab(s) accredited by PNAC & NTISB under NASCEL accreditation standard for PSS compliant evaluations of CEPs. CEVaL is alternatively known as Accredited and Validated Lab i.e. AVL.
   b) **EMI/ EMC & Environmental Testing Lab (ETL)**. NTISB designated Environmental and EMI/ EMC Testing lab(s).
3) **Technical Evaluation Committee (TEC)**. An apex validation committee formed under NTISB for Product Certification validating all evaluations conducted by ELs. TEC comprises of nominated technical representatives from organizations who possess relevant academic qualifications with experience in information assurance related

aspects i.e. operation, development, evaluation etc. TEC is responsible for independently assessing/ validating evaluation report submitted by EL. Similar organization and functions are performed for Lab Accreditation once it comes to giving evaluation charter to ELs.

4) **Developer/ Vendor**. Developer is product designer of CEP. Developer or vendor requests NTISB to conduct security evaluation of CEP. Essentially, developer is responsible to provide equipment, documentation, training (if required) and any other technical support for successful conduct of evaluation within PSS stipulated timelines.
5) **Sponsor**. Sponsor is an organization or department requesting security evaluation of a CEP or a party that wishes to have an evaluated or certified product. Sponsor is essentially responsible to request NTISB for conduct of security evaluation of CEP under PSS prior its induction for use within organization. Developer directly approaching NTISB will also adopt necessary roles/ functions of Sponsor. Roles and responsibilities of Vendor, Developer and Sponsor (VDS) are common, interchangeable and therefore have been alternately defined in this document.

1.4.2 Evaluation and Validation Operational Flow

This section summarizes entire evaluation and validation cycle to assist reader in understanding PSS framework. Operational flow for evaluation, re-validation and certification is as below:-

1) VDS interested in evaluation of cryptographic/ ITSec equipment will formally apply to NTISB and provide device with necessary documentation as per PSS. To ensure **confidentiality**, a Non-Disclosure Agreement (NDA) will also be signed between NTISB/ EL. Single window operation will be ensured for:-
   a) Conduct of Crypto/ ITSec strength evaluation and certification by CEVaL.
   b) Conduct of EMI/ EMC and environmental testing of device by ETL.

Ser	Action	Responsible Entity & Timeline
1.	Submission of device & documentation as per PSS to NTISB/ EL	**VDS** Variable
2.	After NDA, detailed COMSEC/ ITSec evaluation as per PSS	**EL** 24x Weeks
3.	Presentation of Evaluation Reports to TEC	
	• If device not cleared, VDS has right to appeal to TEC	**VDS** Within 4x Weeks
	• If appeal accepted by TEC (within 8x weeks), 20-40% tests to be re-conducted	**EL** Within 8x Weeks
	• Re-presentation of case to TEC along with results	**EL** Within 1x Week
4.	NTISB to issue acceptance certificate or otherwise	**NTISB** Within 3x Weeks

Table 1.1: Evaluation, Validation and Appeal Operational Flow

2) EL will prepare evaluation report for certification covering all aspects of CEP along with EMI/ EMC and environmental testing reports (if applicable). To ensure **integrity**, tests so conducted will be reproducible.
3) Both reports will be presented to TEC by EL within **24x week** timeframe after a formal request of TEC meeting by NTISB.
4) In case device is not cleared by NTISB (partially or fully), VDS will have right to challenge evaluation reports through an appeal to NTISB, which in turn will intimate TEC regarding VDS appeal.
5) If appeal is accepted by TEC, EL will conduct verification of evaluation results. TEC will select upto a maximum of **20 - 40% tests** (numerically, however, remaining within overall complexity/ scope of tests selected) to be re-conducted within **4x weeks**, thus providing **impartiality** & **reproducibility**.
6) EL will again present case to TEC within **1x week** of conduct of tests. Consequently, NTISB will be obliged to issue certification or otherwise within **3x weeks**.
7) Revalidation of a device under all circumstances i.e. in case of algorithm change, design modifications, expiry of certification time or randomly (i.e. after certification/ induction of a system) will be governed as per PSS.

Note: Above mentioned time is in working days.

1.5 PSS Scope

Security Evaluation of COMSEC equipment in PSS deals with crypto security, emission security (EMSEC) and physical security of Cryptographic Primitives (CP), Cryptographic & ITSec equipment (CE) and supporting systems/ devices (collectively referred to as Cryptographic Equipment and Primitives, CEP). Traffic Flow and Transmission Security are operational security aspects of COMSEC equipment and shall be covered in future versions of PSS.

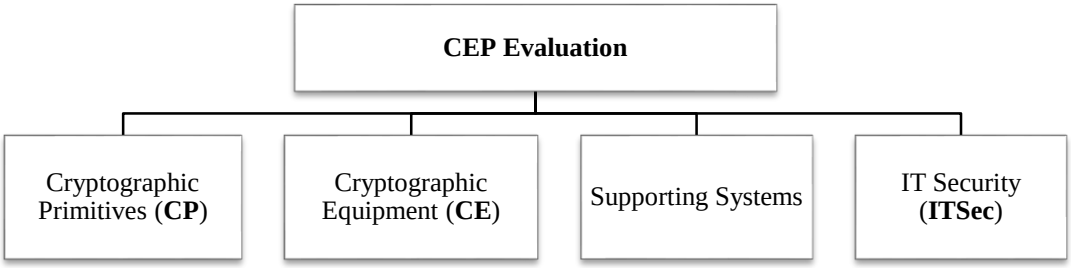

Figure 1.3: PSS Evaluation Scope

1.5.1 Cryptographic Primitives

There are a number of basic cryptographic building blocks i.e. primitives used for providing information security. Examples of primitives include Encryption Schemes, Hash Functions, Random Number Generators, Message Authentication Codes, Identification Schemes and Digital Signature Schemes, Security Protocols, Security Mechanisms, etc. ***Annex A*** provides a schematic listing of the stated primitives and their relationship.

1.5.1.1 Cryptographic Algorithms

Cryptographic algorithms can be broadly classified into six categories, depending on their type, application and functionality e.g. Block Ciphers, Stream Ciphers, Public-Key Based Algorithms, Hash Functions, Digital Signature Algorithms (DSA), Random Number Generators (RNG) etc. With standardization of Post Quantum Algorithms (PQA), such algorithms will be incorporated in next update of PSS.

1.5.1.2 Security Protocols

Security protocols also known as cryptographic protocols are communication protocols designed to provide security assurance using cryptographic algorithms. Security protocols provide information security such as Confidentiality, Integrity, Authentication and Nonrepudiation in an insecure network. Security protocols may be built by using different cryptographic algorithms such as Encryption Schemes, Digital Signatures, Hash Functions and RNGs. Key Exchange Protocols, Key Distribution Protocols and Network Security Protocols etc. are few such examples.

1.5.1.3 Security Mechanisms

An algorithm or mechanism that contributes towards COMSEC without employing a cryptographic algorithm falls under category of security mechanisms. For example hopping algorithms that are used to randomize frequency hopping in radios is an example of a security mechanism.

1.5.2 Cryptographic Equipment (CE)

Set of hardware, software, firmware or combination thereof, that implements cryptographic logic or processes (including cryptographic algorithms and key generation) by operating in peculiar communication environments e.g. wireless, wired, IP, link, standalone etc. are known as cryptographic equipment. CE evaluation covers broad aspects related to design and implementation of cryptographic module including specifications, ports and interfaces, roles, services and authentication, physical security, operational environment, key management, EMI/ EMC, self-tests, design assurance and mitigation of other attacks.

Annex A entails major categories of CE based on communication medium and associated supporting systems. NTISB will also formulate a mechanism under which sample based testing of deployed equipment (from the vendor delivered lot) may also be undertaken.

1.5.2.1 Supporting Systems

CE usually requires supporting devices to provide secure management of cryptographic keys and/ or critical security parameters, centralized network management in which CE operates or for user authentication, etc. Examples of supporting systems/ devices include Key Management Systems (KMS), Simple Network Management Center (SNMC), Smart Cards, secure storage, etc.

1.5.3 ITSec

In present day IT dependence, ITSec evaluation has gained paramount importance in public and private sectors. Important e-government functions, citizen services, financial services, Critical Information Infrastructure (CII) and Critical National Infrastructure (CNI) etc. have become accessible publicly. With the access comes susceptibility to hacking, intrusion, denial of service, data and intellectual property theft etc. and hence the requirement of ITSec evaluation, infrastructure auditing and just in time screening. ITSec evaluation in PSS follows best practices of NIST, ISO-27k, COBIT,OWASP etc. and renowned international standards such as Common Criteria for testing ITSec equipment including Firewalls, Intrusion Detection/ Prevention Systems (IDS/ IPS), access control devices, Unified Threat Management (UTM), routers and switches etc; as shown in ***Annex A***.

1.6 PSS Composition

Broadly, PSS can be divided into 2x main categories i.e. **PSS Implementation Scheme** with 4x documents (2x Public Domain Documents and 2x Restricted Release Documents) and **Security Standard** with 10x documents. General Requirements (GR) define technical, operational, cryptographic requirements with Derived Test Requirement (DTR) documents further elaborating evaluation test requirements and facilitates understanding of VDS in enabling AVL to perform required testing and evaluation.

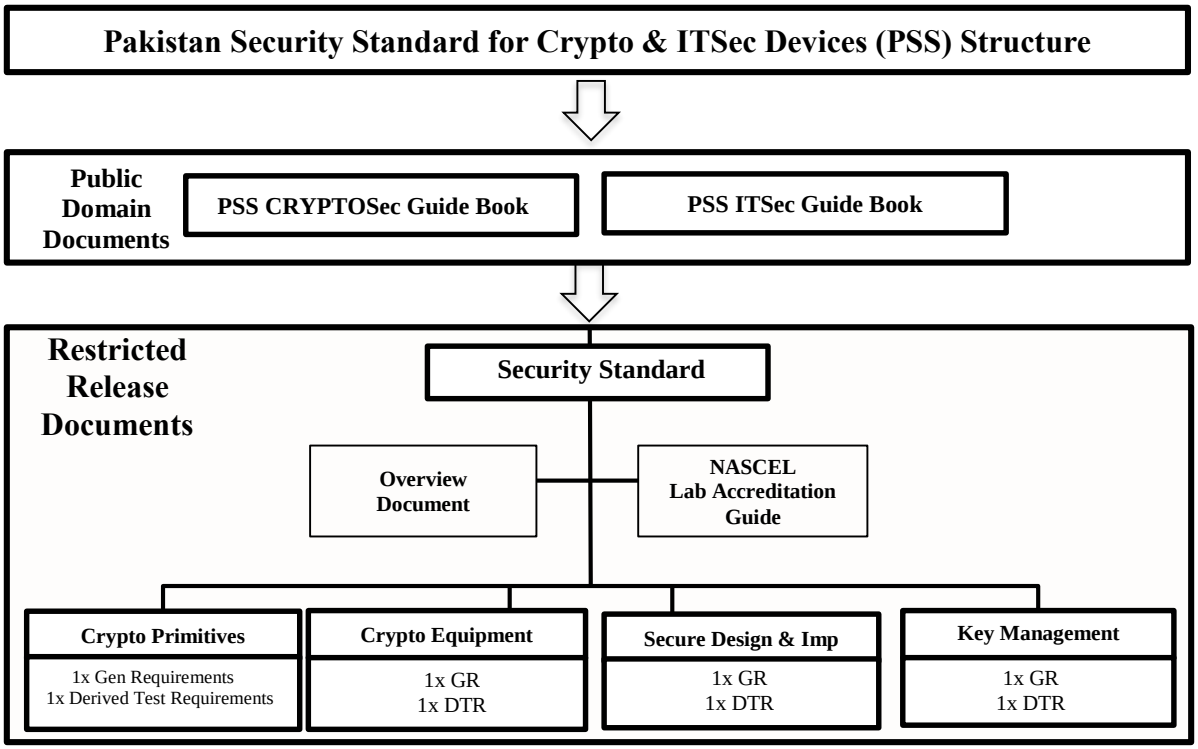

Figure 1.4: PSS Composition

1.6.1 PSS Implementation Scheme (PSSIS)

PSSIS is the framework designed for stipulating procedures, methodologies and functions of NTISB, ELs, VDS and lab accreditation mechanism. This framework consist of following:-

