

***Communication Security
Certification Scheme
(ComSeC)***

Background

- 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
- Govt. of India through DoT has amended Indian Telegraph act, which is Indian Telegraph (Amended) Rules 2017
- According to Indian Telegraph (Amendment) Rules, 2017 every Telecom equipment must undergo mandatory testing and certification prior to sale, import or use of the telecom equipment in India.

Objectives - ComSeC

- Mandatory testing and certification in respect of Security requirements is being implemented through a Scheme titled 'Communication Security Certification Scheme' (ComSeC).
- **Objectives of the scheme**
 - To develop country specific security standards, processes and specifications
 - To develop testing and certification eco-system.
 - To ensure Telecom network elements meet security assurance requirements.
 - To ensure compliance of regulatory requirements pertaining to security testing

Contd...

Scope - ComSeC

- The scope of certification covers all types of telecom equipment to be sold in India and to be connected to Indian telecom network after the date of effect of this scheme for which ITSAR is available and is in force.
- National Centre for Communication Security (NCCS) is responsible for implementation of this scheme.
- NCCS is headed by Sr. DDG who is also the **Scheme Controller**
- Sr. DDG/ Scheme Controller is assisted by three divisions each headed by a DDG:
 - Security Assurance Standards (SAS) Division
 - Security Lab Recognition/Designation (SLR) Division
 - Security Certification (SC) Division

Details – ComSeC

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 & Government bodies etc.
- 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
- The designation is valid for a period of 3 years

Details – ComSeC

Scheme provides for:

- 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

Contd...

