Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

Cryptographic Controls

ITSAR Number: ITSAR001962009
ITSAR Name: NCCS/ITSAR/Standards Applicable for Group of Equipment/Cryptographic Controls/Cryptographic Controls (Applicable to all ITSARs)

Date of Release: 20.09.2020 Version: 1.0.0
Date of Enforcement:

MTCTE के तहत जारी:
Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. Security Assurance Standards (SAS) division of NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sr. No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Cryptographic Controls	ITSAR001962009	1.0.0	20.09.2020	First release

Table of Contents

1. Scope

This document provides a list of the prescribed cryptographic controls applicable to Indian Telecom Security Assurance Requirements (ITSAR).

2. Introduction

In order to ensure that the Network Element is safe to connect in the Indian telecom Network, National Centre for Communication Security (NCCS), A unit of Department of Telecommunications (DOT) under Ministry Of Communications, Government of India specifies the Indian specific Telecom security requirements called Indian Telecom Security Assurance Requirements (ITSAR), for every Telecom Network Element.

Telecom network element that complies with the specific ITSAR must adopt the various categories of cryptographic controls specified in this document, which include symmetric key encryption and decryption, Asymmetric key encryption and decryption, digital signatures and hashing.

All the secure protocols or services at every layer of TCP/IP or OSI stack in the Network element like IPSec at Network layer, TLS/SSL/DTLS at Transport/session layer, SSH/ SNMP/ Diameter/ HTTPS at Application layer, etc. shall strictly implement the list of cryptographic controls specified in this document only.

3. List of Cryptographic Controls

TABLE-1

Sr. No.	Cryptographic Control Category	Prescribed Cryptographic Control
1	Symmetric Key encryption and decryption	AES-128, AES-192, AES-256 and above
2	Asymmetric Key encryption and decryption	RSA-2048 and above
3	Key Exchange	Diffie-Hellman-2048 and above
		RSA-2048 and above
4	Digital Signature	DSA-2048 and above
		ECDSA 224-255, 256 and above
		RSA-2048 and above
5	HASH	SHA-224, SHA 256, SHA-512/224, SHA3-224 and above

This list of cryptographic controls gets amended from time to time based on the security threats posed to the telecom network.

Annexure-I

Acronyms

AES	Advanced Encryption Standard
DOT	Department of Telecommunications
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECDSA	Elliptical curved Digital Signature Algorithm
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
ITSAR	Indian Telecom Security Assurance Requirements
NCCS	National Centre For Communication Security
RSA	Rivest, Shamir, and Adelman
SASF	Security Assurance Standards Facility
SHA	Secure hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security