1) **PSS Cryptographic and ITSec GuideBooks** provide an extensive insight into functions, roles, processes and methodologies established for evaluation of COMSEC and ITSec equipment, algorithms, protocols, services etc. The guide books will be for public release and used as reference when furnishing technical documentation for security evaluation or when designing and developing such security solutions. Due to their diverse nature, ITSec equipment evaluation cannot be confined to a controlled standard. Accordingly, instead of restricting procedures into a single DTR document, ITSec evaluation shall follow best practices and international standards till such time that National Certification Scheme on the lines of Common Criteria Recognition Agreement (CCRA) is developed.
2) **PSSIS-NASCEL** National Accreditation Standard for Crypto & ITSec Evaluation Labs Guide Book is a restricted release document and defines mechanism, requirements and set of procedures for establishing and accrediting evaluation labs. Final accreditation will be granted by Pakistan National Accreditation Council (PNAC) following a successful completion of accreditation process which includes submission of an application, an on-site assessment by PNAC certified assessors,

resolution of any non-conformity identified during on-site assessment, participation in proficiency testing and technical evaluation. This accreditation is only restricted and limited to government/ semi-government/ private organizations within Pakistan that carryout security strength evaluations.

1.6.2 Security Standard

Security Standard is restricted release which will be provided to VDS upon request depending upon type, configuration and operational environment of CEP:-

1) **Cryptographic Primitives Standard** sets forth requirements to evaluate crypto algorithms, protocols, formal verifications and security mechanisms.
2) **Cryptographic Equipment Standard** stipulates requirements to evaluate crypto equipment and its performance and functional testing.
3) **Secure Design and Implementation Standard** defines secure design and implementation techniques, guidelines and mechanisms.
4) **Key Management System Standard** defines criteria for key management life cycle.

1.7 PSS Security Levels

The standard provides **four increasing levels** of security for Cryptographic and ITSec Equipment i.e. Level 1, Level 2, Level 3 and Level 4; **three security grading in increasing order** for CP i.e. A, B and C. These levels are intended to cover wide range of potential applications, devices and environments. Evaluation/ Validation of a CEP as per security level is applicable when device is configured and operated in accordance with the level to which it was tested and validated. Elaborate definition of grading and security levels is as per ***Annex G***.

CEP Security Levels		**Security Levels/ Grading Criteria**				
		CE	**CP**	**KMS**	**SDI**	**NMC (CP)**
Low	Security Level - 1	1	A	1	1	A
Basic	Security Level - 2	2	B	2	2	
Medium	Security Level - 3	3	C	3	3	B
High	Security Level - 4	4		4	4	

Table 1.2: Overall Security Levels in PSS

1.8 Compliance and Certification Roadmap

PSS provides assurance of cryptographic security claims on any product or service containing cryptography. In order to streamline alignment of desired cryptographic security in an earliest possible timeframe, there is a need to introduce a scheduled PSS implementation plan that can facilitate critical sectors, organizations and end users to align their existing as well as future cryptographic and ITSec infrastructure. Timelines for PSS compliance (i.e. conformance to

PSS) and PSS certification (i.e. detailed evaluation as per PSS) of products and services are as per PSS Gazette Notification (***Annex H***). The roadmap is also applicable to end users consuming PKI based cryptographic services accredited by Electronic Certification Accreditation Council (ECAC). ECAC grants or renew accreditation to PKI service providers, their services and security procedure. For the purpose, NTISB will facilitate in cryptographic strength evaluation of offered PKI services by Certification Service Providers. Based upon the NTISB provided report, ECAC will issue accreditation certificate according to its applicable regulations/ procedures.

Chapter 2

Roles of Vendor/ Developer/ Sponsor & EL

2.1 Introduction

VDS is main entity which interacts with NTISB and initiates requirement for an evaluation. Once a developer or sponsoring organization decides to induct a CEP, it shall intimate NTISB about its intent. This will be followed by series of processes with details explained in coming sections. Relationship of sponsor to CEP may vary depending on nature of product or profile and circumstances surrounding evaluation. Developer/ vendor can considerably facilitate evaluation by giving early consideration to factors that can affect costs, timescales and efficient management of an evaluation. A typical case scenario is depicted below.

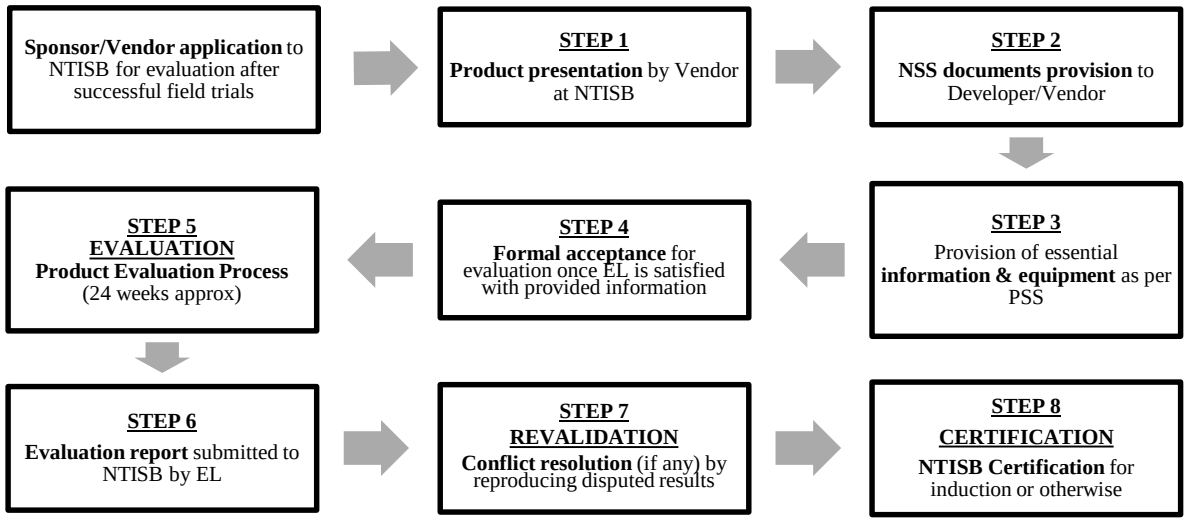

Figure 2.1: Evaluation Case Scenario

During complete evaluation process, sponsor has to work in synch with developer. Regardless of whether or not sponsor is developer, EL must be provided with technical materials and essential deliverables needed to conduct security evaluation in a consistent manner. Provision of documentation, material, assistance etc. and **financial bindings** for ensuring successful conduct of evaluation will be covered through **contractual bindings** and **agreements**.

2.2 Scope of Evaluation

NASCEL Accredited Evaluation Lab(s) is required to perform evaluation of Crypto Equipment, Primitives and Key Management System in full scope according to requirements of PSS. Aim of these evaluations will be to find the weakest link in the complete system which will lead to a compromise in security of the CE. Additionally, avenues of intentionally or unintentionally left development stage vulnerabilities, cryptographic implementation

anomalies, any kind of backdoors, software trojans, software logic bombs, software or hardware bugs etc. will also be explored. Such threats enable adversaries to bypass INFOSEC infrastructure and gain access to classified and critical information. The security evaluation of an INFOSEC product includes analysis and testing of the product for conformance to a set of functional, operational and security requirements laid out as per the role and profile of the product defined by the user.

2.3 Conduct of Evaluation

Evaluation can only be considered independent and impartial if it is possible to demonstrate that neither EL, nor any individual EL staff concerned with a particular evaluation, has any **conflict of interest** in outcome of evaluation. Work performed by evaluators must be independent of development of Target of Evaluation (TOE). During lab accreditation process, Accreditation Body will ensure that EL management has undertaken sufficient safe guards to demonstrate that Evaluators are free from any commercial, financial and other pressures which might influence their technical judgment. EL may not perform evaluation on CEP for which the EL has:-

1) Designed any part of the CEP.
2) Developed original documentation for any part of the CEP.
3) Built, coded or implemented any part of the CEP, or
4) has any ownership or vested interest in the CEP.

2.4 Evaluation Process

PSS splits evaluation cycle in two processes i.e. ***EAAPP*** and ***EVP***; each having distinct phases/ stages. Narrowing down focus here, role of VDS for each stage of evaluation and validation of CEP as per PSS is given in succeeding paras.

2.5 Evaluation Application, Acceptance & Preparation Process

EAAPP spans out from letter of intent from sponsor to formal acceptance of the CEP for further process of evaluation and validation. EAAPP is further split into three phases/ stages i.e. Evaluation Application Phase, Acceptance Phase and Preparation Phase, each having a critical role of sponsor for smooth progression of evaluation and validation from EAAPP to EVP.

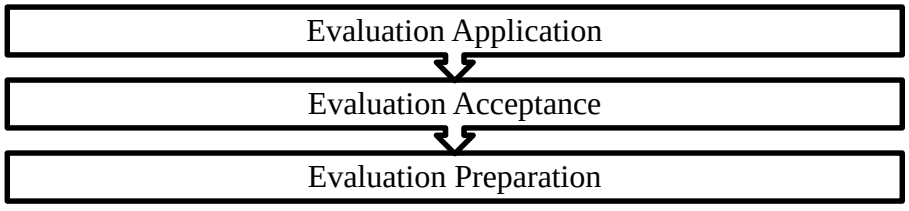

Figure 2.2: EAAPP Phases

2.5.1 Evaluation Application Phase

Evaluation Application Phase incorporates steps needed to be performed by sponsor to initiate an evaluation. It also provides reference timeline after signing the contract. Prior to **"*Evaluation Application*"**, activities are not time lined and depend upon priorities set by sponsor.

Before initiating letter of intent to NTISB, sponsor is advised to keep in focus following contractual considerations:-

1) Sponsor must ensure that CEP earmarked for procurement or induction has been fully developed and during evaluation process, is not under any modification, up-gradation or concurrent development.
2) Sponsor must ensure that if CEP earmarked for procurement or induction falls in any category of re-validation process as discussed in ***Chapter 3*** of this document, specified actions concerning developer/ vendor shall be ensured.
3) If a CEP in full or any component has been evaluated and certified by any international evaluation and validation/ certification scheme, then sponsor is responsible for delivery of possible deliverables, including evaluation results for validated components of CEP.
4) Sponsor has option of engaging a security consultant, ***who cannot be from EL***, to assist with preparations for evaluation under paradigm of PSS. However scope of consultancy work during preparation for evaluation & validation is not controlled by NTISB and is a matter of negotiation between sponsor and consultant.
5) Sponsor should establish separate contracts with developer/ vendor to ensure that he/ she accepts and understands responsibilities to support evaluation process.
6) Sponsor must ensure that there is adequate contractual cover for resolution of issues and observations.
7) Sponsor must ensure to secure all legal rights of CEP and indemnify NTISB and EL.
8) Sponsor must ensure that queries/ questions and responses to EL will only be routed to NTISB through official correspondence in writing.
9) Sponsor must maintain checklist for each stage of process as mentioned in ***Annex B*** which shall be forwarded to NTISB after completion of EAAPP.
10) Sponsor must make clarity on payment of evaluation expenditures to NTISB for which developer/ vendor is liable as per PSS.
11) Reply to queries/ questions and responses to EL will only be routed through sponsor.

