INTERNATIONAL STANDARD

ISO/IEC 20648

First edition
2016-03-01

Information technology — TLS specification for storage systems

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

Reference number
ISO/IEC 20648:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

ISO/IEC 20648 was prepared by the Storage Networking Industry Association (SNIA) [as TLS Specification for Storage Systems, Version 1.0.1] and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by the national bodies of ISO and IEC. The content of ISO/IEC 20648 and SNIA TLS Specification for Storage Systems Version 1.0.1 is identical.

Introduction

Within Information and Communications Technology (CT), one of the best defenses 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 is able to prevent 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 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 specification provides that detail in the form of specific requirements and guidance for using Transport Layer Security (TLS) in conjunction with storage systems.

Information technology — TLS specification for storage systems

1 Scope

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

This specification is relevant to anyone involved in owning, operating or using data storage devices. This includes senior managers, acquirers of storage product 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 referenced documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, 2008

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

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

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
a number associated with the amount of work (i.e. the number of operations) that is required to break a cryptographic algorithm or system

Note 1 to entry: Security strength is specified in bits, and is a specific value from the set {80, 112, 128, 192, 256}. A security strength of b bits means that of the order of 2^b operations are required to break the system.

[SOURCE: ISO/IEC 9797-2:2011, 3.14]

4 Symbols and abbreviated terms

3DES	Triple Data Encryption Standard
AED	Authenticated Encryption with Additional Data
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CDMI	Cloud Data Management Interface
CRL	Certificate Revocation List
CRLDP	CRL Distribution Point
DER	Distinguished Encoding Rules
DHE	Ephemeral Diffie-Hellman
DSA	Digital Signature Algorithm
ECDHE	Elliptic Curve Ephemeral Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDE	Encryption-Decryption-Encryption
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
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
PSK	Pre-Shared Key
RFC	Request For Comment
RSA	Rivest, Shamir, and Adelman algorithm
SHA	Secure Hash Algorithm
SMI-S	Storage Management Initiative – Specification
SNIA	Storage Networking Industry Association
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 Transport Layer Security (TLS) and its predecessor, the Security Socket Layer (SSL), have been used successfully to protect a wide range of communications over TCP/IP. Recognizing this fact, the storage industry has mandated the use of TLS/SSL in conjunction with the Hypertext Transfer Protocol (HTTP) for multiple specifications (see 5.2). Unfortunately, these storage specifications tend to be lengthy and complex, resulting in long development cycles that don't allow for rapid requirements changes due to security vulnerabilities or new attacks.

The objectives for this specification 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

5.2 Storage specifications

As a starting point, the TLS requirements were extracted from the following specification:

- ISO/IEC 17826:2012, Information technology — Cloud Data Management Interface (CDMI)
- Storage Networking Industry Association (SNIA), Storage Management Initiative – Specification (SMI-S), Version 1.6.1

These requirements were then harmonized, eliminating minor differences. The resulting requirements (see clause 6) have been updated to reflect the current state of TLS and attack mitigation strategies.