

Telecom Security For Secure Digital India

One Mantra - Vocal for Local
One Path - Aatmanirbhar Bharat
One Goal - Viksit Bharat

- Hon'ble Prime Minister of India
Shri Narendra Modi



राष्ट्रीय संचार सुरक्षा केंद्र
NATIONAL CENTRE FOR COMMUNICATION SECURITY

दूरसंचार विभाग, भारत सरकार

DEPARTMENT OF TELECOMMUNICATIONS, GOVERNMENT OF INDIA

About NCCS



NCCS is a centre under Department of Telecommunications (DoT), responsible for implementation of Communication Security Certification Scheme (ComSeC). NCCS aims to meet the following objectives in operating and maintaining the ComSeC scheme:

- Development of India specific standards, specifications and processes
- Development of testing and certification eco-system
- Ensure that Telecom network elements meet security assurance requirements
- Ensure compliance of regulatory requirements pertaining to security testing

NCCS Functions

- Telecom Security Standards Development - Indian Telecom Security Assurance Requirements (ITSAR)
- Telecom Security Test Lab (TSTL) Designation
- Security Certification - Certified Products
- Security Standards Development Facility - Security Assurance Standards Facility (SASF)
- Implementation and Controlling ComSeC Scheme & Dispute Resolution

Stakeholders

- OEMs
- Industry Associations
- Telecom Service Providers
- Telecom Security Test Labs (TSTL)
- Academia
- Govt Ministries and Organizations



Ensuring Security of Digital Communications



Development of indigenous security standards



Enhanced Security of Telecom Networks with certified products



Development of domestic telecom security testing ecosystem

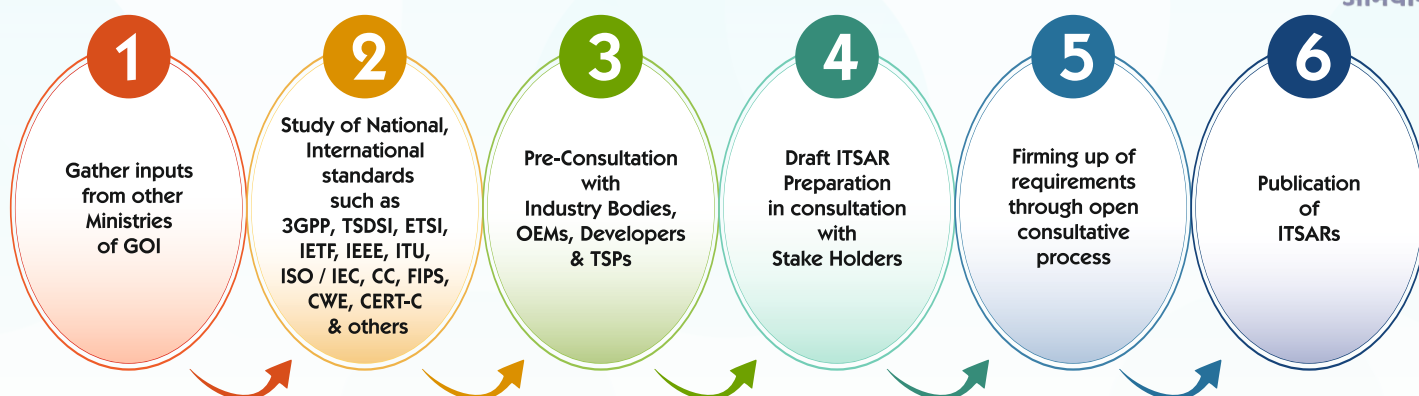


Single window system for Ease of Doing Business

Threat Outlook

- Authentication bypass, Privilege escalation, Man-in-the-Middle (MITM), Eaves dropping, Masquerading, Packet Sniffing, Repudiation, Data corruption, Information disclosure etc.
- Routing Table Poisoning, DNS Cache poisoning, DNS Spoofing, Amplification and Route redirections, Sink holding etc.
- DDoS, Malware, Code-injection, Exploitation of Known Vulnerabilities, weaknesses in software etc.
- Weaker Cryptographic Implementations, Known plain text attack, Key Truncation, Key padding etc.
- Session Hijack, Bidding down, Cross site scripting (XSS), SQL Injection, File Inclusion etc.
- Broken Access Control, Server Side Request Forgery, Insecure Design etc.
- Cross-Site Request Forgery, NULL Pointer Dereference etc.