2.5.1.1 Letter of Intent

Once sponsor decides to induct or procure any CEP and final approval has been sought by respective competent authority, sponsor is required to inform in writing to NTISB about its intent mentioning type of CEP required. In letter of Intent (***Annex F***), sponsor must commit in writing to fulfill sponsor's role during complete cycle of evaluation along with inclusion of following details:-

1) Names of CEP(s)
2) Family of products it belongs to
3) Products' brochures
4) Requirements/ purpose of induction/ procurement
5) List of competitive products under consideration (without any details)
6) Procurement timelines
7) Targeted time of commissioning CEP after evaluation and validation

2.5.1.2 Operational Trials and Selection of CEP

Sponsor will conduct operational trials of shortlisted CEPs which are under consideration/ competition by various companies. During trials sponsor shall ensure that CEP will be selected after rigorous testing. The duration of this activity is variable and depends upon priorities set by sponsor. Sponsor will do following in this regard:-

1) Define scope of operational trials as per his requirements. In general, it must be ensured that equipment shall perform in all targeted operational environments/ platforms.
2) Shortlist the best available CEP based on operational performance.
3) Forward a certificate to NTISB, mentioning conduct of successful trials of CEP in operational environments.
4) Forward brochure of selected CEP to NTISB along with confirmation that CEP is mature and is not still under development.

2.5.1.3 Scope Defining Meeting (SDM) and Provision of Documents

Letter of Intent supplemented by selection of CEP (after its successful operational trials by sponsor) is followed by SDM. It is a joint meeting/ discussion arranged by NTISB in which reps from NTISB, EL and sponsor participate. Developer/ vendor is NOT invited for SDM. SDM may take 2~3 days for its completion but complete activity shall preferably be completed within 2 weeks after intimation to NTISB by sponsor for selected CEP. Sponsor will deliver a presentation encompassing following:-

1) Requirement of his organization/ setup

2) List of products considered, mentioning vendors/ developers against each
3) Justification of selected CEP
4) Vendor's/ developer's profile
5) Brief technical and cryptographic specifications of selected CEP
6) Procurement timelines
7) Targeted time of commissioning CEP after evaluation and validation
8) Targeted level of security depending on requirements of organization/ setup
9) Contractual details with developer/ vendor
10) Possibility of using previous evaluation results of component(s) of CEP
11) Sponsor shall get latest copies of following restricted domain documents from NTISB after signing NDA:-
    a) Overview Document
    b) Applicable documents of Security Standard

2.5.1.4 Agreements for Provision of PSS Evaluation Documents (PED) & Equipment

Vendor/ developer will sign PSS Non-Disclosure Agreement (NDA) with Sponsor and NTISB/ EL. After signing NDA, sponsor shall provide latest copies of following documents obtained from NTISB to vendor/ developer, and official handing taking over document shall be signed by both parties. Following are document listing:-

1) PSS (Public domain) documents
    a) Overview Document
    b) Applicable documents of Security Standard

Vendor/ developer shall keep following points in consideration while handling above mentioned documents:-

1) These documents can be obtained by vendor/ developer only under a PSS Non-Disclosure Agreement (NDA) with Sponsor and NTISB.
2) Vendor/ developer shall ensure that these documents are handled with utmost care.
3) Loss of any document will involve legal obligations for all involved parties.
4) Sufficient safeguards will be assured for shared intellectual property specific to cryptographic domain by NTISB, Sponsor and EL.
5) In addition to above, vendor/ developer must ensure that no part of PSS is copied, reproduced or modified, and shall give a written assurance in this regard.

In addition to above considerations vendor/ developer shall agree for provision of proprietary information.

2.5.1.5 Provision of Written Agreement from Vendor for Provision of PED

After studying PSS and PSSIS documents, sponsor shall get written consent in the form of a contract (3x copies) from developer/ vendor for provision of PED (including proprietary information under NDA) as per PSS. In contract, sponsor is responsible to include following clauses:-

1) Developer/ vendor agrees to provide PSS evaluation information including proprietary information and evaluation equipment after signing NDA. Failure in provision will be liable to cancellation of contract without any prior notice at any time.
2) CEP will be inducted only after successful completion of evaluation and issuance of certificate by NTISB.
3) Developer/ vendor agrees not to publish or disseminate information given in PSS and PSSIS without prior approval by NTISB.

This activity may preferably be completed within 2 weeks after provision of PSS & PSSIS documentation to sponsor.

2.5.1.6 Contract Signing

Developer/ vendor shall provide PED in accordance with PSS and PSSIS. Contract shall then be signed between developer/ vendor and sponsor. In contract, vendor/ developer shall agree to following clauses:-

1) Developer/ vendor shall provide PED including proprietary information and evaluation equipment.
2) Developer/ vendor shall not publish or disseminate information given in PSS under any circumstances.
3) All evaluation expenditure shall be paid by developer/ vendor.

It is important to remember that, failure of provision of any information or payment will be liable to cancellation of evaluation without any prior notice at any time.

2.5.1.7 Preparation for PSS Evaluation Documentation

After thorough review and understanding scope of PSS and PSSIS documents, sponsor shall hold sessions with developer/ vendor for following:-

1) To set targets for meeting requirements of evaluation and validation as per PSSIS.
2) To define time lines for preparation of required documentation supplemented by review meetings. Sponsor must notify developer/ vendor to prepare PED preferably within 1 ~ 2 months after contract signing.

3) Plan to carry out a final review of documentation prepared by developer/ vendor before handing them over to NTISB and EL. Review must be carried out in line to requirements of PED given in ***Chapter 5***.

2.5.1.8 Signing of Non-Disclosure Agreement (NDA)

After completion of PED, sponsor shall also arrange signing of NDA for proprietary information. Following must be ensured in this regard:-

1) NDA is to be signed by NTISB, VDS and EL.
2) NDA warrants a commitment by all parties to keep proprietary information secret provided by developer/ vendor for evaluation.
3) No part of provided proprietary information will be published or disseminated in any scenario to any party.
4) All provided proprietary information will be returned or destroyed upon completion of evaluation.

2.5.1.9 Evaluation Application by Sponsor

As soon as PED is complete, sponsor will formally request NTISB to undertake evaluation of CEP. Reference time of complete evaluation cycle starts from here. Sponsor shall do following in this regard:-

1) Send application to NTISB within 10 days of signing contract with vendor/ developer.
2) Attach 1x set of contract signed with developer/ vendor in original, or at least pages/ clauses related to evaluation.

2.5.1.10 Payment of Evaluation Expenditures

As per PSS, VDS will be required to make payment to NTISB at this stage of evaluation process. The amount of evaluation fee will depend upon type of equipment and scope of evaluation and will be decided by NTISB. Refer to ***Annex E*** for **latest payment details**. Sponsor must ensure following in this regard:-

1) Clarify from NTISB on current policy for:-
    a) Amount of evaluation expenditures
    b) Mode of payment
2) Payment of evaluation expenditures in vogue must be included in initial contractual deal with developer/ vendor. Coordinate with developer/ vendor for payments to be made within 2 weeks after preparation of PED.
3) Intimate NTISB about payments made by developer/ vendor.

Sponsor must review portion of checklist attached as ***Annex B*** of this document for this phase and ensure its completion. Signing of NDA (***Annex C***) culminates evaluation application phase and moves EAAPP processing to Acceptance Phase.

2.5.2 Acceptance Phase

Acceptance phase includes steps such as provision of PED to NTISB and analysis of its completeness, request for additional information required from vendor and subsequent submission of that information. Evaluation Startup Meeting (ESM), one of most critical activities of evaluation and validation cycle, also falls in this phase.

2.5.2.1 Requirements for Provision of PSS Evaluation Documentation (PED)

A CEP can only be evaluated, if requisite information in all areas of PSS is provided by VDS. Developer/ vendor is responsible for preparing required PED in consultation with sponsor, but may seek advice from NTISB as and when needed. The details on PED required to be provided by developer/ vendor is given in ***Chapter 4*** of this document. Sponsor must ensure that PED essentially include following:-

1) Vendor claims.
2) Operational and technical design details of CEP as defined in PSS.
3) Operational and design details of CEP algorithms protocols and Key Management System as defined in PSS along with their cryptographic strength proofs.
4) EMC/ EMI (***MIL-STD-461E***) compliance certificate from recognized and authorized lab on EMC/ EMI testing, if applicable.
5) Environmental (MIL-STD-810F) certification from any recognized and authorized lab on environmental testing, if applicable.
6) Details on implementation verification setup.
7) Data of Known Answer Tests (KAT).

2.5.2.2 Preparation and Submission of Missing Information

Since acceptance decision of CEP by NTISB is conditional to developer/ vendor's response on provision of additional deliverables/ missing information, EL will undertake documentary evaluation to prepare details of missing information. Consequently a questionnaire will be forwarded to developer/ vendor through NTISB. Sponsor will:-

1) hand-over copy of questionnaire received from NTISB to developer/ vendor;
2) plan a schedule of necessary sessions for discussion with developer/ vendor and security consultant on questionnaire and additional requirements;
3) observations/ queries, if any, will be clarified from NTISB on priority;

4) obtain a written consent from developer/ vendor for provision of required information and equipment for evaluation and forward same to NTISB;
5) finalize response from developer/ vendor and forward response documentation to NTISB;
6) submit missing information/ additional deliverables to NTISB;
7) intimate NTISB about delay (if any) along with reasons of delay(s);
8) agree to take further assistance from developer/ vendor for future requirement(s).

2.5.2.3 Agreement by Vendor for Additional Information & Equipment

Vendor/ developer shall agree to provide all type of assistance/ support to NTISB/ EL through sponsor which will help in a successful evaluation process. Vendor/ developer shall:-

1) Agree to fully support evaluation process.
2) Provide any additional information required by NTISB/ EL/ Sponsor.
3) Deliver any additional presentation/ information when required during evaluation process.
4) Provide any additional equipment demanded by sponsor/ EL which helps in evaluation.
5) Reply to all questionnaires/ queries raised by EL.

2.5.2.4 Evaluation Start up Meeting (ESM)

Aim of ESM is to agree upon suitability of the proposed equipment for evaluation, and to discuss evaluation and validation process for said equipment. It involves reps from VDS, EL, NTISB and any other interested parties as considered. Since developer/ vendor has to deliver a presentation on CEP's Scope Information in meeting, sponsor must ensure that following is covered in presentation by developer/ vendor:-

1) Vendor's brief profile.
2) CEP details.
3) Whether CEP is a complete product/ equipment or part of equipment. In case CEP is not a complete product, CEP scope and boundary must be clearly defined, i.e. which parts are included in evaluation and validation.
4) Details and design of cryptographic primitives (algorithms, security mechanisms and protocols being used in CE).
5) Product's decomposition into major components or subsystems.
6) CEP Architecture.
7) Security Architecture (including required Hardware, Firmware and Software).

