National Centre for Communication Security
Department of Telecommunications
Ministry of Communications
Government of India

Security Certification Of Telecommunication Products

R Babu Srinivasa Kumar
DDG, NCCS

07 October 2023

IoT SF Bengaluru Chapter

Why Communication security is important

- “In today’s interconnected world, telecommunications are transforming the way people engage in their everyday lives. Economic development is strongly related to the existence and well-functioning of the telecommunication networks. Electronic communications services guarantee the smooth transmission of data in this strongly interconnected world by providing the infrastructure for business services to run. Electronic communication services also play a significant role in national security, emergency response and in the economic development of a country. As a result, an outage in any one of these areas can result in severe consequences”
- The security of telecommunication network is of paramount importance for any country in terms of economic prosperity, social wellbeing and national security, Country’s sovereignty, territorial integrity, strengthening the rule of law…

Critical Information Infrastructure

- Critical infrastructure is defined as “those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period would impact on the wellbeing of the nation or affect a nation’s ability to conduct national defence and ensure national security”
- Telecommunication sector is one of the seven critical sectors declared by National Critical Information Infrastructure Protection Centre (NCIIPC) established under the Information Technology Act, 2000.
- Govt, Strategic & Public Enterprises, Power & Energy ,Banking Financial Services & Insurance, Transport and Healthcare are others.

Critical Information Infrastructure

- Each sector depends on services from the Communications Sector to support its operations and associated day-to-day communication needs for corporate and organizational networks and services (e.g., internet connectivity, voice services, and video teleconferencing capabilities etc) –Critical enabling function across all sectors.
- Telecommunication network infrastructure includes communication links, communication nodes and other support systems which carry voice, data and video from source to destination.
- Telecommunication network include PSTN, PLMN, Satellite Network, Broadband Network, Leased Line Network etc.

Early Initiatives

- A pilot project tiled ‘National Test Bed for Telecom Equipment Testing and Certification’ for establishing test lab in IISc Bangalore was started in 2007.
- This project was aimed to build capability and capacity in security certification of communication equipment used in Indian Telecommunication Equipment.
- After the initial work, Govt decided to set up Telecom Testing and Security Certification Centre(TTSCC) under DoT.

Early Initiatives

- As the indigenous security certification process was taking time, Govt in the year 2011 amended the license.
- In order to ensure telecom network elements are safe to connect DoT came up with the idea of Telecom Testing and Security Certification. However, as an interim measure, licenses were modified to include conditions on Security as below in Unified License

Early Initiatives

- “The LICENSEE shall induct only those network elements into its telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards e.g. IT and IT related elements against ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards, Telecom and Telecom related elements against 3GPP security standards, 3GPP2 security standards etc. The certification shall be got done only from authorized and certified agencies/ labs in India or as may be specified by the Licensor.”