ITSAR Development Process



Total 55 ITSARs have been published covering wide variety of Telecom products / Network Functions

Security Requirements addressed by ITSARs

Access and Authorization | Authentication Attribute Management | Protocol Robustness Testing | Software Security | System Secure Execution Environment | User Audit | Data Protection & Cryptography | Network Services Security | Attack Prevention Mechanisms | Vulnerability Testing Requirements | Operating System Security | Web Servers Security

List of ITSARs Published

Cloud Security:

- Network Function Virtualization (NFV)

5G-Network Equipment:

- Aggregated GNB NSA Option-3,7 & 4
- Aggregated GNB SA Option-2
- 5G Disaggregated RAN gNB [CU-DU-RU]

5G-Network Functions:

- User Plane Function (UPF)
- Session Management Function (SMF)
- Unified Data Management (UDM)
- Network Repository Function (NRF)
- Network Data Analytics Function (NWDAF)
- Service Communication Proxy (SCP)
- Security Edge Protection Proxy (SEPP)
- Access and Mobility Management Function (AMF)
- Authentication Server Function (AUSF)
- Network Exposure Function (NEF)
- Non-3GPP Interworking Function (N3IWF)
- Short Message Service Function (SMSF)
- Unified Data Repository (UDR)
- Application Function (AF)
- Binding Support Function (BSF)
- Policy Control Function (PCF)
- Unstructured Data Storage Function (UDSF)
- Network Slice Selection Function (NSSF)
- Location Management Function (LMF) & Gateway Mobile Location Centre (GMLC) .
- Charging Function (CHF)
- Network Slice Admission Control Function (NSACF)
- UE Capability Management Function (UCMF)
- Equipment Identity Register (EIR)
- Lawful Interceptions System (LI)

Crypto Controls:

- Crypto Controls Applicable for all ITSARs

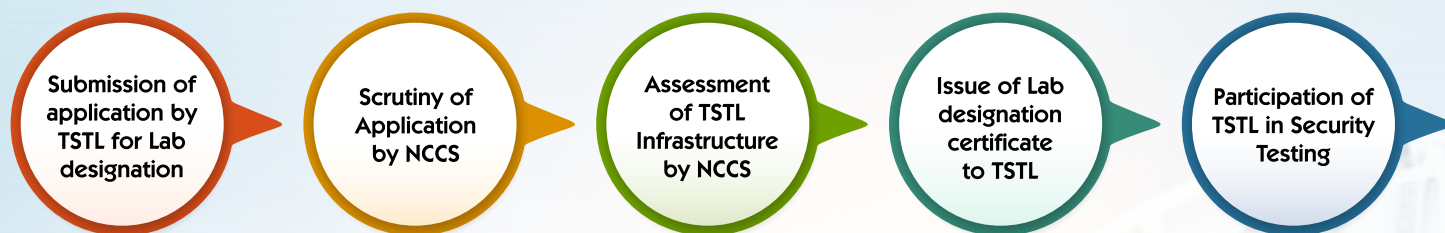
4G-Network Elements:

- Serving-Gateway (S-Gateway)
- Policy and Charging Rules Function (PCRF)
- Home Subscriber Server (HSS)
- Mobility Management Entity (MME)
- Evolved-Node-B (E-Node-B)
- Packet Data Network-Gateway (P-Gateway)

Other Network Elements:

