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/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols and abbreviated terms 2
5 Overview and concepts 3
5.1 General 3
5.2 Storage specifications 4
5.3 Overview of TLS 4
5.3.1 TLS background 4
5.3.2 TLS functionality 4
5.3.3 Summary of cipher suites 5
5.3.4 X.509 digital certificates 6
5.3.5 Quantum computing and TLS 7
6 Requirements 7
6.1 TLS protocol requirements 7
6.2 Cipher suites 7
6.2.1 Required cipher suites for interoperability with TLS 1.2 7
6.2.2 Recommended cipher suites for enhanced security with TLS 1.2 8
6.2.3 Recommended cipher suites and extensions with TLS 1.3 9
6.3 Digital certificates 9
6.3.1 Certificate profile requirements 9
6.3.2 Certificate validity and path validation requirements 10
6.3.3 Certificate encoding requirements 10
6.4 Compression methods 10
7 Guidance for the implementation and use of TLS in data storage 11
7.1 Digital certificates 11
7.1.1 Certificate model 11
7.1.2 Chain of trust 11
7.1.3 Certificate lifecycle 11
7.1.4 Revocation 11
7.2 Security awareness 12
7.3 Cipher suites 12
7.4 Using TLS with HTTP 12
7.5 Use of pre-shared keys 12
Bibliography 14

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved