

INTERNATIONAL STANDARD



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

**(<https://standards.iteh.ai>)
Document Preview**

[ISO/IEC 14776-481:2019](https://standards.iteh.ai/catalog/standards/iso/efe7818c-49a5-4b0d-9f7b-622197e22fac/iso-iec-14776-481-2019)

<https://standards.iteh.ai/catalog/standards/iso/efe7818c-49a5-4b0d-9f7b-622197e22fac/iso-iec-14776-481-2019>



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2019 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 14776-481:2019](https://standards.iteh.ai/catalog/standards/iso/efe7818c-49a5-4b0d-9f7b-622197e22fac/iso-iec-14776-481-2019)

<https://standards.iteh.ai/catalog/standards/iso/efe7818c-49a5-4b0d-9f7b-622197e22fac/iso-iec-14776-481-2019>

INTERNATIONAL STANDARD



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

Document Preview

ISO/IEC 14776-481:2019

<https://standards.iteh.ai/catalog/standards/iso/efe7818c-49a5-4b0d-9f7b-622197e22fac/iso-iec-14776-481-2019>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.200

ISBN 978-2-8322-7663-1

Warning! Make sure that you obtained this publication from an authorized distributor.



**ISO/IEC
14776-481**

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

**iTeh Standards
(<https://standards.itih.ai>)
Document Preview**

[ISO/IEC 14776-481:2019](https://standards.itih.ai/catalog/standards/iso/efe7818c-49a5-4b0d-9f7b-622197e22fac/iso-iec-14776-481-2019)

<https://standards.itih.ai/catalog/standards/iso/efe7818c-49a5-4b0d-9f7b-622197e22fac/iso-iec-14776-481-2019>

Reference
ISO/IEC 14776-481

Contents

Page

FOREWORD.....	9
INTRODUCTION.....	11
1 Scope.....	12
2 Normative references.....	12
3 Terms and definitions, symbols, abbreviations, and conventions	14
3.1 Terms and definitions	14
3.2 Abbreviations and symbols.....	24
3.2.1 Abbreviations.....	24
3.2.2 Symbols.....	25
3.2.3 Mathematical operators	25
3.3 Keywords.....	25
3.4 Editorial conventions	27
3.5 Numeric and character conventions	27
3.5.1 Numeric conventions	27
3.5.2 Units of measure	28
3.5.3 Byte encoded character strings conventions.....	29
3.6 Bit and byte ordering	29
4 Security features model common to all device types.....	31
4.1 Security features for SCSI devices.....	31
4.1.1 Security associations.....	31
4.1.1.1 Principles of SAs.....	31
4.1.1.2 SA parameters.....	32
4.1.1.3 Creating an SA.....	34
4.1.2 Key derivation functions	35
4.1.2.1 KDFs overview	35
4.1.2.2 IKEv2-based iterative KDF	36
4.1.2.3 HMAC-based KDFs.....	36
4.1.2.4 AES-XCBC-PRF-128 IKEv2-based iterative KDF	38
4.1.3 Using IKEv2-SCSI to create an SA	38
4.1.3.1 Overview.....	38
4.1.3.2 IKEv2-SCSI Protocol summary	42
4.1.3.3 IKEv2-SCSI Authentication.....	44
4.1.3.3.1 Overview.....	44
4.1.3.3.2 Pre-shared key authentication.....	45
4.1.3.3.3 Digital signature authentication	46
4.1.3.3.3.1 Overview.....	46
4.1.3.3.3.2 Certificates and digital signature authentication	46
4.1.3.3.3.3 Example of certificate use for digital signature authentication.....	47
4.1.3.3.3.4 Handling of the Certificate Request payload and the Certificate payload	47
4.1.3.4 Constraints on skipping the Authentication step.....	47
4.1.3.4 Summary of IKEv2-SCSI shared keys nomenclature and shared key sizes	49
4.1.3.5 Device Server Capabilities step.....	50
4.1.3.6 IKEv2-SCSI Key Exchange step	52
4.1.3.6.1 Overview.....	52
4.1.3.6.2 Key Exchange step SECURITY PROTOCOL OUT command	52
4.1.3.6.3 Key Exchange step SECURITY PROTOCOL IN command	53
4.1.3.6.4 Key Exchange step completion	54
4.1.3.6.5 After the Key Exchange step	54
4.1.3.7 IKEv2-SCSI Authentication step.....	54