8) Security Functionality.
9) How CEP interfaces to its environment, including relevant standards and protocols.
10) Operational use including modes of operation.
11) Target security level or security level claim.
12) Claimed platforms.
13) Evaluated components and any re-use of previously obtained results.
14) Implementation verification setup.
15) Development status and timescales.
16) Additional Security claims.
17) Evaluation Expenditures.

Observation(s), if any, must be discussed by Sponsor at ESM. At this stage, acceptance phase of EAAPP will finish, moving EAAPP process to Preparation Phase. Sponsor must review portion of checklist, attached as ***Annex B***, for this phase and ensure all actions as required for its completion.

2.5.3 Preparation Phase

Preparation phase involves active participation by EL and developer/ vendor. Sponsor plays a passive and supportive role in this phase. Major activities of preparation phase pertaining to sponsor are discussed in following sub-sections.

2.5.3.1 Training by Vendor

Within two weeks, after acceptance by NTISB, developer/ vendor is required to give training of CEP to evaluators/ validators. Sponsor must ensure following in this regard:-

1) Get the list of individuals planned to attend the training from NTISB.
2) Finalize training schedule with developer/ vendor.
3) Finalize training syllabi with developer/ vendor.
4) Intimate NTISB in writing (with info copy to developer/ vendor) about :-
    a) Venue of training to be conducted.
    b) Detailed schedule of training.
    c) Training scope and contents to be covered.

During training, developer/ vendor shall:-

1) Conduct a detailed training covering all necessary aspects.
2) Address points and issues raised by sponsor/ NTISB/ EL at various occasions during interaction.
3) Be well prepared to answer any queries/ points raised by participants.

4) Formally intimate sponsor for training completion at end of training session(s). On completion of training, sponsor must intimate NTISB in writing about:-
    a) The conduct of training.
    b) During conduct of training if trainees have asked for additional requirements to be provided by developer/ vendor.
    c) Equipment handing/ taking over between developer/ vendor and EL reps.

2.5.3.2 Evaluation Equipment Handing/ Taking Over

Training of EL's evaluators and NTISB validators will finish with equipment handing /taking over. Following can be provided by VDS to support equipment:-

1) Items of hardware, firmware or software which constitute CEP itself
2) Supporting equipment documentation
3) Guidance documentation
4) Technical support

Sponsor must ensure following:-

1) EL and developer/ vendor agree on full set of deliverables that will be required for evaluation.
2) Supply of all evaluation deliverables at this stage.
3) 3x copies of proper documentation for equipment handing/ taking over (1x copy must be forwarded to NTISB).
4) Operational check of all deliverables shall be performed by EL prior to acceptance of evaluation equipment.
5) Intimate NTISB for additional deliverables and requirements, pointed out by EL's evaluators and validators during training, if applicable.
6) Unless specifically agreed otherwise, sponsor shall be responsible for all deliverables even after equipment handed over to EL.
7) EL may require VDS to sign a disclaimer to effect that EL will not be held liable if any damage occurs during testing of equipment under evaluation. Such damage might, for example, involve physical, data, programs, source files and configuration parameters.

Evaluation of CEP will be formally accepted by NTISB conditional to following:-

1) Successful handing taking over of CEP.
2) Fulfillment of additional requirements/ deliverables identified during training.
3) Provision of questionnaire response by developer/ vendor.

NTISB will intimate in writing to all concerned (EL, sponsor, developer/ vendor, etc.) that CEP will be evaluated in principle.

2.6 Evaluation and Validation Process (EVP)

Objective of evaluation and validation process is to determine required security level and to find out whether cryptographic equipment meets PSS security requirements. It involves the following activities:-

1) Evaluation of cryptographic equipment, including analysis and testing.
2) Evaluation of cryptographic primitives, including analysis, testing and cryptanalysis.
3) Interaction between parties involved, to ensure effective co-operation between evaluation processes.

All activities of this phase are related to NTISB and EL. Developer/ vendor is only involved in last two phases of EVP. If required, 2x Crypto/ Info Sec qualified officers from sponsor may be attached with concerned EL. On completion of evaluation and validation of CEP by EL, sponsor will receive an evaluation report (SSER-SP) from NTISB. In case of developer/ vendor, (SSER-DP) evaluation report will be shared.

Figure 2.3: EVP Phases

2.6.1 Security Strength Evaluation Report for (SSER-SP)/ (SSER-DP)

This report is prepared with a view point to highlight weaknesses of the system for further improvements by developer/ vendor or to give a glimpse to sponsor about security offered by device. Accompanying SSER-SP/ DP, a Certificate will also be issued by NTISB to Sponsor. Regarding SSER-SP/ DP and certificate, Sponsor must remember that:-

1) SSER-SP/ DP and Certificates are NTISB Copyrights. Reproduction and distribution of their contents is not authorized.
2) Sponsor shall not share SSER-SP with developer/ vendor.
3) Portion(s) of report, necessary for improvement in CEP component(s), shall ONLY be discussed with developer/ vendor (SSER-DP).
4) If evaluation request is by developer/ vendor, a detailed SSER-DP will be shared.
5) Observation(s), if any, will be communicated to NTISB in writing.
6) Appeal to evaluation results, if any, may be communicated to NTISB in writing within four weeks of certificate issuance.
7) SSER-SP/ DP and Certificate by NTISB on CEP evaluation and validation will dictate process of contractual funds release and induction of equipment by Sponsor.

2.6.2 Validation Phase (VP)

This phase involves activities related to reports validation by NTISB, appeals process, data record/ configuration management by NTISB, certificate and report issuance to sponsor.

2.6.2.1 Appeal to Evaluation Results

Vendors/ developers affected by NTISB decisions and actions have right to file a formal complaint and appeal decision when they believe that NTISB actions have not been conducted according to PSSIS rules, procedures or PSS, or actions have resulted in unfair treatment of persons participating in or who are affected by NTISB. Any dispute concerning operation of CEP evaluations may be referred to NTISB by any party, i.e. EL, Sponsor, Developer/ Vendor. Appeals concerning evaluation shall be forwarded to NTISB in written within 1 month of report submission. The procedure for submitting inquiry and dealing with is discussed below:-

1) An Official Request must be submitted to NTISB in writing with signature of initiator. If requestor represents an organization, official request must be on the organization's letterhead.
2) Assertions must be objective and not subjective.
3) CEP must be identified by reference or certificate number and specific technical details must be identified. Request must be nonproprietary and must not prevent further distribution by NTISB.
4) Secretary NTISB is responsible to resolve matter as per ***normal procedure*** discussed below or refer case to ***TEC***.

Normal procedure for handling appeals is as below:-

1) NTISB will share official request with EL.
2) EL shall determine merits of inquiry.
3) Once EL has completed its review, it will provide to NTISB a response with rationale on technical validity regarding merits of official request. EL will state its position whether its review of official request regarding CEP:-
    a) Is without merit and evaluation of CEP unchanged?
    b) Has merit and evaluation of CEP affected? EL will further state its recommendations regarding impact to evaluation.
4) NTISB will review EL rationale supporting its conclusion and forward its recommendation to TEC.
5) As per the decision reached in TEC, EL may reproduce 20 ~ 40% results in presence of developer/ vendor, where operationally and administratively possible. EL will

submit results of re-tests to NTISB/ TEC along with final recommendation. TEC will be called within 8x weeks of receiving results from EL.

6) Alternatively, if NTISB/ TEC concurs that official request is without merit, no further action is taken and same will be intimated to developer/ vendor. In any case, decision of NTISB will be considered final.

2.6.3 Task Close-Down Phase

After receiving SSER-SP and certificates, sponsor must do following with regards to CEP and documentation handover:-

1) Smooth handing and taking over of CEP and associated documentation back from EL to developer/ vendor.
2) Intimate NTISB in writing about successful handing/ taking over of CEP and documentation.
3) Retrieve documents handed over to developer/ vendor including documents of PSS and PSSIS publications from developer/ vendor and submit them back to NTISB after thorough checking.
4) Render a certificate to NTISB that no PSS document has been photocopied or reproduced.

Developer/ vendor shall:-

1) Ensure that all equipment handed over by EL through sponsor, to developer/ vendor is in operational state.
2) Receive all documents/ material or any supporting device etc.
3) Receive a document from sponsor intimating that evaluation has been completed.
4) Intimate sponsor in writing about successful handing/ taking over of CEP, documentation and other related material.
5) Render a certificate to NTISB that no PSS document has been photocopied or reproduced.

2.7 Post Evaluation Actions

After completion of evaluation and validation of CEP, some of post evaluation activities/ issues need to be focused by sponsor, in particular are:-

1) Sponsor must accept that the NTISB reserves right to record vulnerabilities and use of this information to guard against similar vulnerabilities that may occur in similar CEPs.
2) Sponsor must not make any statements in press releases or other promotional material which might be misleading, might misrepresent conclusion of evaluation and validation, or might bring PSSIS into disrepute.

3) When particular CEP is evaluated and validated, sponsor must only market that CEP on basis of a valid certificate received from NTISB.
4) Sponsor must not exaggerate benefits of evaluation and validation by claiming features or versions that have not been validated.
5) Sponsor is responsible for ensuring that developer/ vendor understands that he has similar responsibility.
6) Sponsor must inform NTISB of any vulnerability in CEP, if observed after it has been evaluated or during conduct of evaluation/ operation.

2.8 Appeals Procedure

Organizations affected by NTISB decisions and actions have right to file a formal complaint and appeal decision when they believe that NTISB actions have not been conducted according to PSSIS rules, procedures or PSS, or actions have resulted in unfair treatment of persons participating in or who are affected by NTISB. Any dispute concerning operation of CEP evaluations may be referred to NTISB by any party, e.g. EL, VDS.

Appeals concerning evaluation report (SSER) and results of evaluation/ validation shall be forwarded to NTISB in written within **1 month of submission of report** i.e. SSER sponsor/ developer. Procedure for submitting inquiry and dealing with is discussed below:-

1) An Official Request must be submitted to NTISB in writing. If requestor represents an organization, official request must be on organization's letterhead.
2) Assertions must be objective and not subjective.
3) CEP must be identified by reference or certificate number and specific technical details. Request must be nonproprietary and must not prevent further distribution by NTISB.
4) Secretary NTISB is responsible to resolve matter as per ***normal procedure*** discussed below or refer case to **TEC**.

Normal procedure for handling appeals is that:-

1) NTISB will share official request with EL.
2) EL shall determine merits of inquiry.
3) Once EL has completed its review, it will provide to NTISB a response with rationale on technical validity regarding merits of official request. EL will state its position whether its review of official request regarding CEP:-
    a) Is without merit and evaluation of CEP unchanged?
    b) Has merit and evaluation of CEP affected? EL will further state its recommendations regarding impact to evaluation.

4) NTISB will review EL rationale supporting its conclusion and forward its recommendation to TEC which will be called within 8 weeks.
5) As per decision reached in TEC, EL may reproduce 20 ~ 40% results in presence of sponsor reps, if technically and procedurally possible. EL will submit results of re-tests to NTISB/ TEC alongwith final recommendation.
6) Alternatively, if NTISB/ TEC concurs that official request is without merit, no further action is taken and same will be intimated to initiator/ sponsoring organization. In any case, decision of NTISB will be considered final.

