ISO/IEC 14776-481

Edition 1.0 2019-12

INTERNATIONAL STANDARD

colour inside

Information technology – Small Computer System Interface (SCSI) – Part 481: Security features for SCSI commands (SFSC)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.200

ISBN 978-2-8322-7663-1

ISO/IEC 14776-481

Information technology - Small Computer System Interface (SCSI) - Part 481: Security features for SCSI commands (SFSC)

Reference
ISO/IEC 14776-481

Contents

Figures

Tables

INFORMATION TECHNOLOGY – SMALL COMPUTER SYSTEM INTERFACE (SCSI) –

Part 481: Security features for SCSI commands (SFSC)

FOREWORD

1) 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.
2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.
3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.
8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 14776-481 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of the ISO/IEC 14776 series, under the general title *Information technology – Small computer system interface (SCSI)*, can be found on the IEC and ISO web sites.

The text of this standard is based on the following documents:

CDV	Report on voting
JTC1-SC25/2845/CDV	JTC1-SC25/2871/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2, except as described in 3.4 and 3.5.

A bilingual version of this publication may be issued at a later date.

IMPORTANT - The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

ISO/IEC 14776 (all parts) provides for many different commands that define device models and commands for different SCSI devices. This document defines security features for use by all SCSI devices. This document defines the security model that is basic to every device model and the parameter data that may apply to any device model.

Figure 1 shows the relationship of this document to the other documents and related projects in the SCSI family of standards.

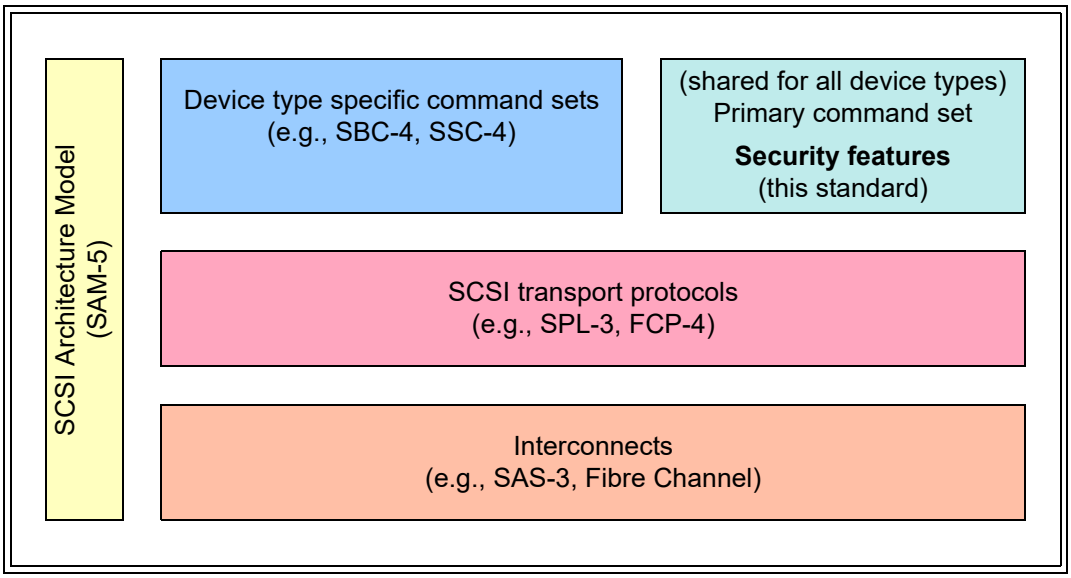

Figure 1 — SCSI document structure

The SCSI document structure in figure 1 shows the general applicability of the documents to one another. Figure 1 is not intended to imply a relationship such as a hierarchy, protocol stack, or system architecture.

The term SCSI is used to refer to ISO/IEC 14776 (all parts).

These documents specify the interfaces, functions and operations necessary to ensure interoperability between conforming implementations. This document contains a functional description. Conforming implementations employ any design technique that does not violate interoperability.

INFORMATION TECHNOLOGY – SMALL COMPUTER SYSTEM INTERFACE (SCSI) –

Part 481: Security features for SCSI commands (SFSC)

1 Scope

ISO/IEC 14776 (all parts) provides for many different types of SCSI devices (e.g., disks, tapes, media changers). This part of ISO/IEC 14776 defines a device model that is applicable to all SCSI devices. Other command standards expand on the general SCSI device model in ways appropriate to specific types of SCSI devices.

ISO/IEC 14776 (all parts) specifies the interfaces, functions, and operations necessary to ensure interoperability between conforming SCSI implementations. This document is a functional description. Conforming implementations employ any design technique that does not violate interoperability.

This document defines security features for use by all SCSI devices. This document defines the security model that is basic to every device model and the parameter data that applies to any device model. For additional information on the security goals and threat model discussed in this document see Annex A.

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 14776-415, *Information Technology – Small computer system interface (SCSI) - Part 415: SCSI Architecture Model - 5 (SAM-5)*

ISO/IEC 10646:2017, *Information technology - Universal Coded Character Set (UCS)*

INCITS 496-2012, *Information Technology - Fibre Channel - Security Protocols - 2 (FC-SP-2)*

INCITS 496-2012/AM1-2015, *Information Technology - Fibre Channel - Security Protocols - 2/Amendment 1 -(FC-SP-2/AM1)*

INCITS 502, *Information technology – SCSI Primary Commands - 5 (SPC-5)*

INCITS 516, *Information technology – SCSI Stream Commands - 4 (SSC-4)*

ANSI/IEEE 1619.1-2007, *Standard for Authenticated Encryption with Length Expansion for Storage Devices*

RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec* [1]

RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1* [1]

RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)* [1]

RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec* [1]

RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec* [1]

[1] Copies of the IETF RFCs may be obtained at http://www.ietf.org/.

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload* [1]

RFC 4309, *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload* [1]

RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)* [1]

RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)* [1]

RFC 6151, *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms* [1]

RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)* [1]

NIST SP (Special Publication) 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter (GCM) Mode for Confidentiality and Authentication and GMAC* [2]

FIPS 180-4, *Secure Hash Standard* [2]

FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)* [2]

[2] Copies of the NIST and FIPS standards may be obtained at http://csrc.nist.gov/publications/.