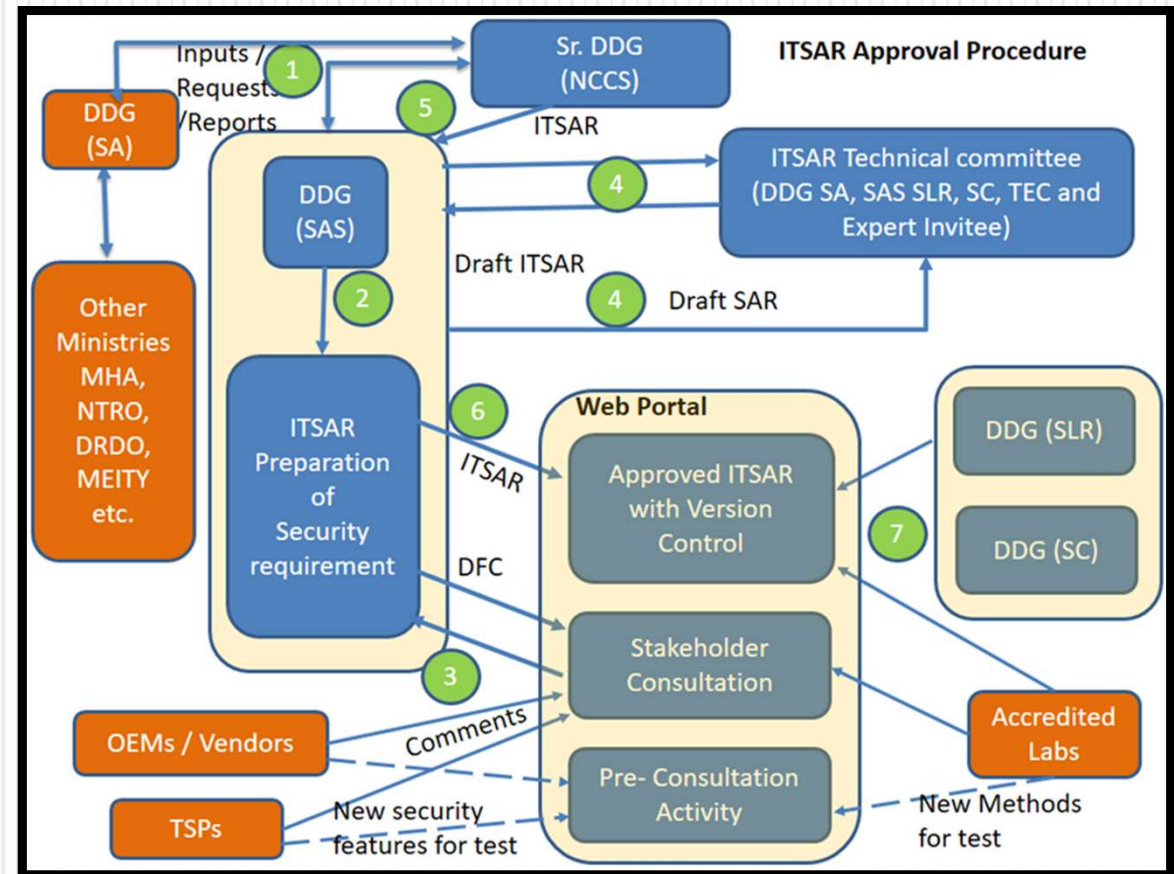
Details – ComSeC

Scheme provides for:

- Dispute resolution mechanism for various process under the scheme.
- Surveillance to ensure compliance to scheme requirements.
- Dealing with non-confirmity and contraventions.

ITSAR preparation

1. Request generation,
Taking inputs /
requests
2. Preparation of ITSAR
3. Stakeholders
Consultation
4. ITSAR Technical
Committee Review
5. Approval of ITSAR
6. Publish of ITSAR
7. Use of ITSAR



DETAILS OF ITSARs PUBLISHED

S No	Category	NEs/NFs for which ITSARs published	No of NEs/NFs
1	5G Network	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) gnodeB SA (Option 2) gnodeB NSA (Option 3, 4 and 7) NFV	14
2	CPE	Wi-Fi (CPE) Modem Mobile user equipment Pluggable (U)ICC Optical Network Terminal (ONT) - PON family Broadband Private Automatic Branch Exchange (PABX) Hybrid Set Top Box	6