Chapter 3

Re-Validation Processes

3.1 Introduction

Certificate initially awarded applies to specific evaluated version of Cryptographic Equipment (CE) and Cryptographic Primitives (CP) in its evaluated configuration. However, most CEPs are subject to post-evaluation changes that are outside scope of that evaluation, e.g. up-gradations, modifications etc. by developer/ vendor. Sponsor may choose to have a contract with NTISB to perform a re-evaluation of CEP, to ensure that validation extends to new version as well. However, it is not normally cost-effective to re-evaluate every new version of a CEP completely. Hence, CEP will be re-validated if changes made are significant and have impact on the security grading of device, otherwise validation will be maintained. Re-validation processes can be categorized into following:-

1) CEP validation maintenance.
2) CEP partial re-validation.
3) CEP full re-evaluation.
4) Re-evaluation on evaluation certificate expiry.

In addition, an evaluated device/ system may be required to undergo re-validation (i.e. after induction and during active operation) for purpose of verification confirmation and identification of possible vulnerabilities introduced in cryptographic community after its formal evaluation.

Re-validation process provides a means of establishing confidence that security level in a CEP is maintained without always requiring a formal full re-evaluation. Under these processes sponsor/ developer is able to maintain CEP validation with minor changes or CEP under goes partial re-validation without full re-evaluation for each of incorporated changes. VDS should always consider possibility of CEP validation maintenance at time of original evaluation. Re-validation process is given in ***Figure 3.1.***

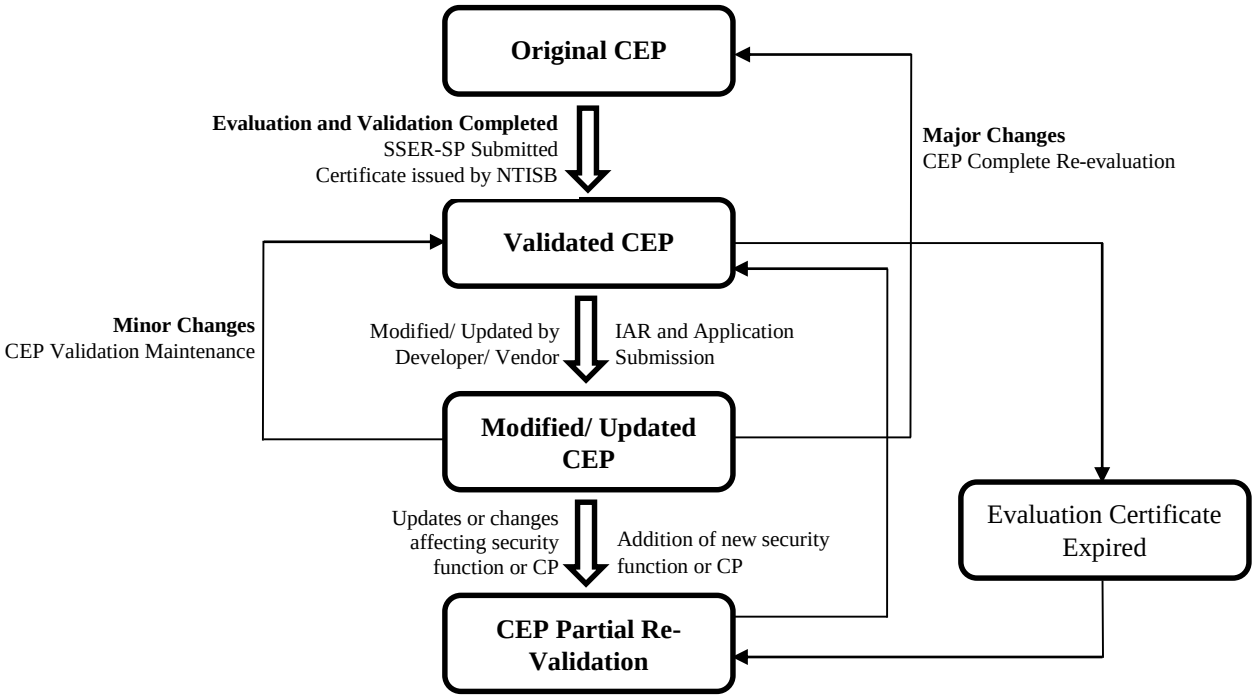

Figure 3.1: Re-Validation Process

3.2 Revalidation Expenditures

Expenditure for re-validation categories will depend upon extent of testing required for re-validation, and will be decided by NTISB in consultation with EL.

3.3 Impact Analysis Report (IAR)

For re-validation, IAR detailing security impact of changes (of a modified device) on evaluated CEP is prepared by developer/ vendor. Sponsor must ensure following in this regard:-

1) Before any contractual deal, developer must prepare IAR.
2) Sponsor will forward IAR received from developer/ vendor to NTISB for necessary review.
3) Alongwith the IAR, sponsor will also forward re-evaluation application to NTISB.

3.4 Certificate Validity Period and Re-evaluation on Evaluation Certificate Expiry

Evaluation certificate or evaluation results issued by NTISB will be valid for 5 years or as mentioned on certificate. After 5x years, CEP partial re-evaluation has to be performed whereas full re-evaluation will not be required. **However, in case new vulnerabilities or attacks against public domain algorithms or protocols inside CEP are announced, its certificate will be revoked**. Effort will be made by user that available updates or patches or system improvements will be applied as soon as possible. Report to this effect or otherwise will be shared with relevant authority and NTISB. Device shall be subjected to re-evaluation during

active operation for ascertaining maintainability of results obtained during initial evaluation prior induction.

3.5 Guidance on Usability of Previous Evaluation Results

For re-use of previous evaluation results, i.e. if a previously evaluated CEP is a component of a new CEP, or is to be re-evaluated after upgrade, sponsor should consider following guidelines:-

1) If security requirement of a previously evaluated component is greater than, or equal to, target security requirement of CEP, then previous evaluated results for that component can be used directly in evaluation of validation of new CEP.
2) If security requirement of a previously evaluated component is below target security requirement of CEP, then previous evaluated results for that component will NOT be used without further evaluation being performed.
3) If an evaluated component is used as a component of a new CEP, then context of its use may have changed. Hence, any vulnerabilities introduced in context of its new use, or found since previous evaluation, need to be tested.
4) If evaluated CEP has been subjected to a major upgrade/ change and the sponsor/ developer wishes later version to be evaluated and validated, a CEP full re-evaluation would be required.
5) If all of changes in previously evaluated CEP and its documentation are non-security related, then NTISB in consultation with EL may define scope of evaluation activity required as per re-validation process defined in this chapter.

Chapter 4

PSS Evaluation Documentation (PED) Requirement

4.1 Introduction

This chapter states broad guidelines, requirements and considerations for developer/ vendor when writing/ providing documentation in support of evaluation. Developer/ Vendor is required to provide documentation to NTISB for successful evaluation of CEP. Whereas, Evaluator will be obliged to complete evaluation based upon provided information and grade security classification accordingly. Requirements for evaluation fall in following two domains:-

1) Basic Documentation Requirements
2) System-Specific Documentation Requirements

4.2 Basic Documentation Requirements

Developer/ Vendor is required to provide following basic documents for complete and successful evaluation by EL, however, it is broadly, responsibility of the designer to satisfy EL's queries through documents, trainings, consultative sessions etc:-

1) Security policy
2) Required vendor information (against each assertion of PSS security standard documents, refer to ***Annex D*** for sample assertion to be filled by vendor/ developer)
3) Operational manual
4) User manual
5) Administration manual (if applicable)
6) Technical manual
7) Design document for CP

Detailed requirements for these documents are stated as follow:-

4.2.1. User/ Operational Documentation

User manual(s) shall be provided for evaluation by developer/ vendor. Manual(s) shall be structured, consistent, and shall have no vague or ambiguous information essentially containing following:-

1) Security functions relevant to end user.

2) Detailed analysis of functions relevant to end user.
3) Details of Installation and un-installation procedures for CEP.
4) Details of interaction/ installation/ un-installation procedures of related hardware and software and other components of CEP.
5) Guidelines for secure operation, showing how to use CEP in a secure manner.
6) Guidelines for plain mode of operation, showing how to use CEP in a bypass mode.
7) Operational details of KMS.

4.2.2. Maintenance Manual

Maintenance manual(s) shall be provided for evaluation. Manual(s) shall be accurate, structured, consistent, and shall have no vague or ambiguous information essentially comprising following:-

1) Types of maintenance relevant events.
2) Details of maintenance procedures, showing how CEP is maintained.
3) Details about how CSPs, keys etc. are removed when maintenance is carried out.
4) Instructions for installing and configuring CEP after maintenance.
5) Installation procedures after maintenance.
6) Assembling and mounting procedures after maintenance.
7) De-assembling and maintenance procedures.
8) Details related to KMS.

4.2.3. Administration Documentation

Regardless of fact that administration of CEP is a separate document or part of operational/ user manual, it shall have following contents:-

1) Functionality relevant to administrator.
2) Functions which provide information, and those which control security parameters, covering all parameters under administrator's control.
3) Security relevant events related to administrator.
4) Details of administrational procedures for operating CEP in plain & cipher mode.
5) Instructions for installing and configuring CEP.
6) Details related to KMS.
7) Other administrative information that is essential for administrator.
8) Administrative details of interaction/ installation/ un-installation procedures of related hardware and software and other components of CEP.

4.2.4. Technical Manual

Technical manual(s) shall be provided for evaluation by developer/ vendor. Manual(s) shall be structured, consistent, and shall have no vague or ambiguous information essentially containing following:-

1) Technical details of security functions.
2) Detailed design of hardware, software(s), and firmware.
3) Technical details of algorithm(s) and security mechanisms.
4) Implementation verification details.
5) High Level Design (HLD) details.
6) Details of Key loading, Key generation, key zeroization, key exchange mechanisms/ protocols and algorithms.
7) Details of cipher text authentication, device handshaking protocols and other security mechanisms.
8) Details related to CP security and verification.
9) All technical features of CEP.
10) Complete instruction set used to configure CE.
11) Details related to KMS.

4.2.5. Delivery and Configuration Documentation

Delivery and configuration procedures must be specified, showing how they maintain security, and covering:-

1) Impact of different configurations on security.
2) Details for delivery, transportation and environmental effects on CEP.
3) Details for installation and un-installation.
4) Details for mounting and un-mounting device(s).

4.2.6. Start up and Operation Documentation

Procedures for startup and operation in secure and plain modes shall be given in detail for evaluation, showing how they maintain security, and covering:-

1) Details of functions that can be deactivated or modified during startup, normal operation or maintenance.
2) Showing how to restore CEP after error states.
3) Details related to KMS.
4) Showing how to reconfigure and re-operate CEP after error/ faulty state.
5) Procedures to restore device to a secure state after failure or software/ hardware error.

6) Diagnostic tests (administrator, end-user or automatically initiated) for security enforcing hardware components.

4.2.7. Architectural Design

Architectural design shall be provided. Architectural design shall include:-

1) General structure of CEP.
2) All external interfaces.
3) All logical and physical paths.
4) Supporting hardware and firmware.
5) Security enforcing functions and protection mechanisms.
6) Functional block diagram, showing major components, with supporting statements.
7) Details related to KMS.
8) Design methodology shall be provided with supporting descriptions for formal specifications.

