Indian Telecom Security Assurance Requirements (ITSAR)

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

Cryptographic Controls

(Draft for comments)

ITSAR Number: ITSAR09601YYMM
ITSAR Name: NCCS/ITSAR/Standards Applicable for Group of Equipment/Cryptographic Controls/Cryptographic Controls (Applicable to all ITSARs)

Date of Release: DD.MM.YYYY Version: 2.0.0
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. 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	ITSAR096012009	1.0.0	22.09.2020	First release
2.	Cryptographic Controls	ITSAR09601YYMM	2.0.0	DD.MM.YYYY	Second Release

Table of Contents

A) Outline

Telecom network element that complies with the specific ITSAR must adopt the various categories of cryptographic controls. The objective of this document is to prescribe list of crypto graphic controls to be adopted by various ITSARs published by NCCS.

The specifications/standards produced by various regional/ international standardization bodies/ organizations/associations like National Institute of Standards and Technology (NIST)- USA, Federal Office for Information Security (BSI) - Germany, Canadian Centre for Cyber Security, French Cyber Security Agency – ANSSI, Global Platform etc. along with the country-specific cryptographic requirements are the basis for this document.

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.

This document commences with a brief description of encryption, decryption, hashing, digital signature, Message Authentication Code etc. and then proceeds to prescribe the cryptographic controls.

B) Scope

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

C) Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above

Chapter 1 - Overview

Introduction

In order to ensure that the Network Element is safe to connect to 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, Message authentication Code, Random bit generators etc.

1. **Symmetric Key encryption and decryption:** A cryptographic algorithm that uses the same secret key for its operation and, if applicable, for reversing the effects of the operation (e.g., an AES key for encryption and decryption).
   AES 128, 192, 256 and Three-key TDEA are the existing symmetric encryption and decryption mechanisms. However, as per NIST SP 800-131A publication, encryption using three-key TDEA is deprecated through December 31, 2023. The Table 1 in Chapter 2 lists the latest algorithms in force.

2. **Asymmetric Key encryption and decryption:** A cryptographic algorithm that uses two separate keys to exchange data, one to encrypt or digitally sign the data and one for decrypting the data or verifying the digital signature. It is also known as public key cryptography.
   For asymmetric encryption, RSA with key size ≥ 2048 bits is in legacy and the RSA modulus length should be increased to at least 3072 bits by the end of 2023 as mentioned by Global Platform paper and NIST Special Publication 800-57 P1R5.

3. **Key Exchange:** The process of exchanging public keys (and other information) in order to establish secure communications. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of the mechanisms and protocols associated with the keys, and the protection afforded by the keys. All keys need to be protected against unauthorized substitution and modification. Secret and private keys need to be protected against unauthorized disclosure. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.
   In key exchange, for a period of use beyond 2023, Diffie-Hellman with key size of 3072 bits should be used as per BSI and NIST Special Publication 800-57 Part 1 Revision 5. RSA with key size ≥ 2048 bits is in legacy and the RSA modulus length should be increased to at least 3072 bits by the end of 2023 as mentioned by Global Platform

paper and in NIST Special Publication 800-57 P1R5. ECDH with key size of at least 256 bits and above should be used as suggested by Global Platform and BSI.

4. **Digital Signature:** Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. Signature generation uses a private key to generate a digital signature; signature verification uses a public key that corresponds to, but is not the same as, the private key. Each signatory possesses a private and public key pair. Public keys may be known by the public; private keys are kept secret. Anyone can verify the signature by employing the signatory's public key. Only the user that possesses the private key can perform signature generation.
   For digital signature, DSA is no longer approved for digital signature generation as specified in FIPS 186-5. RSA with key size ≥ 2048 bits is in legacy and the RSA modulus length should be increased to at least 3072 bits by the end of 2023 as mentioned by Global Platform paper and NIST Special Publication 800-57 P1R5. For ECDSA, as mentioned in NIST Special Publication 800-57 Part 1 Revision 5, ECC keys in the range of 224 to 255 bits are weak and vulnerable to attack by modern standards by 2023. It is recommended to use ECDSA keys with a size of at least 256 bits for secure communication.

5. **HASH:** A cryptographic hash algorithm (alternatively, hash "function") is designed to provide a random mapping from a string of binary data to a fixed-size "message digest" and achieve certain security properties. Hash algorithms can be used for digital signatures, message authentication codes, key derivation functions, pseudo random functions, and many other security applications. Hash functions are used in the generation and verification of digital signatures, for key derivation, for random number generation, in the computation of message authentication codes and for hash-only applications.
   SHA2-224, SHA2-256, SHA2-384, SHA2-512/224, SHA2-512/256, SHA3-224 and above are recommended as per NIST Special Publication 800-131 A Revision 2 of March 2019,

6. **MAC:** A family of secret-key cryptographic algorithms acting on input data of arbitrary length to produce an output value of a specified length (called the MAC of the input data). The MAC can be employed to provide an authentication of the origin of data and/or data-integrity protection.
   HMAC, CMAC, GMAC with Key length of 128 bits and above is recommended by BSI and tag length for CMAC and GMAC should be greater than 96 bits. However, for HMAC the recommended tag length should be at least 128 bits as per NIST 800-131A Revision 2, ANSSI and BSI documents.

