International Standard

ISO/IEC 20648

Information technology — TLS specification for storage systems

Technologies de l'information — Spécification TLS pour systèmes de stockage

Second edition
2024-07

Reference number
ISO/IEC 20648:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by SNIA (as TLS Specification for Storage Systems, Version 2.1) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

This second edition cancels and replaces the first edition (ISO/IEC 20648:2016), which has been technically revised.

The main changes are as follows:

— a statement has been added regarding the relevance of ISO/IEC 20648 to Datagram Transport Layer Security (DTLS) implementations;

— a statement has been added regarding quantum computing and TLS;

— a statement has been added encouraging the use of TLS 1.3;

— a recommendation has been added to guard against replay attacks on zero round-trip time (0-RTT) for TLS version 1.3;

— the recommended cipher suites have been aligned with the RFC 7525 recommendations on forward secrecy;

— the requirements concerning 112 bits of security strength have been changed to 128 bits of security strength;

— the requirements for the maximum certificate validity period have been changed from 3 years to 398 days;

— the requirements associated with the ECDSA signature certificate have been clarified;

— a requirement has been added for including the TLS 1.3 extension for pre-shared key (PSK) support.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Within information and communications technology, one of the best defences against telecommunications attacks is to deploy security services implemented with mechanisms specified in standards that are thoroughly vetted in the public domain and rigorously tested by third party laboratories, by vendors, and by users of commercial off-the-shelf products. Three services that most often address network user security requirements are confidentiality, message integrity and authentication.

The Internet Engineering Task Force (IETF) with its Transport Layer Security (TLS) has a standard that supports preventing tampering, message forgery, and eavesdropping by encrypting data units, or segments, from one end of the transport layer to the other. In addition, TLS is application protocol independent, which means higher-level protocols like the Hypertext Transfer Protocol (HTTP) can layer on top of the TLS protocol transparently.

Additional details beyond the basic TLS protocol specification are necessary to ensure both security and interoperability. This document provides detail in the form of specific requirements and guidance for using TLS in conjunction with storage systems.

Information technology —TLS specification for storage systems

1 Scope

This document details the requirements for use of the Transport Layer Security (TLS) protocol in conjunction with data storage technologies. The requirements set out in this document are intended to facilitate secure interoperability of storage clients and servers as well as non-storage technologies that may have similar interoperability needs.

This document is relevant to anyone involved in owning, operating or using data storage devices. This includes senior managers, acquirers of storage products and service, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security and/or storage security, storage operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design and implementation of the architectural aspects of storage security.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, May 2008

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, IETF, August 2008

IETF RFC 5746, *Transport Layer Security (TLS) Renegotiation Indication Extension*, IETF, February 2010

IETF RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3*, IETF, August 2018

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1
cipher suite
named combination of authentication, encryption, and message authentication code algorithms used to negotiate the security settings for a network connection

Note 1 to entry: Cipher suites are typically used with the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) network protocols.

3.2
digital certificate
data structure signed with a digital signature that is based on a public key and which asserts that the key belongs to a subject identified in the structure

3.3
perfect forward secrecy
security condition in which a leaving entity cannot obtain any subsequent shared secret keys

[SOURCE: ISO/IEC 11770-5:2011, 3.24]

3.4
proxy
intermediary that acts as both a server and a client for the purpose of making requests on behalf of other clients

3.5
self-signed certificate
digital certificate (3.2) that is signed by the same entity whose identity it certifies

Note 1 to entry: A self-signed certificate is one signed with its own private key.

3.6
security strength
number associated with the amount of work that is required to break a cryptographic algorithm or system and specified in bits such that security strength *s* bits implies the required number of operations is 2^s

Note 1 to entry: Common values of security strength are 80, 112, 128, 192, and 256.

[SOURCE: ISO/IEC 9797-2:2021, 3.13, modified — Note to entry 1 has been replaced.]

4 Symbols and abbreviated terms

AEAD	Authenticated Encryption with Additional Data
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
CA	certificate authority
CBC	cipher block chaining
CDMI	Cloud Data Management Interface
CRL	certificate revocation list
DER	distinguished encoding rules
DHE	Ephemeral Diffie-Hellman
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECDHE	Elliptic Curve Ephemeral Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm

GCM	Galois/Counter Mode
HKDF	HMAC key derivation function
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	message authentication code
MD5	Message Digest 5
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
PKCS	Public-Key Cryptography Standards
PKI	public key infrastructure
PRF	pseudorandom function
PSK	pre-shared key
RFC	Request For Comment
RSA	Rivest, Shamir, and Adelman algorithm
SHA	Secure Hash Algorithm
SMI-S	Storage Management Initiative – Specification
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security

5 Overview and concepts

5.1 General

Data storage systems and infrastructure increasingly use technologies such as protocols over TCP/IP to manage the systems and data as well as to access the data. In many situations, the historical reliance on isolated connectivity, specialized technologies, and the physical security of data centers are not sufficient to protect data, especially when the data is considered sensitive and/or high value. Thus, there is a need to include security at the transport layer and at the same time, ensure interoperability.