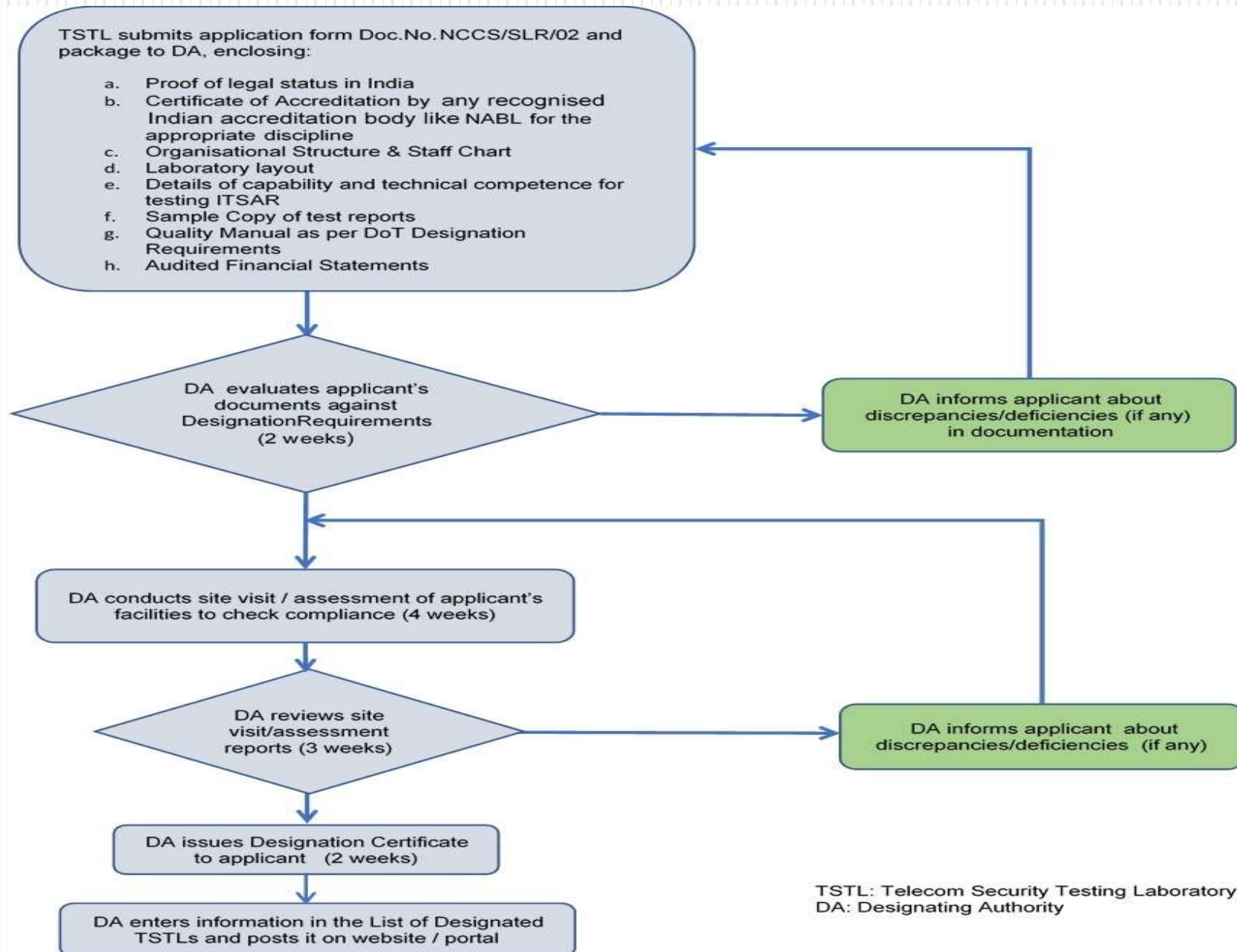
DETAILS OF ITSARs PUBLISHED

S No	Category	NEs/NFs for which ITSARs published	No of NEs/NFs
3	4G Network	Mobility Management Entity Serving Gateway PDN Gateway Policy and Charging Rules Function Home Subscriber Server E-Node – B (4G Access Network Element)	6
4	Miscellaneous	IP Router Cell Broadcast centre Transmission Terminal Equipment Optical Line Terminal (OLT) – PON family Broadband CPE (ONT)	4
	Total		30
	Crypto controls applicable for all ITSARs		

TSTL Designation Scheme

- Applications were invited from TSTLs from 20-06-2022 for Router, UICC and WiFi CPE
- Further, Now applications are invited for all published ITSARs
- One Lab M/S Accucert Labs LLP has been designated for IP Router and Wi-Fi CPE on 30.12.22.