4.2.8. Detailed Design

Detailed design shall be provided. Documentation shall contain:-

1) Relevant features.
2) Characteristics are described.
3) CEP features implementation.
4) Requirements for specification of interfaces between components.
5) Requirements relating to modularity.
6) Provision of Data flow diagrams.
7) Flow charts.
8) Entity Relationship diagrams.
9) Hardware schematics.
10) Details related to KMS.
11) Entity life histories, etc. with supporting descriptions.

4.2.9. Key Hierarchy and Key Types Documentation

Vendor/ developer shall provide document showing key hierarchy implemented in CE, software, firmware and KMS. It shall contain details of types of keys generated, employed and used in CEP. It shall also explain purpose of each type of key in CEP.

4.2.10. Security Policy

Vendor/ developer shall provide a complete and detailed security policy. Policy shall contain that how security mechanisms are employed and used within the system. Security

policy of CEP may contain details of types of keys generated their usage and purpose of each key with key hierarchy.

4.2.11. Source Code

Vendor/ Developer shall provide annotated source code of CPs and facilitate walkthrough of source code for CEP. Vendor/ Developer shall pay attention to comments within source code so that they provide assistance to evaluators in understanding code. Comments will describe the way the code works, and will not be meaningless.

4.2.12. Source Code Implementation

Source code implementation shall include:-

1) Variables, Statements and functions etc. used in source code shall be well-defined, so that source code is unambiguous.
2) Details of selected compiler options may also be provided.
3) In addition details of any run time libraries (e.g. DLLs) used, various components (e.g. ActiveX) if used, shall also be provided.

4.2.13. Source Code and Hardware Drawings

Detailed design shall identify source code modules and functions; supporting information shall be provided either in detailed design, or in source code comments. Source code shall contain sufficient comments for evaluators to comprehend those aspects of code that are not clear from detailed design. In case hardware/ firmware code cannot be provided, arrangement for code walk through will be made by Vendor/ Developer/ Sponsor. For any conflict, secretary NTISB's decision will be final.

4.2.14. Testing Documents

Vendor/ developer shall provide details for testing/ evaluation, in-order to help evaluators to reproduce results as stated by vendor/ developer. Moreover test configuration(s) shall be provided for all tests mentioned in documentation by vendor/ developer.

4.2.15. Components Identification

Components and documentation shall be uniquely identified by an identifier, to be used in all references. Source code and hardware drawings shall also be uniquely identified.

4.3 System Specific Documentation Requirements

In addition to common documentation requirements, developer/ vendor is required to include all necessary system-specific information/ details in provided documentation for each area of complete evaluation process as described below:-

4.3.1. CP

Developer/ vendor is required to include following information /details about CP in provided documentation:-

1) Mathematical Model
2) Block Diagrams clearly showing CP components
3) Pseudo code
4) Annotated source code
5) Detailed design
6) Randomness testing details
7) Known Answer Tests details
8) Vendor Testing details (if any)
9) Test vectors, IVs and CSPs
10) Cryptanalysis report (if any)
11) Vendor claims
12) Components details and their flow diagrams

4.3.2. CE

CE evaluation documentation related to secure design and implementation of cryptographic module including specifications, ports and interfaces, roles, services and authentication, physical security, operational environment, key management, self-tests, design assurance and mitigation of other attacks.

4.3.3. EMC/ EMI

EMC/ EMI testing is an important consideration in selection of encryptor and must be tested for. Vendor/ sponsor is required to get EMC/ EMI certification of his device from recognized lab (NTISB designated) and submit the same for validation.

4.3.4. Key Management Requirements

KMS requirements include evaluation of KMS, procedures, rules and regulations, methods and protocols involved in generation, distribution, destruction, storage and establishment of keys and other CSPs. It encompasses key management centers governing these procedures, as well as interaction between them and protocols, rules and procedures involved in interaction. Vendor/ Developer is required to provide following information/ details:-

1) Technical manual of key management.
2) Documents describing testing performed by vendor/ developer along with test results.

3) OS details.
4) Block diagram of KMS.
5) Certification registration, public key infrastructure details.
6) Key hierarchy and key classification details.
7) KMS maintenance manual.
8) KMS operational manual.
9) Key management, key generation and key distribution mechanisms.

4.3.5. Implementation Verification Requirements (IVR)

It is desired that implementation verification of all implemented algorithms, protocols, and security mechanism be performed by Developer/ vendor to:-

1) Ensure that cryptographic functions are implemented and working correctly in CE.
2) Ensure that CEs are configured with specified parameters.
3) Verify that there are no backdoors in CE and only required data is output.

4.3.6. Claimed Security Level of CEP

Documentation must include a claimed rating for minimum strength of all security mechanisms/ components separately. Each critical algorithm, protocol, mechanism, components shall be given a rating based on its ability to withstand malicious activities.

Chapter 5

Indigenous Development & Export of Cryptographic Equipment

5.1 Introduction

Indigenous Information Assurance/ Cryptographic/ ITSec solutions are offered by private sector companies as well as public establishments for protection of information systems/ networks. For use within country, indigenously developed INFOSEC product, service, criteria etc. will be **preferred**. Prior induction, such equipment will undergo PSS based evaluation. In pursuit of **knowledge based economy** development and benefiting from such niche technologies, **export** of these solutions present a desirable opportunity for **securing foreign exchange**; however, **sensitivities related with cryptographic exports warrant restrictions** that should be applied on export of such systems.

5.2 Export of Cryptographic Equipment

Following points should be taken into consideration while applying for export of cryptographic equipment:-

1) Export of cryptographic solutions that remained under use or are currently in use or are under evaluation or are under consideration for Government, Armed forces or Critical National Infrastructure (CNI) is prohibited.
2) Export of solutions that have neither been evaluated by NTISB nor used by Government, Armed Forces or CNI may be allowed but after evaluation by NTISB for sole purpose of "Crypto Export Evaluation".
3) Till such time that "Crypto Export Evaluation" requirements are finalized, clause 5.2 (1) and 5.2 (2) shall be applicable.
4) Export of Crypto Solutions offer opportunity for exploitation with regards to system details/ information of similar solutions under use of Government/ Armed Forces/ CNI. It is therefore, only in presence of necessary safeguards/ variations that such devices will be cleared for export subject to assessment through Crypto Export Evaluation.
5) For detailed instructions, developers/ vendors must approach NTISB beforehand for obtaining current guidelines, procedures and regulations on cryptographic exports.
6) Crypto Export Evaluation will be financed by developer/ vendor.

All local firms engaged in Research & Development/ production of cryptographic solutions must register themselves with NTISB and/ or Ministry of Defense Production.

Annex 'A'