The objectives for this document are to:

— Specify the TLS elements necessary to secure storage management and data access

— Facilitate timely updates and enhancements to the security for the storage specifications

— Ensure storage clients and systems can interoperate securely

— Support non-storage technologies that may have similar TLS interoperability needs

While many elements of this document can be relevant to Datagram Transport Layer Security (DTLS), no provisions have been added to address DTLS conformance.

5.2 Storage specifications

As a starting point, the original TLS requirements described herein were extracted from the following specifications:

— ISO/IEC 17826:2012, Information technology — Cloud Data Management Interface (CDMI)

— SNIA Storage Management Initiative – Specification (SMI-S), Version 1.6.1

These original requirements were then harmonized, eliminating minor differences.

5.3 Overview of TLS

5.3.1 TLS background

TLS is a protocol that provides communications security over networks. It allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. TLS is layered on top of a reliable transport protocol (e.g., TCP), and it is used for encapsulation of various higher-level protocols (e.g., HTTP).

Version 1.2 of TLS is specified in IETF RFC 5246. The more recent version 1.3 of TLS is specified in IETF RFC 8446. Earlier, and less secure, versions of TLS are also specified and in use; TLS versions 1.0 is specified in IETF RFC 2246, and TLS versions 1.1 is specified in IETF RFC 4346. The predecessor to TLS, The Secure Sockets Layer (SSL), and in particular, version 3.0 is also in use, but also considered less secure; SSL 3.0 is documented in the historical IETF RFC 6101, *The Secure Sockets Layer (SSL) Protocol Version 3.0*.

5.3.2 TLS functionality

TLS provides endpoint authentication and communications privacy over the network using cryptography. Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (whether an individual or an application) has a measure of assurance with whom they are communicating. Mutual authentication (the identities of both endpoints are verified) requires, with few exceptions, the deployment of digital certificates on the client.

TLS involves three basic phases:

— Peer negotiation for algorithm support

— Key exchange and authentication

— Symmetric cipher encryption and message authentication

During the first phase, the client and server negotiate cipher suites (see 5.3.3), which determine the ciphers to be used, the key exchange, authentication algorithms, and the Message Authentication Codes (MACs). The key exchange and authentication algorithms are typically public key algorithms. The MACs are made up from a keyed-Hash Message Authentication Code (HMAC).

5.3.3 Summary of cipher suites

TLS cipher suite names consist of a set of mnemonics separated by underscores (i.e., "_"). A registered[1] 16-bit (4 hexadecimal digit) number, called the cipher suite index, is assigned for each defined cipher suite. The naming convention in TLS 1.3 differs from the convention shared in TLS 1.0, 1.1, and 1.2. In all TLS cipher suites, the first mnemonic is the protocol name (i.e., "TLS"). Cipher suite names in TLS 1.0. 1.1, and 1.2 have the following form:

TLS_*KeyExchangeAlg*_WITH_*EncryptionAlg_MessageAuthenticationAlg*

where:

KeyExchangeAlg consists of one (e.g., RSA, PSK, etc.) or two (e.g., ECDHE_ECDSA) mnemonics.

EncryptionAlg indicates the symmetric encryption algorithm and associated mode of operations.

MessageAuthenticationAlg is generally the hashing algorithm to be used for HMAC, if applicable.

The following examples illustrate how to interpret the cipher suite names:

— TLS_DHE_RSA_WITH_AES_256_CBC_SHA256: Ephemeral DH is used for the key exchange. The server's ephemeral public key is authenticated using the server's RSA public key. Once the handshake is completed, the messages are encrypted using AES-256 in CBC mode. SHA-256 is used for both the PRF and HMAC computations.

— TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384: Ephemeral ECDH is used for the key exchange. The server's ephemeral public key is authenticated using the server's ECDSA public key. Once the handshake is completed, the messages are encrypted and authenticated using AES-256 in GCM mode, and SHA-384 is used for the PRF. Since an authenticated encryption mode is used, messages neither have nor require an HMAC message authentication code.

TLS 1.3 cipher suites have the following form:

TLS_*AEAD_HASH*

where:

AEAD indicates the AEAD algorithm that is used for confidentiality, integrity, and message authentication.

HASH indicates the hashing algorithm that is used with the HKDF during key derivation.

The following examples illustrate how to interpret TLS 1.3 cipher suite names:

— TLS_AES_256_GCM_SHA384: Messages are encrypted and authenticated with AES-256 in GCM mode, and SHA-384 is used with the HKDF.

— TLS_AES_128_CCM_SHA256: Messages are encrypted and authenticated with AES-128 in CCM mode, and SHA-256 is used with the HKDF.

The negotiation of the key exchange method is handled elsewhere in the TLS 1.3 handshake.

[1] The Internet Assigned Numbers Authority (IANA) documents registries and important TLS parameters, which can be found at: https://www.iana.org/assignments/tls-parameters/tls-parameters.xml.