- Mobile User Equipment (Ver 2.0.0)
- Hybrid Set Top Box
- Transmission Terminal Equipment
- Cell Broadcast Centre
- Optical Network Terminal (ONT)-PON Family Broadband
- Optical Line Terminal (OLT)-PON family Broadband
- Private Automatic Branch Exchange (PABX)
- IP Router
- Wi-Fi (CPE) Modem
- Plugable (U) ICC
- e-UICC (e-SIM)
- Operating System
- Firewall
- Feedback Device - IoT
- Vehicle Tracking Device - IoT
- Smart Energy Meter - IoT
- Smart Camera - IoT
- CSR Group - I Devices (5G Core Network Functions)
- CSR Group - IV Devices (IP Router and Other Elements)
- CSR Group - V Devices (OLT and ONT)

TSTL Designation Process

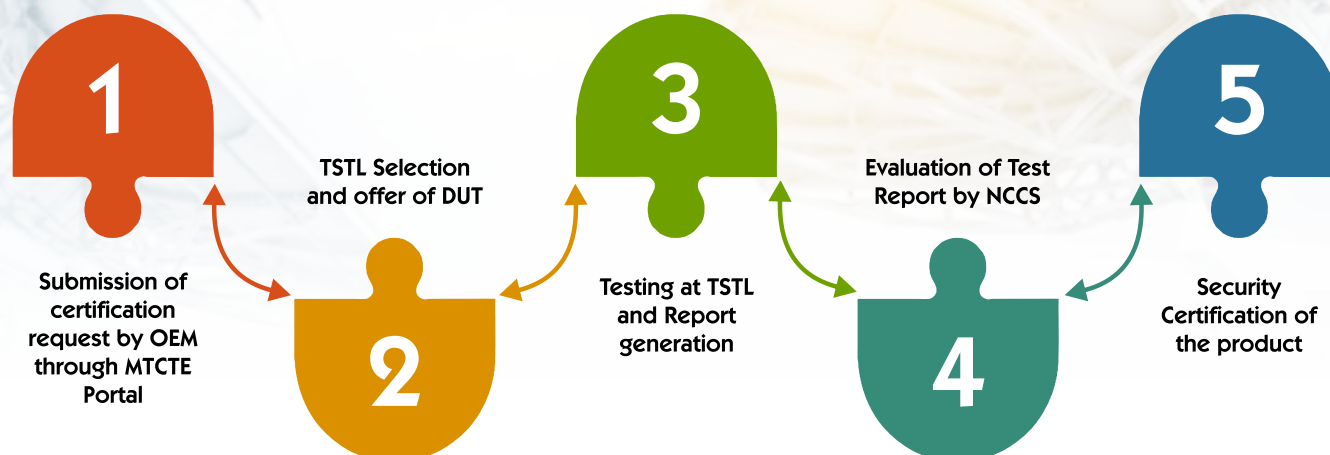


Designated TSTLs

- | | | |
|--|--|---|
| 1. M/s Acucert Labs LLP | 4. M/s Deltaphi Labs Private Limited | 7. M/s IITM Pravartak Technologies Foundation |
| 2. M/s UL India Private Limited | 5. M/s Matrix Shell Technologies Private Limited | 8. M/s Inteleciber Services Private Limited |
| 3. M/s Granite River Labs India Services Private Limited | 6. M/s Nemko India (Test Lab) Private Limited | 9. M/s Compliance International Private Limited |

Total 27 Telecom Products / Network Functions have been covered

Security Certification Process



Total 148 Security Certification Applications have been received and under process.

Mandatory security certification for IP Router, WiFi-CPE and SMF (5G Core) is in force.

Mandatory Security Certification of OLT & ONT with effect from 01/01/2026 and many more to follow.

Key Focus Areas

- Satellite Communication
- Quantum Cryptography
- IoT Security
- 5G & Beyond
- Cloud & Virtualisation Security

Future Roadmap

- Establishment of test bed for 5G and Beyond Technologies.
- Facilitate Startups for design and development of security related Products / Services.
- Enabling security testing ecosystem.
- Capacity Building in telecom security domain.
- Research and Innovation in telecom security for creation of Intellectual Property.
- Collaboration with Industry and Academia

National Centre for Communication Security - NCCS

City Telephone Exchange, Sampangirama Nagar,
Bengaluru - 560027