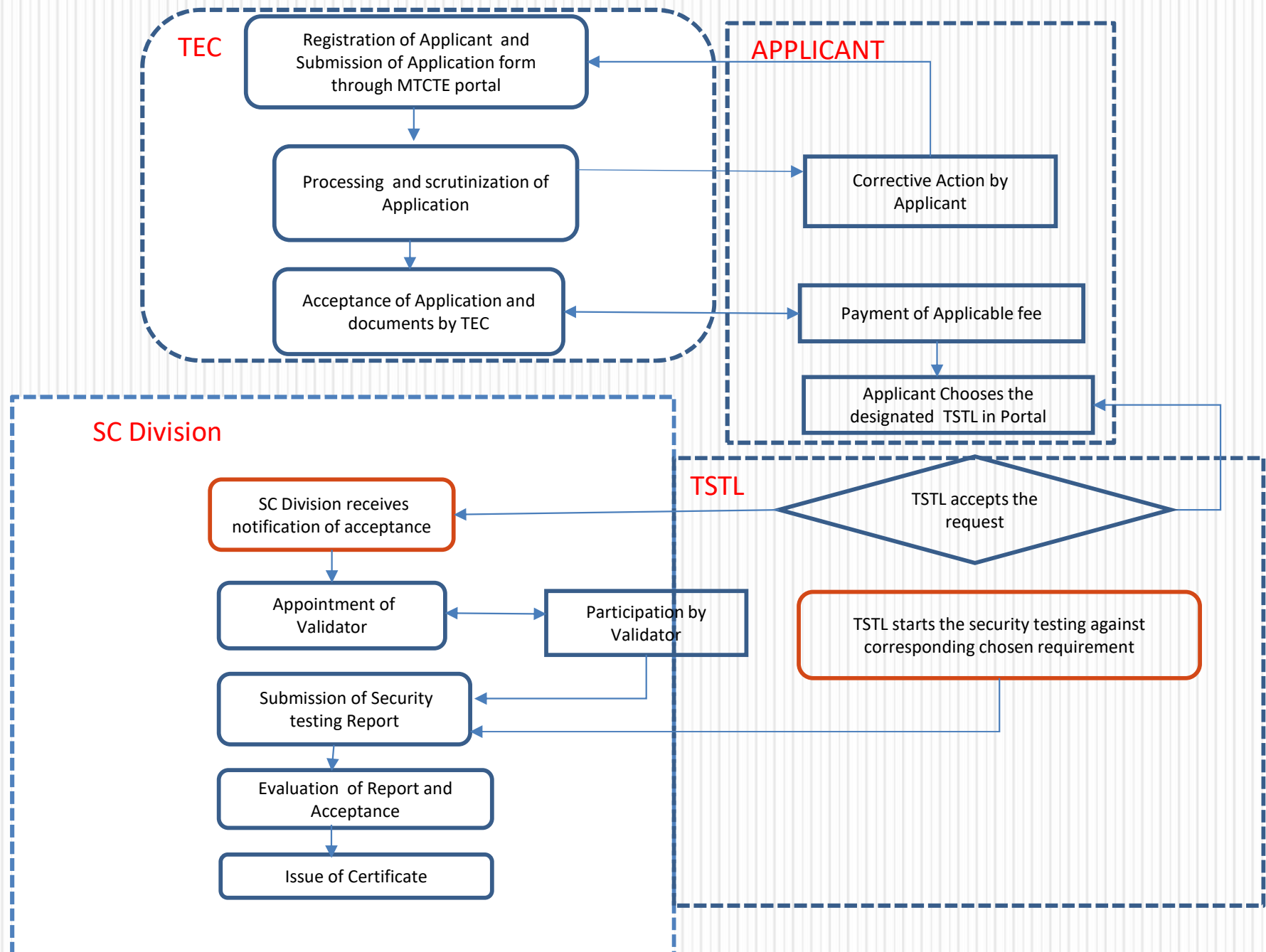
TSTL Designation Process



Security Certification Process

1. Preparation and publishing of equipment specific ITSAR.
2. Designation of TSTLs by NCCS as per designation scheme.
3. Applicants intending to get their equipment certified will register on MTCTE portal and provide ER BoM, ITSAR BoM along with paying the requisite fee as per type of certificate(ER, ER+ITSAR, ITSAR only).
4. After registration, the Applicant can choose a designated TSTL for security testing of his equipment against the applicable ITSAR.
5. TSTL will conduct the requisite testing under the supervision of a validator from NCCS.
6. After completion of the testing, test reports will be submitted by the TSTL for evaluation and security certification by NCCS.
7. On successful evaluation, security certificate will be issued.