4.1.3.7.1 Overview.....	54
4.1.3.7.2 Authentication step SECURITY PROTOCOL OUT command	55
4.1.3.7.3 Authentication step SECURITY PROTOCOL IN command	56
4.1.3.8 Generating shared keys	57
4.1.3.8.1 Overview.....	57
4.1.3.8.2 Generating shared keys when the Authentication step is skipped	58
4.1.3.8.3 Generating shared keys when the Authentication step is processed	58
4.1.3.8.4 Initializing shared key generation	58
4.1.3.8.4.1 Initializing for SA creation shared key generation	58
4.1.3.8.4.2 Initializing for generation of shared keys used by the created SA.....	59
4.1.3.8.5 Generating shared keys used for SA management.....	59
4.1.3.8.6 Generating shared keys for use by the created SA.....	60
4.1.3.9 IKEv2-SCSI SA generation.....	61
4.1.3.10 Abandoning an IKEv2-SCSI CCS.....	62
4.1.3.11 Deleting an IKEv2-SCSI SA	63
4.1.4 Security progress indication	63
4.1.5 ESP-SCSI encapsulations for parameter data	64
4.1.5.1 Overview.....	64
4.1.5.2 ESP-SCSI required inputs	64
4.1.5.3 ESP-SCSI data format before encryption and after decryption	65
4.1.5.4 ESP-SCSI outbound data descriptors	66
4.1.5.4.1 Overview.....	66
4.1.5.4.2 ESP-SCSI CDBs or Data-Out Buffer parameter lists including a descriptor length.....	67
4.1.5.4.2.1 Initialization vector absent	67
4.1.5.4.2.2 Initialization vector present	68
4.1.5.4.3 ESP-SCSI Data-Out Buffer parameter lists for externally specified descriptor length.....	70
4.1.5.4.3.1 Initialization vector absent	70
4.1.5.4.3.2 Initialization vector present	71
4.1.5.5 ESP-SCSI Data-In Buffer parameter data descriptors	71
4.1.5.5.1 Overview.....	71
4.1.5.5.2 ESP-SCSI Data-In Buffer parameter data including a descriptor length	72
4.1.5.5.2.1 Initialization vector absent	72
4.1.5.5.2.2 Initialization vector present	74
4.1.5.5.3 ESP-SCSI Data-In Buffer parameter data for externally specified descriptor length.....	75
4.1.5.5.3.1 Initialization vector absent	75
4.1.5.5.3.2 Initialization vector present	76
4.1.6 Security algorithm codes	77
4.2 Secure random numbers	79
5 Security protocol parameters for all device types	80
5.1 Security protocol information description.....	80
5.1.1 Overview.....	80
5.1.2 CDB description.....	80
5.1.3 Supported security protocols list description	81
5.1.4 Certificate data description	82
5.1.4.1 Certificate overview	82
5.1.4.2 Public Key certificate description.....	82
5.1.4.3 Attribute certificate description	82
5.1.5 Security compliance information description	83
5.1.5.1 Security compliance information overview	83
5.1.5.2 Compliance descriptor overview.....	84
5.1.5.3 FIPS 140 compliance descriptor.....	85
5.2 SA creation capabilities	86
5.2.1 Overview.....	86
5.2.2 SA creation capabilities CDB description	86
5.2.3 SA creation capabilities parameter data formats.....	87
5.2.3.1 Supported device server capabilities formats parameter data format	87

5.2.3.2 IKEv2-SCSI device server capabilities parameter data format.....	88
5.3 IKEv2-SCSI	88
5.3.1 Overview.....	88
5.3.2 IKEv2-SCSI SECURITY PROTOCOL IN CDB description	89
5.3.3 IKEv2-SCSI SECURITY PROTOCOL OUT CDB description	90
5.3.4 IKEv2-SCSI parameter data format.....	91
5.3.5 IKEv2-SCSI payloads.....	98
5.3.5.1 IKEv2-SCSI payload format.....	98
5.3.5.2 No Next payload	99
5.3.5.3 Key Exchange payload.....	100
5.3.5.4 Identification – Application Client payload and Identification – Device Server payload.....	101
5.3.5.5 Certificate payload.....	102
5.3.5.6 Certificate Request payload	103
5.3.5.7 Authentication payload	104
5.3.5.8 Nonce payload.....	106
5.3.5.9 Notify payload	107
5.3.5.10 Delete payload.....	108
5.3.5.11 Encrypted payload.....	109
5.3.5.11.1 Combined mode encryption.....	109
5.3.5.11.2 Encrypted payload introduction	110
5.3.5.11.3 IKEv2-SCSI AAD	112
5.3.5.11.4 Processing a received Encrypted payload	113
5.3.5.12 IKEv2-SCSI SA Creation Capabilities payload.....	115
5.3.5.13 IKEv2-SCSI SA Cryptographic Algorithms payload.....	116
5.3.5.14 IKEv2-SCSI SAUT Cryptographic Algorithms payload	118
5.3.5.15 IKEv2-SCSI Timeout Values payload.....	119
5.3.6 IKEv2-SCSI cryptographic algorithm descriptors	120
5.3.6.1 Overview.....	120
5.3.6.2 ENCR IKEv2-SCSI cryptographic algorithm descriptor	122
5.3.6.3 PRF IKEv2-SCSI cryptographic algorithm descriptor	124
5.3.6.4 INTEG IKEv2-SCSI cryptographic algorithm descriptor	126
5.3.6.5 D-H IKEv2-SCSI cryptographic algorithm descriptor.....	127
5.3.6.6 IKEv2-SCSI authentication algorithm IKEv2-SCSI cryptographic algorithm descriptor.....	129
5.3.7 Errors in IKEv2-SCSI security protocol commands	131
5.3.8 Errors in IKEv2-SCSI security protocol parameter data	133
5.3.8.1 Overview.....	133
5.3.8.2 Errors with high denial of service attack potential	133
5.3.8.3 Errors with low denial of service attack potential.....	134
5.3.9 Translating IKEv2 errors.....	134
Annex A (informative) Security goals and threat model	136
A.1 Overview	136
A.2 Security goals.....	136
A.3 Threat model.....	137
A.4 Types of attacks	137
A.5 SCSI security considerations	138
Annex B (informative) Variations between this document and equivalent security protocols	139
B.1 IKEv2 protocol details and variations for IKEv2-SCSI.....	139
B.2 ESP protocol details and variations for ESP-SCSI	142
BIBLIOGRAPHY	143