7. **Random Bit Generator:** A random bit generator that includes a DRBG algorithm and (at least initially) has access to a source of randomness is known to be Deterministic Random Bit Generator (DRBG). The DRBG produces a sequence of bits from a secret

initial value called a seed. A cryptographic DRBG has the additional property that the output is unpredictable given that the seed is not known. A DRBG is sometimes also called a Pseudo-Random Number Generator (PRNG) or a deterministic random number generator.
Hash_DRBG, HMAC_DRBG and CTR_DRBG are approved by NIST in NIST Special Publication 800-90A Revision 1 and ITSP 40.111 Canadian centre for cyber security paper. The Random bit generators size depends on the application and the intended use of the DRBG.

8. **Modes of Operation:** An algorithm that uses a block cipher algorithm as a cryptographic primitive to provide a cryptographic service, such as confidentiality or authentication. A confidentiality mode of operation of the block cipher algorithm consists of two processes that are inverses of each other: encryption and decryption. Encryption is the transformation of a usable message, called the plaintext, into an unreadable form, called the ciphertext; decryption is the transformation that recovers the plaintext from the ciphertext.
CBC and CTR are approved by NIST in NIST Special Publication 800-38A. Global Platform and BSI suggests use of CBC or CTR as mode of operation. CCM and GCM are approved as per NIST in NIST Special Publication 800-38D and recommended by Global Platform, BSI and ANSSI.

Various standard documents available in the above domains are studied in developing this ITSAR. It is observed that various versions of the cryptographic protocols were considered as legacy and were deprecated by the end of December 2023. Hence, it is proposed to revise the ITSAR and the updated cryptographic controls table is recommended in Chapter 2.

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.

Chapter 2 - List of Cryptographic Controls

TABLE 1

Sl. 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-3072 and above		
3	Key Exchange	Diffie-Hellman-3072 and above RSA-3072 and above ECDH-256 and above		
4	Digital Signature	ECDSA 256 and above RSA-3072 and above EdDSA-256 and above		
5	HASH	SHA2-224, SHA2-256, SHA2-384, SHA2-512/224, SHA2-512/256 SHA3-224 and above		
6	MAC	Algorithm	Key Length	Tag Length
		HMAC	≥128 bits	≥128 bits
		CMAC	≥128 bits	≥96 bits
		GMAC	≥128 bits	≥96 bits
7	Random Bit Generators	HASH_DRBG, HMAC_DRBG, CTR_DRBG		
8	Modes Of Operation	CTR, CBC, GCM, CCM		

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

Note: The above Table 1 of Cryptographic controls shall be effective from 01.01.2025.

Annexure I

Definitions

1) **Advanced Encryption Standard (AES):** The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) digital information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

2) **Cipher-based message authentication code (CMAC):** A message authentication code (MAC) algorithm that is based on a symmetric key block cipher. CMAC is appropriate for information systems in which an approved block cipher is more readily available than an approved hash function. CMAC is based on an approved symmetric key block cipher, such as the Advanced Encryption Standard. CMAC can be considered a mode of operation of the block cipher.

3) **Cipher Block Chaining (CBC):** The Cipher Block Chaining (CBC) mode is a confidentiality mode whose encryption process features the combining ("chaining") of the plaintext blocks with the previous cipher text blocks. The CBC mode requires an Initialization Vector to combine with the first plaintext block. The IV need not be secret, but it must be unpredictable.

4) **Counter with Cipher Block Chaining Mode (CCM):** CCM is based on an approved symmetric key block cipher algorithm whose block size is 128 bits, such as the Advanced Encryption Standard (AES) algorithm. CCM consists of two related processes: generation-encryption and decryption-verification, which combine two cryptographic primitives: counter mode encryption and cipher block chaining-based authentication. Only the forward cipher function of the block cipher algorithm is used within these primitives.

5) **Counter Mode (CTR):** The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the cipher text, and vice versa.

6) **CTR_DRBG:** CTR_DRBG is a Cryptographically Secure Pseudorandom Bit Generator that is used for generating sensitive data such as encryption keys. The implementation uses the AES-256 block cipher and derivation function to generate random bytes.

7) **Diffie-Hellman:** A method used to securely exchange or establish secret keys across an insecure network. Ephemeral Diffie-Hellman is used to create temporary or single-use secret keys.

8) **Edwards-curve Digital Signature Algorithm (EdDSA):** EdDSA is a variant of the Digital Signature Algorithm protocol using Edwards-curve cryptography having two curves Edwards25519 and Edwards448.

9) **Elliptic-curve Diffie–Hellman (ECDH):** ECDH is a key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret. It is a variant of the Diffie–Hellman protocol using elliptic-curve cryptography.