Categories of Cryptographic Primitives, Crypto and ITSec Equipment

A 1.1 Cryptographic Primitives

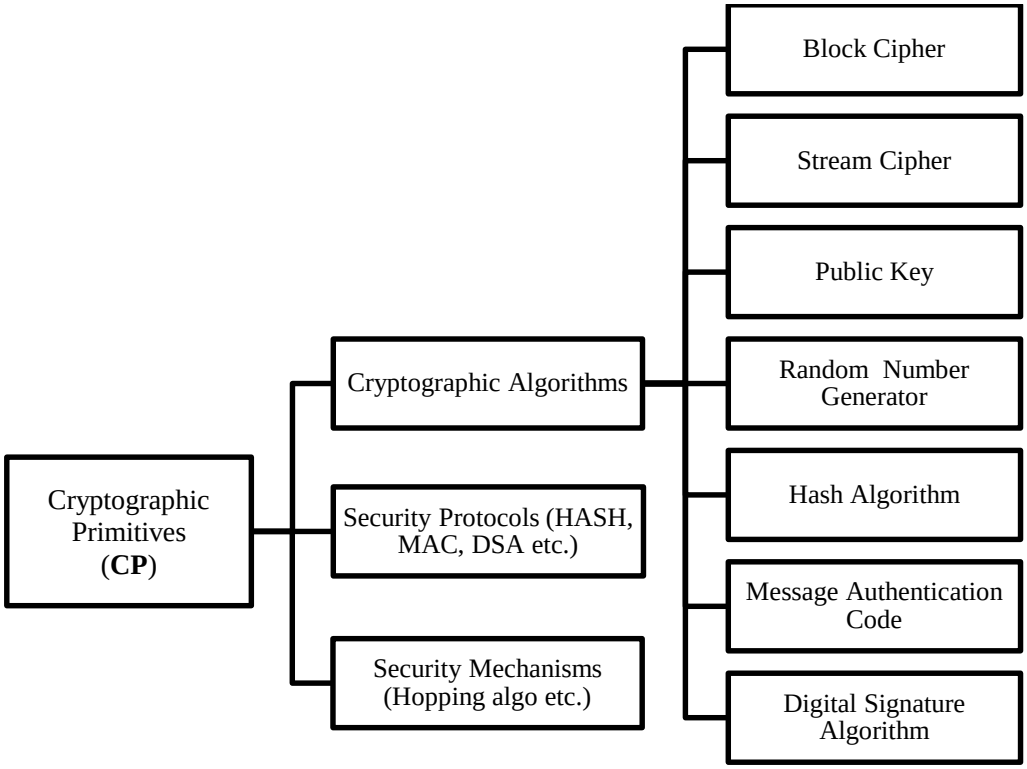

Figure A-1.1: Taxonomy of CPs

A 1.2 Cryptographic Equipment & Supporting Systems

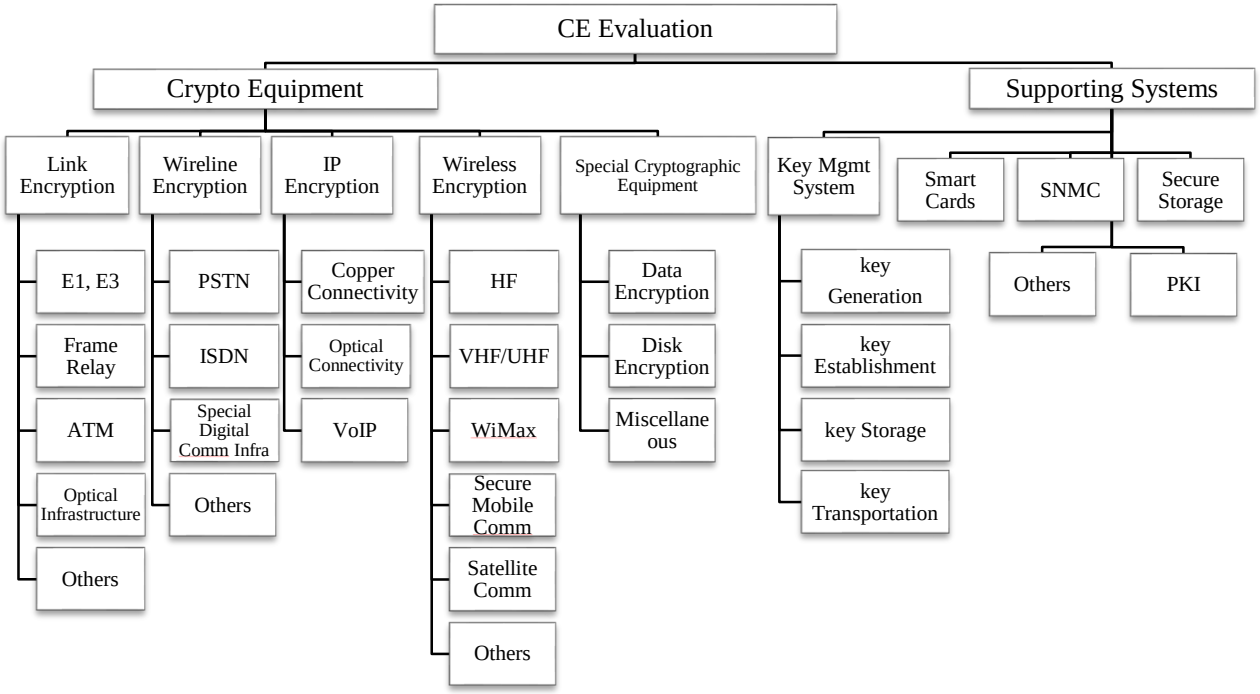

Figure A-1.2: Categories of CE and Supporting Systems

A 1.3 ITSec Categories

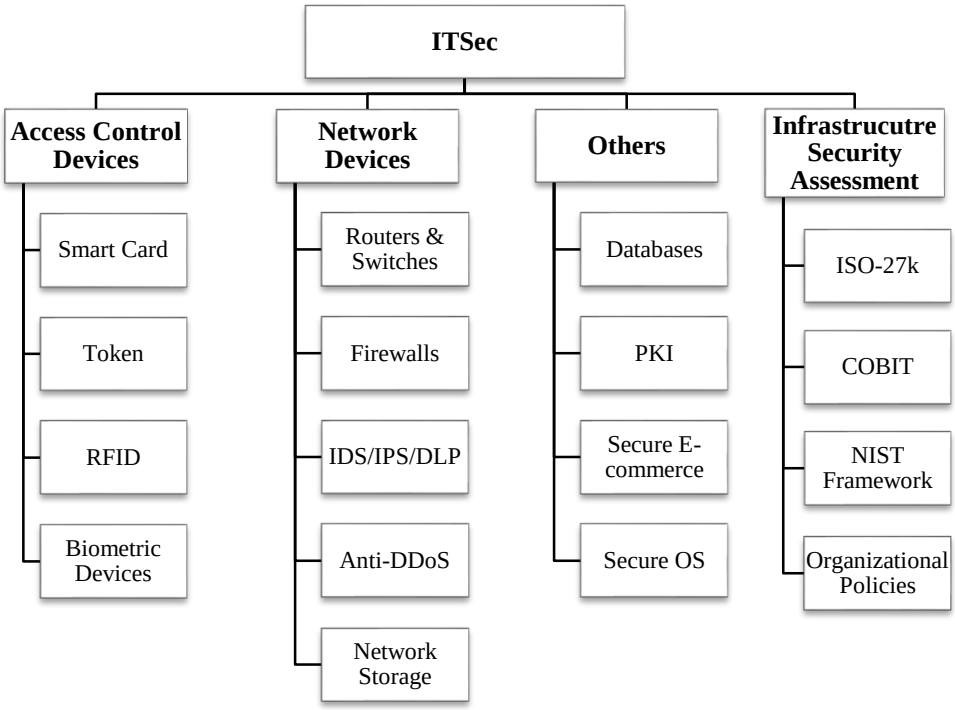

Figure A-1.3: ITSec Categories

Annex 'B'

PSS info Checklist for VDS

S/No	Checklist - Summary Guidance to Sponsor	Status
	Before EAAPP	
1.	CEP earmarked for procurement or induction is fully matured.	
2.	CEP has not been evaluated and validated as per PSS in any form before.	
3.	If a CEP; in full or any component has been evaluated and certified by any international evaluation and certification scheme, then evaluation results for validated components of CEP are available.	
	EAAPP	
	Evaluation Phase	
1.	Letter of Intent Initiated.	
2.	Certificate for Operational Trials to NTISB.	
3.	CEP Selection by Sponsor.	
4.	Preparation of SDM.	
5.	Documents from NTISB received.	
	a) PSS Publications – 2 Documents b) PSS (Restricted domain) documents – 10 Documents	
6.	PSS Non-Disclosure Agreement (PNDA) with NTISB.	
7.	NDA with Developer/ Vendor.	
8.	Hand over PSS & PSSIS Documents to Developer/ vendor.	
9.	Received NDA and receipt from developer about PSS & PSSIS document and dispatched to NTISB.	
10.	Received confirmation/ certificate from Developer/ vendor on providing proprietary information and dispatched to NTISB.	
11.	Contract Signing with developer/ vendor.	
12.	Preparation for PED.	
	a) Target defined with developer/ vendor. b) Timelines defined with developer/ vendor. c) Review of PED prepared by developer/ vendor.	
13.	Submission of evaluation application to NTISB.	

14.	Payment of evaluation expenditures to NTISB by developer/ vendor through sponsor.	
15.	Intimation to NTISB about payment made by developer/ vendor.	
16.	Signing of NDA for Proprietary Information. *By NTISB, Sponsor, Security consultant (if applicable) and EL.*	
Acceptance Phase		
1.	Requirements for Provision of PED to EL through NTISB	
	a) Vendor claims. b) Operational and technical design details of CEP as defined in PSS. c) Operational and design details of CE algorithms protocols and Key Management System as defined in PSS alongwith their cryptographic strength proofs. d) EMC/ EMI (MIL-STD-461E) compliance certificate from recognized and authorized lab on EMC/ EMI testing. e) Environmental (MIL-STD-810F) certification from any recognized and authorized lab on environmental testing. f) Details on implementation verification setup. g) Data of Known Answer Tests (KAT).	
2.	Submission of PED and Sponsor's PED Checklist to NTISB.	
3.	Preparation of response to Documentary Evaluation & Review (DER)/ Questionnaire.	
	a) Copy of Questionnaire to developer/ vendor. b) Meeting sessions with developer/ vendor & Security Consultant (if applicable). c) Clarification of queries, if any, from NTISB. d) Written agreement form developer/ vendor provision of required info/ supporting material and its submission to NTISB. e) Submission of timely response to NTISB.	
4.	Submission of response (missing info reply) of Questionnaire to NTISB.	
5.	Coordination & Preparation for Evaluation Start up Meeting.	
6.	Acceptance Decision of CEP by Secretary NTISB.	

Preparation Phase		
1.	Conduct of training by developer/ vendor.	
	a) List if individuals to under training from NTISB. b) Training Schedule. c) Training Syllabi/ contents. d) Intimation to NTISB in Writing on above points. e) Intimation to NTISB on completion of training.	
2.	Intimation to NTISB about additional requirements/ deliverables, if raised during training, mentioning due response/ stance from Developer/ Vendor.	
3.	Equipment Handing/ taking over between Developer/ vendor and EL reps with necessary documentation.	
4.	Submission of one copy of equipment handing/ taking over documents to NTISB.	
5.	Ensured Developer/ vendor's response to additional deliverables/ documentation.	
6.	Formal acceptance of CEP by NTISB.	

Annex 'C'

Template: PSS Non-Disclosure Agreement

THIS AGREEMENT, made this _____day of _____, 20___, is between _____, hereinafter referred to as developer/ vendor/ sponsor, _____, hereinafter referred to as sponsor and National Telecommunication and Information Security Board, hereinafter referred to as NTISB. WHEREAS, developer/ vendor/ sponsor, and NTISB desire to enter into evaluation and discussions concerning a product described as _____ submitted to NTISB. To enable NTISB to conduct necessary government oversight of evaluation of product by evaluation lab, it may be necessary for Sponsor to disclose security evaluation requirements in the form of Pakistan Security Standard (PSS) and PSS Implementation Scheme (PSSIS) documentation to developer/ vendor on behalf of NTISB. NOW THEREFORE, to protect such sensitive and classified Information, developer, sponsor and NTISB agree as follows:-

1) PSS and PSSIS Documentation will not be reproduced/ published in any form i.e. electronic and hard copy.
2) Photocopy of any part/ page/ section of PSS and PSSIS documentation will not be made in any case.
3) Information contained in PSS and PSSIS documentation will not be disseminated to any third party in any form.
4) Any Involved party shall be liable for legal obligations in case of any breach/ violation mentioned above.
5) PSS and PSSIS Documentation shall be returned to NTISB after culmination of security evaluation in its original form.
6) This agreement may only be modified by a writing signed by an officer of party to be bound. If any court of competent jurisdiction determines that any provision of this agreement is invalid, remainder of agreement will continue in full force and effect, and invalid provision shall be restated to most nearly give effect to its stated intent.

National Telecommunication and Information Security Board,

Cabinet Division, Government of Pakistan.

BY: _____
TITLE: _____
DATE: _____

SPONSOR'S NAME
Address
City

BY:_____
TITLE:_____
DATE:_____

DEVELOPER'S NAME
Address
City

BY: _____
TITLE: _____
DATE: _____

Annex 'D'

Template for Assertions Details

Vendor / developer shall furnish required vendor information document by replying to each assertion given in PSS security standard documents in following format:-

Assertion	**Assertion Number: AS03.11**
Statement: (example) If CE permits an operator to change roles without re-authentication, then CE shall verify authorization of identified operator to assume any role that was not previously authorized.	
Security Level	**Level 1/ 2/ 3/ 4**
Applicable	**YES/ N.A**
Vendor Information	Vendor/ developer has to provide sufficient information for evaluator to fully assess assertion.

Annex 'E'

Payments

Miscellaneous expenditures are borne by NTISB and EL during each evaluation. Specific test equipment is required to conduct evaluation which might not be available with EL. At times technical consultancy/ expertise is also required. Keeping this in view, an evaluation fee structure needs to be defined. Therefore, developer/ vendor shall be required to make payments for evaluation to NTISB/ EL for subject purpose. The amount of evaluation fee will depend upon the type of equipment, scope of evaluation, overall security level etc. and will be decided by NTISB in consultation with EL. Broadly, following fee structure will be followed:-

S#	Type of Evaluation	Broad Level Evaluation Requirements (To be submitted as per PSS Evaluation Requirements document)	Evaluation Timeline	Fee (Rs)
IT SECURITY PRODUCTS EVALUATION				
1.	**Surface Evaluation**	• Product specifications including Name, Model, Device Version/ Series, OS/ Firmware version, Security Features offered, UTM features (if any) etc. • Relevant Product Data sheet • Relevant Test Report(s) by third party labs (ICSA Labs, PSS Labs, etc.) • 3rd party Product Certifications e.g. FIPS 140-2, Common Criteria, etc. • International Ranking e.g. Gartner, Forrester, etc. • Client requirement(s)/ RFP – Security/ Operations (if any)	15x Working days	0.2M
2.	**Detailed Evaluation** with Standard Crypto/ Security algorithm	• All requirements at **Serial 1** with following additions o Vendor Testing Report (if any) o Algorithms Specifications (e.g. name, key size, block size, mode(s) used in product, reference to standard implementations, etc.) o Vendor Claims (if any) o Configuration Manual(s) o User Manual (s) o Technical/Administration Manual(s) o Proposed Deployment Model (High Level/ Low Level) • 2x functional devices with all Security and functional features including UTM licenses enabled and details of licenses as per contract (SLA & OLA) • Facilitation of Code Walkthrough	30x Working days	0.5M
3.	**Detailed Evaluation** with Proprietary Crypto/ Security Algorithm	• All requirements at **Serial 2** and **4** with following additions o Algorithm Source code and simulator provision o Implementation verification setup availability with proprietary Crypto algo(s) o Interactive sessions and support deemed necessary during evaluation	**1~3 Months	*1.0M
CRYPTOGRAPHIC/ SECURITY ALGORITHM EVALUATION				
4.	**Detailed Evaluation**	• Algorithm Specifications including but not limited to	**1~3 Months	*1.0M