MTCTE

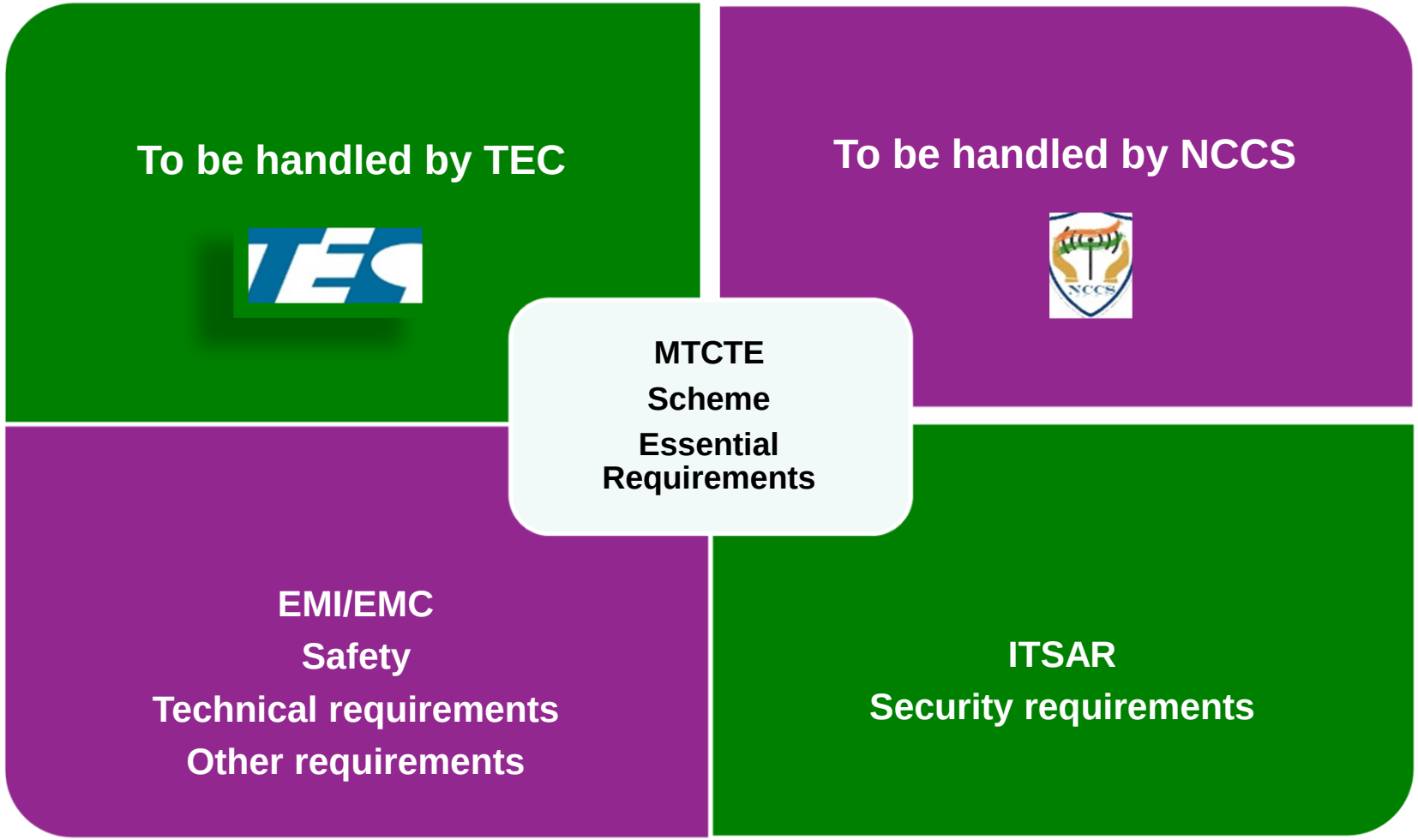
MTCTE

- The Indian Telegraph (Amendment) Rules, 2017, provides that every telecom equipment must undergo mandatory testing and certification prior to sale, import of use in India
- The detailed procedure for Mandatory Testing and Certification of Telecom Equipment (MTCTE) under these rules has been notified.
- MTCTE is to be carried out for conformance to Essential Requirements(ER) for the equipment, by Indian Accredited Labs designated by TEC /NCCS and based upon their test reports, certificate shall be issued .

MTCTE

- Essential Requirements of an equipment are a set of requirements against which Mandatory Testing and Certification of Telecom Equipment (MTCTE) will be carried out under MTCTE Procedure.
- Essential Requirements
  - ◊ EMI/EMC
  - ◊ Safety
  - ◊ Technical requirements
  - ◊ Other requirements
  - ◊ Security requirements will be handled by NCCS/DoT (ITSAR)

MTCTE


To be handled by TEC
To be handled by NCCS
MTCTE
Scheme
Essential Requirements
EMI/EMC
Safety
Technical requirements
Other requirements
ITSAR
Security requirements

ComSec Scheme

- Mandatory testing and certification in respect of Security requirements is planned to be implemented through a Scheme titled ‘Communication Security Certification Scheme’ (ComSeC).
- National Centre for Communication Security (NCCS) shall be responsible for implementation of this scheme. The headquarters of NCCS is located at Bengaluru
- NCCS is headed by Sr.DDG who is also the Scheme Controller.
- Sr.DDG/ Scheme Controller is assisted by three divisions:
  - ◊ Security Assurance Standards (SAS) Division
  - ◊ Security Lab Recognition/Designation (SLR) Division
  - ◊ Security Certification (SC) Division

ComSec Scheme

- Objectives of the scheme
  - ◊ To develop country specific security standards, processes and specifications.
  - ◊ To develop security testing and certification eco-system.
  - ◊ To ensure Telecom network elements meet security assurance requirements.
  - ◊ To ensure compliance of regulatory requirements pertaining to security testing
- EU is mulling security certification under EU 5G scheme(European cybersecurity certification scheme for 5G networks)

ComSec Scheme

- Scheme provides for
  - ◊ Preparation and publication of various process documents for the three division of NCCS to carry out their tasks.
  - ◊ Preparation and publication of ITSARs based on country specific security requirements, International Standards and consultations with stakeholders such as OEMs, TSTLs, TSPs, Academic institutes, Industry and Government bodies.
  - ◊ Designation of Labs as TSTLs after satisfactory evaluation of their application and competency of the lab to perform the security testing as per ITSAR. The labs from private and public sector can be designated as TSTLs .

NCCS Role

Development of country specific Security assurance standards called ***Indian Telecom Security Assurance Requirements (ITSAR)*** for every Telecom equipment

Designation of third party Telecom Security Test Laboratories (TSTL) meeting the specified requirements. The Designated TSTLs will be responsible for carrying out the security testing of telecom equipment as per ITSAR's requirements

Evaluation and Certification of the telecom equipment against ITSAR by NCCS.