10) **Elliptic Curve Digital Signature Algorithm (ECDSA):** A digital signature algorithm that is an analogue of DSA using elliptic curves. A variant of ECDSA with a deterministic signature generation procedure is known as deterministic ECDSA.

11) **Galois/Counter Mode (GCM):** Galois/Counter Mode (GCM) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption. It can be implemented in hardware to achieve high speeds with low cost and low latency. Software implementations can achieve excellent performance by using table-driven field operations. It uses mechanisms that are supported by a well-understood theoretical foundation, and its security follows from a single reasonable assumption about the security of the block cipher.

12) **Galois Message Authentication Code (GMAC):** If the GCM input is restricted to data that is not to be encrypted, the resulting specialization of GCM, called GMAC, is simply an authentication mode on the input data.

13) **Hash-based message authentication code (HMAC):** Message authentication is achieved via the construction of a message authentication code (MAC). MACs based on cryptographic hash functions are known as HMACs. The purpose of a MAC is to authenticate both the source of a message and its integrity without the use of any additional mechanisms. An HMAC function is used by the message sender to produce a value (the MAC) that is formed by condensing the secret key and the message input. The MAC is typically sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key and HMAC function as were used by the sender, and compares the result computed with the received MAC. If the two values match, the message has been correctly received, and the receiver is assured that the sender is a member of the community of users that share the key.

14) **HASH_DRBG:** HASH_DRBG is a deterministic random bit generator using HASH specified in NIST SP 800-90. HASH_DRBG is a pseudorandom bit generator if HASH is a pseudorandom function.

15) **HMAC_DRBG:** HMAC_DRBG is a deterministic random bit generator using HMAC specified in NIST SP 800-90. HMAC_DRBG is a pseudorandom bit generator if HMAC is a pseudorandom function.

16) **Rivest, Shamir and Adelman (RSA):** A public-key algorithm that is used for key establishment and the generation and verification of digital signatures.

17) **Secure Hash Algorithm (SHA):** The Secure Hash Algorithm defined in Federal Information Processing Standard 180-1 as a hash algorithm with the property that it

is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.

Annexure II

Acronyms

AES	-	Advanced Encryption Standard
CBC	-	Cipher Block Chaining
CCM	-	CBC (Cipher Block Chaining) counter mode
CMAC	-	Cipher-based message authentication code
CTR	-	Counter Mode
CTR_DRBG	-	CTR-based Deterministic Random Bit Generator
DH	-	Diffie-Hellman
DRBG	-	Deterministic Random Bit Generator
DOT	-	Department of Telecommunications
DSA	-	Digital Signature Algorithm
DTLS	-	Datagram Transport Layer Security
ECDSA	-	Elliptical curved Digital Signature Algorithm
ECDH	-	Elliptic-curve Diffie–Hellman
EdDSA	-	Edwards-curve Digital Signature Algorithm
GCM	-	Galois counter mode
GMAC	-	Galois Message Authentication Code
HMAC	-	Hash-based message authentication code
HASH_DRBG	-	Hash-based Deterministic Random Bit Generator
HMAC_DRBG	-	HMAC-based Deterministic Random Bit Generator
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
TDEA	-	Triple Data Encryption Algorithm
TLS	-	Transport Layer Security

Annexure III

References

1. NIST Special Publication 800-38D "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", November 2007.
2. NIST Special Publication 800-56A Revision 3 "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography", April 2018.
3. NIST Special Publication 800-57 Part 1 Revision 5 "Recommendation for Key Management", May 2020.
4. NIST Special Publication 800-131A Revision 2, "Transitioning the Use of Cryptographic Algorithms and Key Lengths", March 2019.
5. NIST Special Publication 800-56B Revision 2, "Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography", March 2019.
6. NIST Special Publication 800-57 Part 3 Revision 1, "Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance" January 2015.
7. NIST Special Publication 800-38A, "Recommendation for Block 2001 Edition Cipher Modes of Operation", December 2001.
8. NIST Special Publication 800-38E, "Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices" January 2010.
9. NIST Special Publication 800-90A Revision1, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", June 2015.
10. NIST FIPS-186-5, "Digital Signature Standard", February 3, 2023.
11. NIST publication 800-52 Revision 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations", August 2019.
12. NIST FIPS 197, "Advanced Encryption Standard", May 9, 2023.
13. NIST – CISA Defend Today, "Cybersecurity Framework Implementation Guidance", November 2023.
14. NIST IR.8459 Report on the Block Cipher Modes of Operation in the NIST SP 800-38 Series, March 2023.
15. ITSP.40.111 - Canadian Centre for Cyber Security September 2022, Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information Revision 2.
16. H2020-ICT-2014 – Project 645421 of 2018, ECRYPT – CSA Algorithms, Key Size and Protocols Report.
17. Global Platform Technical Note Crypto Algorithm Recs v2.0 Public Release June 2021
18. BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths dated January 9, 2023.
19. ANSSI "Algorithms Selection Guide Cryptographic", March 2021, https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf summary at: https://www.keylength.com/en/5/.