	Proprietary Crypto/ Security Algorithm only	○ Algorithm Description including Name, Key size, Block size, mode(s) ○ Algorithm Sourcecode/ Simulator in a high level language preferably C/ C++ ○ Mathematical model and design details with block diagram(s) ○ Component level details with rationale of components in the algorithm design Vendor Testing Report ○ Test Vectors, IVs, CSPs ○ Vendor Claims ○ Cryptanalysis Report (if any)		
CRYPTOGRAPHIC DEVICE EVALUATION				
5.	**Detailed Evaluation** with Proprietary crypto/ security algorithm(s)	• All requirements at **Serial 4** with following additions ○ Device Specifications (High level Design Details, Component Details, Block diagrams, State transition Diagrams, Flow Diagrams, etc.) ○ Vendor Claims (if any) ○ Vendor Testing Report (if any) ○ Device Security Policy ○ Details of Algorithms Mode(s) used in product ○ User/ Operational Manual(s) ○ Configuration Manual ○ Technical/ Administration Manual ○ All approved & Non-Approved Operational Mode(s) ○ Key Mgmt System Details ○ 1x Key Mgmt Device (if any) ○ Supporting Systems Details ○ RNG Details • Implementation verification setup availability with proprietary crypto algo(s) • Interactive sessions and support deemed necessary during evaluation.	**3~6 Months	*1.5M
SECURE SOFTWARE APPLICATION EVALUATION				
6.	**Surface Evaluation with/ without Security Features Validation**	• Software Executable(s) • Test accounts (if required) • Datasheet/ Product Specification and User Manual (if any) • Software Test Reports (if any) • Product Certification (if any)	**15~30 Working days	**0.1 M ~0.3 M
7.	**Detailed Evaluation** with proprietary Crypto/ Security Algo	• All requirements at **Serial 4 & 6** • Software Source code Analysis and/ or Proprietary Algorithm Analysis • Fee structure will change if proprietary algorithm analysis also required • Client or server level software deployment requirements (if any) • Interactive sessions and support deemed necessary during evaluation	**15 ~ 30 Working days	*0.5M
8.	**Customized Evaluation**	• To be decided on case to case basis as per complexity and type of Target of Evaluation.		

Table E-1.1: Evaluation Fee

The fee is applied to new module submissions, modified module submissions and for report reviews that require additional time due to complexity or quality. All concerned may consult latest payment document from NTISB website (*www.cabinet.gov.pk)* prior engaging in PSS modalities.

Annex 'F'

Letter of Intent Template

[ORGANIZATION/ CUSTOMER NAME]

[ORGANIZATION/ CUSTOMER ADDRESS]

[DATE]

(Name Secretary NTISB with Rank)

Secretary NTISB

Cabinet Division

Islamabad

To Whom It May Concern

This letter is to inform you that the [**ORGANIZATION**] intends to evaluate/ purchase [**PRODUCT NAME and VERSION**] from [**VENDOR NAME**] in support of [**PROJECT NAME or CONTRACT NAME**].

Following is the brief information of [**PRODUCT NAME and VERSION**]:

1. Full product name and version number.
2. Description of the expected usage scenario and operational environment in which the product will be implemented. And, if approved certificate of the product exist then clearly mentioning the details of approval with version number and any change from previously evaluated version of TOE. If no approved certificate of the product exist then clearly mentioning the details of modules systems/ sub-system with version number and algorithms employed in TOE.
3. Government agency technical point of contact to include organization/ office designator, phone number and email address.
4. Government agency acquisition authority point of contact to include organization/ office designator, phone number and email address.

This letter in no way binds **[**CUSTOMER or ORGANIZATION**]** to purchase this product. However, successful evaluation of this product will be a determining factor in our acquisition decision process.

Date: ___ Month, Year

Name: _____
Title: _____

Official Seal:_____

Annex 'G'

PSS Security Levels

G-1.1 CP Security Grading

CP Type	Security Grading in CP Standard		
	A	**B**	**C**
Block Cipher	**Key Length Size**		
	≥128 <192	≥192 <256	≥ 256
	Block Length		
	≥128		
	User-Customizable Parameter(s)		
	$\geq 10^{506}$		
	S-box Customization Space (when S-box is not considered as User-Customizable Parameter)		
	$\geq 10^{13} < 10^{52}$	$\geq 10^{52} < 10^{506}$	$\geq 10^{506}$
	LSM Order		
	≥ 16		
Stream Cipher	**Key Length Size**		
	≥128 <192	≥192 <256	≥ 256
	Key Stream Period		
	$\geq 2^{128} < 2^{192}$	$\geq 2^{192} < 2^{256}$	$\geq 2^{256}$
	User-Customizable Parameter(s)		
	$\geq 10^{506}$		
	S-box Customization Space (when S-box is not considered as User-Customizable Parameter)		
	$\geq 10^{13} < 10^{52}$	$\geq 10^{52} < 10^{506}$	$\geq 10^{506}$
	LSM Order		
	≥16		
Public Key Cipher	**Modulus Length for IF Based Algorithms**		
	≥2048<3072	≥3072<4096	≥4096
	Field order for DLP based Algorithm		
	≥2048<3072	≥3072<4096	≥4096
	Subgroup Order for DLP Based Algorithm		
	≥224<256	≥256<384	≥384
	Binary Field Sub group Order of ECDLP based Algorithm		
	≥223<283	≥283<409	≥409
	Prime Field Sub group Order of ECDLP based Algorithm		
	≥224<256	≥256<384	≥384
Digital Signature Algorithm	**Key Length for DLP Based Algorithm**		
	≥2048<3072	≥3072<4096	≥4096
	Key Length for RSA-DS Based Algorithm		
	≥2048<3072	≥3072<4096	≥4096
	Key Length for ECDSA over Binary Based Algorithm		
	≥223<283	≥283<409	≥409
	Key Length for ECDSA over Prime Based Algorithm		
	≥224<256	≥256<384	≥384
Hash Algorithm	**Length of Hash Value**		
	≥256<384	≥384<512	≥512

Table G-1.1: Security Grading for CP Standard

G-1.2 CE Security Levels

A security level for CE standard can be ascertained by considering security levels in respective standards of SDI, CP, KMS and network management of overall system where CE is deployed. Following is the criteria for determining overall security level of CE while also incorporating respective levels for SDI, CP, KMS and NMC. Overall level for CE will be the **minimum** level attained in any area. Level-1 is the lowest, level-4 most stringent and requirements are primarily cumulative by level.

Security Levels	Security Levels Criteria		
	CE	**SDI**	**KMS**
1.	1. Security Level 1 in SDI. 2. Security Grade A in all CPs being used in CE. 3. Security Level 1 in KMS. 4. Minimum Security Grade A for all the CPs being used in network management.	1. **Lowest level of security.** 2. Basic security requirements are specified for the CE. 3. **CE does not require specific physical security mechanisms.**	1. Security Level 1 of SDI. 2. Minimum Security Grade A defined in GR of CP for all the CPs being used in KMS.
2.	1. Security Level 2 in SDI. 2. Security Grade A in all CPs being used in CE. 3. Security Level 2 in KMS. 4. Minimum Security Grade A for all the CPs being used in network management.	1. **Enhances the physical security mechanisms**. Adding requirement for tamper-evidence such as: • Tamper-evident coatings • Seals • Pick-resistant locks on removable covers. • Doors of the equipment. 2. **Shall also have role based authentication mechanisms**.	1. Security Level 2 of SDI. 2. Minimum Security Grade A defined in GR of CP for all the CPs being used in KMS.
3.	1. Security Level 3 in SDI. 2. Security Grade B in all CPs being used in CE. 3. Security Level 3 in KMS. 4. Minimum Security Grade B for all the CPs being used in network management.	In addition to requirements of Security Level 2, Level **3 requires identity based authentication** techniques.	1. Security Level 3 of SDI. 2. Minimum Security Grade B defined in GR of CP for all the CPs being used in KMS.
4.	1. Security Level 4 in SDI. 2. Security Grade C in all CPs being used in CE. 3. Security Level 4 in KMS. 4. Minimum Security Grade B for all the CPs being used in network management.	1. **Highest level of security**. 2. Level 4 requires providing a complete envelope of protection around it. 3. **Penetration of the CE enclosure** from any direction shall be detected and results in immediate zeroization of all plaintext CSPs. 4. **Identity based authentication mechanisms.**	1. Security Level 4 of SDI. 2. Minimum Security Grade C for all the CPs being used in KMS.

Table G-1.2: Security Levels for CE Standard

Annex 'H'

PSS Gazette Notification

REGISTERED No. M - 302
L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, THURSDAY, JUNE 22, 2023

PART II

Statutory Notifications (S.R.O.)

GOVERNMENT OF PAKISTAN

MINISTRY OF SCIENCE AND TECHNOLOGY

NOTIFICATION

Islamabad, the 14th June, 2023

S. R. O. 762(I)/2023.—In exercise of the powers conferred by section 14 of the Pakistan Standards and Quality Control Authority Act, 1996 (VI of 1996), the Federal Government in consultation with the Pakistan Standards and Quality Control Authority is pleased to:—

(a) prohibit with effect from **1st June, 2028,** the manufacture, storage and sale of the articles specified in column (2) of the Schedule below for sectors requiring cryptographic and IT security systems to protect sensitive information in computer, telecommunication or cyber systems which do not conform to the Pakistan standards established by the Pakistan Standards and Quality Control Authority as mentioned in column (3) of the Schedule;

(b) direct that each such article which conforms to the Pakistan Standards relating to that article shall be marked with standard mark of the Authority specified in column (3) of the Schedule, namely:—

(1853)

Price: Rs.5.00

[1196(2023)/Ex. Gaz.]

SCHEDULE

Sr.No	Description of article	Pakistan standard
(1)	(2)	(3)
1.	**IT Security**. Such articles that claim provision of a specific cyber security function such as all kinds of firewalls, network routers, high capacity switch, intrusion detection and prevention, end point security, secure access control systems, security information management, security information and event management, secure operating systems, secure applications, secure database management, anti-denial of service, anti-virus, anti-spyware, anti-theft, anti-malware or any other such solution.	PS:5543 Pakistan Security Standard for Cryptographic & ITSec Devices- ITSec Guide Book
2.	**Cryptographic**. Such articles that claim provision of confidentiality, integrity, authentication, availability or non-repudiation to users, networks or systems such as all kinds of cryptographic encryptors, hardware security modules, key generation, management or distribution systems, cryptographic tokens or systems for secure access or user authentication, cryptographic algorithms or protocols or operations, cryptography based communication or web applications, secure Virtual Private Networks or other such solutions.	PS:5544 Pakistan Security Standard for Cryptographic & ITSec Devices- Crypto Guide Book;

(c) direct that sectors requiring immediate adoption for deployment may undertake appropriate actions at their level with consultation of respective regulators or PPRA; and

(d) direct that consumer electronics or IT systems or solutions that do not claim the provision of security functionality shall stand excluded from this Notification.

[F. No. 5(87)/2021-ATA-II.]

AMIR MUHAMMAD KHAN NIAZI,
Deputy Secretary (Admn).

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER, STATIONERY AND FORMS, UNIVERSITY ROAD, KARACHI.