BS ISO/IEC 20648:2016

BSI Standards Publication

Information technology — TLS specification for storage systems

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 20648:2016.

The UK participation in its preparation was entrusted to Technical Committee ICT/-/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 89890 7

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2016.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20648:2016

BS ISO/IEC 20648:2016

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)

AVA Documents
Document Sharing Hub
© ISO/IEC 2016

Full document details: BS ISO/IEC 20648:2016

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20648:2016

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 ... 3
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 ... 4
5.3.4 X.509 digital certificates ... 5
6 Requirements ... **5**
6.1 TLS protocol requirements ... 5
6.2 Cipher suites ... 6
6.2.1 Required cipher suites for interoperability ... 6
6.2.2 Recommended cipher suites for enhanced security ... 6
6.3 Digital certificates ... 7
7 Guidance for the implementation and use of TLS in data storage ... **7**
7.1 Digital certificates ... 7
7.1.1 Certificate model ... 7
7.1.2 Chain of trust ... 8
7.1.3 Certificate lifecycle ... 8
7.1.4 Revocation ... 8
7.2 Security awareness ... 8
7.3 Cipher suites ... 9
7.4 Using TLS with HTTP ... 9
7.5 Use of pre-shared keys ... 9
Bibliography ... **11**

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20648:2016

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.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20648:2016

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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20648:2016