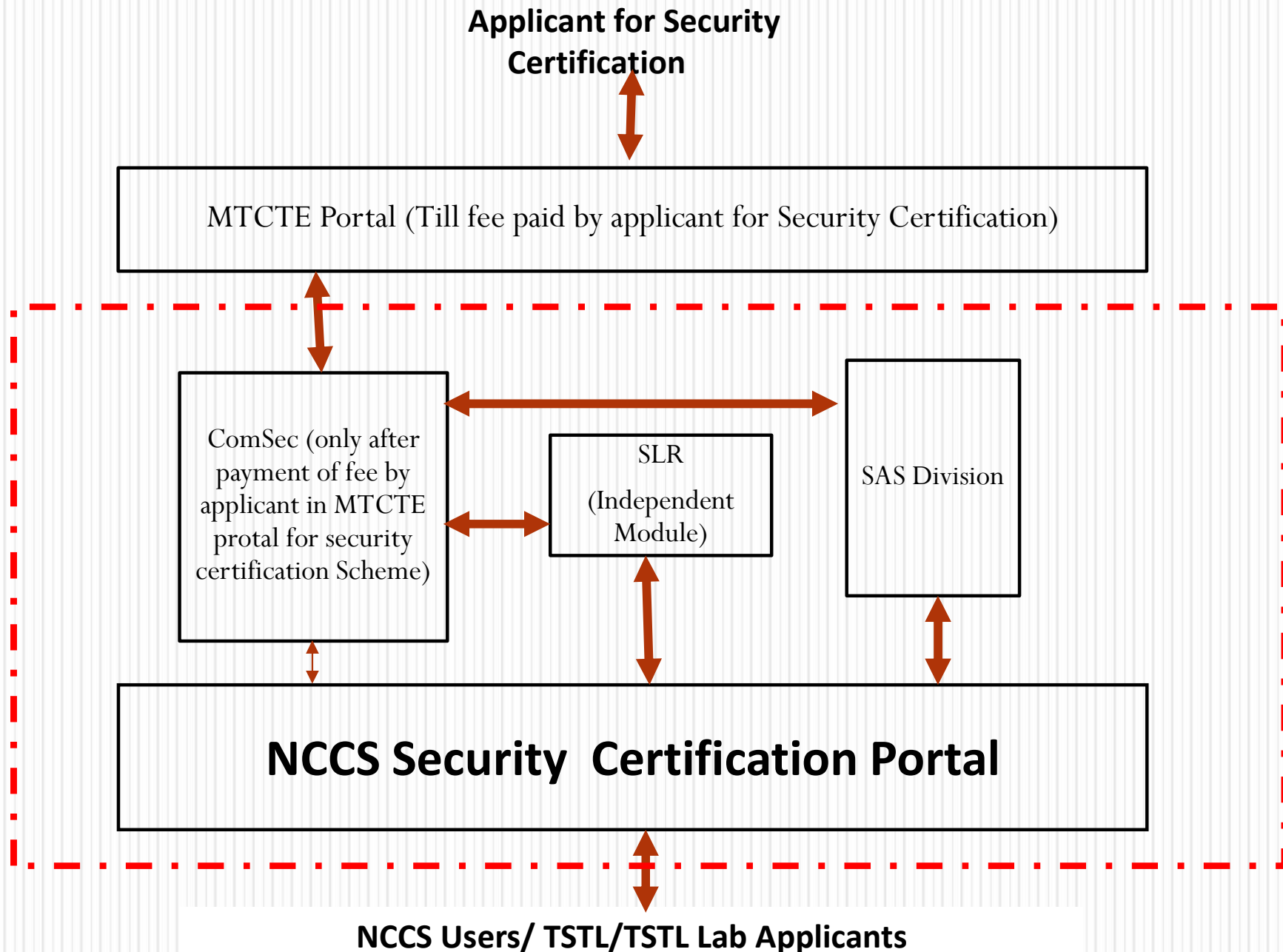
Certification process flow



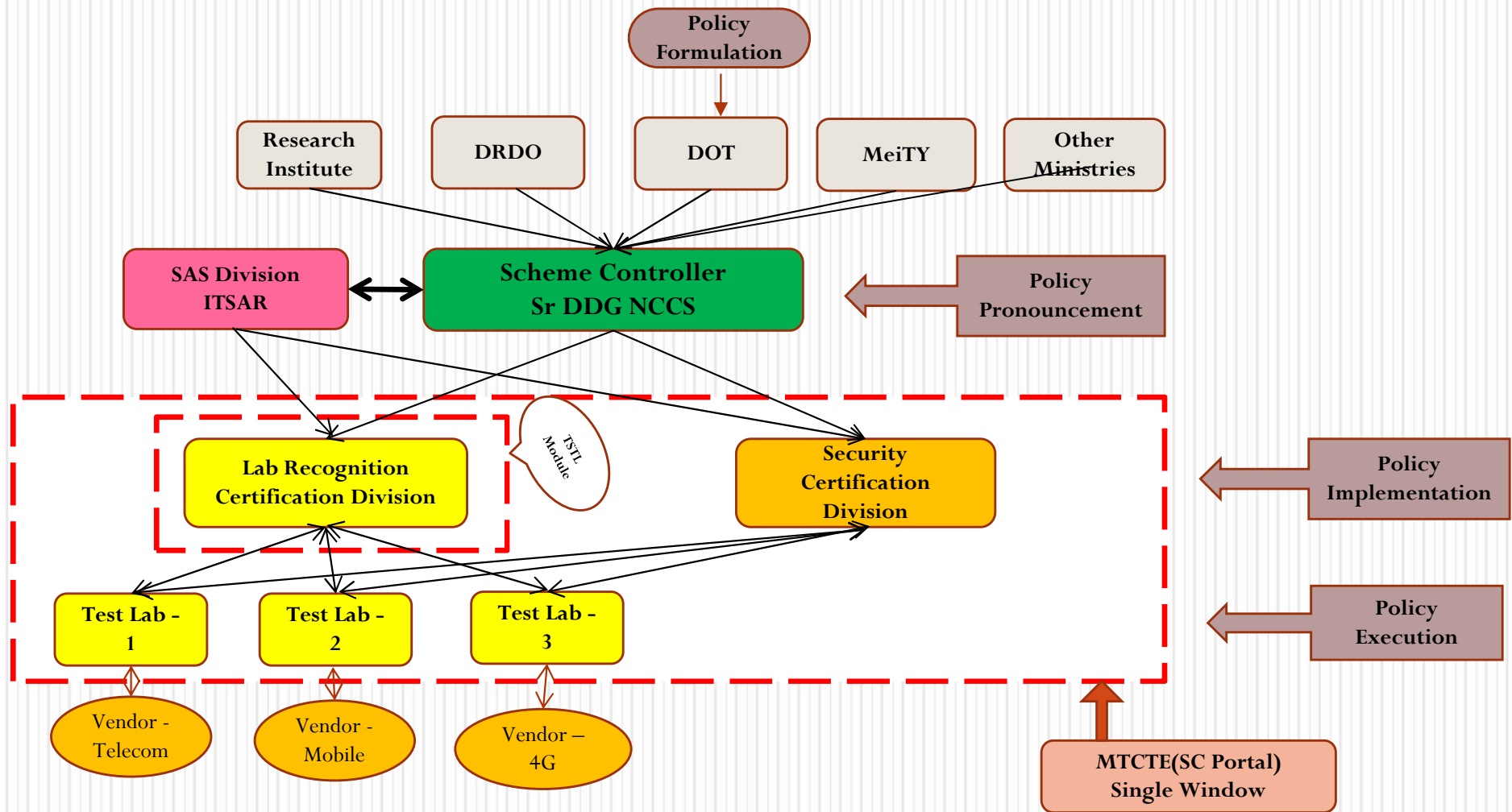
Security Certification portal & integration with MTCTE

- Implementation of ComSeC scheme needs development of Security Certification portal and modification of existing MTCTE portal as a Single Window System in coordination with TEC.
- C-DOT has been entrusted with responsibility of developing and integrating security certification portal with MTCTE Portal of TEC in Dec, 2022. Beta version of portal is expected to be ready by Oct 2023.
- Final version likely to be ready by end Dec, 2023.

NCCS Security Certification Portal



Security Testing Framework



THANK YOU