ComSec Scheme

- The designation is valid for a period of 3 years
- Issue of Security Certificate for a Telecom equipment after evaluation of test results submitted by TSTL chosen by the applicant viz., OEM, TSP, Importer etc. Certificate is valid for 5 years or till the equipment is modified, whichever is earlier.
- Renewal and modification of certificates issued to TSTLs and the equipment.
- Issue of temporary certificates to facilitate quick deployment of software patches like updates and upgrades.
- Collection of fee for designation of TSTLs and certification of equipment.

ComSec Scheme

- Dispute resolution mechanism for various process under the scheme.
- Surveillance to ensure compliance to scheme requirements.
- Dealing with non-conformity and contraventions.
- PI visit https://nccs.gov.in for further details

Security Certification Process

- Preparation and publishing of equipment specific ITSAR.
- Designation of TSTLs by NCCS as per designation scheme.
- Applicants intending to get their equipment certified will register on MTCTE portal.
- After registration, the Applicant can choose a designated TSTL for security testing of his equipment against the applicable ITSAR.
- TSTL will conduct the requisite testing under the supervision of a validator from NCCS.
- After completion of the testing, test reports will be submitted by the TSTL for evaluation and security certification by NCCS.
- On successful evaluation, security certificate will be issued.

ITSAR

Telecom Peculiarities

- Telecom is a network of networks(system of systems)
- Telecom is
  - Highly connected systems
  - Requires High (Cyber) resilence
  - Protects Highly valuable assets
- Very large attack surface

India’s Approach

- Common Criteria approach
- 3GPP
- ITSAR
- ITSAR making is a consultative approach
- Two parts
  - ◊ Common Security Requirements
  - ◊ Specific Security Requirements
- Requirements are based on widely accepted security standards (baseline)+ based on threat modelling

Common Security Requirements

- Management Plane
  - ◊ Access(Remote Access guidelines) & Authorization
  - ◊ Authentication Attribute Management
- Life Cycle Management(Secure update/upgrade)
- Software Security(Source Code Analysis)
- Audit and logging
- Data Security; data at rest, data in motion; covert channel
- Overload Protection, DoS Attack
- Vulnerability Analysis(CVE, CVSS, zero day vulnerability)
- Fuzzing
- Hardware Security and OS hardening

Common Security Requirements

- Cryptographic Module (FIPS 140-2/3 standards)
- Secure Boot
- Secure NTP
- Crypto controls defined separately(to be updated for Post Quantum cryptography)
- OEM support during the entire lifecycle of the product

ITSARs so far

Sl No	Category	No of NEs/NFs
1	5G Core and RAN	13
2	4G Core and RAN	06
3	CPE	06
4	Miscellaneous	05

IoT ITSARs

IoT ITSARs

- ITSARs are prepared considering IoT security specifications of various regional/ international standardization bodies/ organizations/associations like ISO, ETSI, NIST, IoTSF, GSMA, ENISA and OWASP ISVS along with the country-specific security requirements .

- ITSAR will have two sections i.e Common Security Requirements(CSR) and then the entity specific Security Requirements (SSR)

IoT ITSARs

- Feedback device
- Vehicle tracking
- Smart energy meters
- Smart camera
- IoT Gateway
- Asset tracking device
- Pet tracking device
- Human tracking device

ITSAR Sections

IoT devices ITSAR covers sections on	
Authentication	Identity management
Authorization and Access Control	Storing Sensitive Information Securely
Make it easy for user to delete data	Data protection
Secure input and output handling	Communicate securely
Lifecycle management	Cryptography
Minimized exposed attack surfaces	Implement a means to manage reports of vulnerabilities
Vulnerabilities Management	Incident management
Make systems resilient to outages	Ensure software integrity
Incident management	Keep software updated
Firmware and Bootloader security	Hardware security
Installation and maintenance of device	Supply chain

National Trust Centre

- To develop a national framework for regulation and establishment of trust in IoT/M2M ecosystem.
- To design and develop a software platform which will enable a standardized way of information exchange between NTC and siloed IoT/M2M implementations.
- To create registries of IoT/M2M devices, manufacturers, service providers, Application providers and Applications are integrate them all to ensure accountability and trust in IoT/M2M eco system
- To integrate with PKI of GoI, thereby bringing all sectoral CAs under the Root certificate Authority of India established by Controller of Certifying Authorities
- To be interfaced with MTCTE portal

National Trust Centre

- Registration of IoT/M2M service providers.
- Registration of IoT/M2M ASP in a federated way.
- Registration of certified connected devices
- Registry of M2M/IoT applications
- Registry of tamper resistant end point identifiers

Thank You