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)

ISO/IEC 14776-481:2019-12(en)

IEC Central Office
3, rue de Varembé
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 It also gives information on projects, replaced and withdrawn publications.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.

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

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
4.1.3.3.4 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

Figures

Page
Figure 1 — SCSI document structure 11
Figure 2 — SA relationships 31
Figure 3 — IKEv2-SCSI Device Server Capabilities step 42
Figure 4 — IKEv2-SCSI Key Exchange step 42
Figure 5 — IKEv2-SCSI Authentication step 43
Figure 6 — IKEv2-SCSI Delete operation 44

Tables

Page
Table 1 — Numbering conventions examples ... 28
Table 2 — Comparison of decimal prefixes and binary prefixes ... 29
Table 3 — Minimum SA parameters ... 32
Table 4 — USAGE_TYPE SA parameter ... 34
Table 5 — Security protocols that create SAs ... 35
Table 6 — KDFs summary ... 36
Table 7 — HMAC-based KDFs ... 37
Table 8 — Hash functions used by HMAC based on KDF_ID ... 37
Table 9 — RFC 3566 parameter translations for the KDF based on AES-XCBC-PRF-128 ... 38
Table 10 — IKEv2-SCSI shared key names and SA shared key names ... 49
Table 11 — Shared key size determination ... 50
Table 12 — Device Server Capabilities step parameter data requirements ... 51
Table 13 — IKEv2-SCSI command terminations that do not abandon the CCS ... 62
Table 14 — ESP-SCSI data format before encryption and after decryption ... 65
Table 15 — ESP-SCSI outbound data descriptors ... 66
Table 16 — ESP-SCSI CDBs or Data-Out Buffer parameter list descriptor without initialization vector ... 67
Table 17 — ESP-SCSI CDBs or Data-Out Buffer full parameter list descriptor ... 69
Table 18 — ESP-SCSI Data-Out Buffer parameter list descriptor without length and initialization vector ... 70
Table 19 — ESP-SCSI Data-Out Buffer parameter list descriptor without length ... 71
Table 20 — ESP-SCSI Data-In Buffer parameter data descriptors ... 72
Table 21 — ESP-SCSI Data-In Buffer parameter data descriptor without initialization vector ... 72
Table 22 — ESP-SCSI Data-In Buffer full parameter data descriptor ... 74
Table 23 — ESP-SCSI Data-In Buffer parameter data descriptor without length and initialization vector ... 75
Table 24 — ESP-SCSI Data-In Buffer parameter data descriptor without length ... 76
Table 25 — Security algorithm codes ... 77
Table 26 — SECURITY PROTOCOL SPECIFIC field for SECURITY PROTOCOL IN protocol 00h ... 80
Table 27 — Supported security protocols SECURITY PROTOCOL IN parameter data ... 81
Table 28 — Certificate data SECURITY PROTOCOL IN parameter data ... 82
Table 29 — Security compliance information SECURITY PROTOCOL IN parameter data ... 83
Table 30 — Compliance descriptor format ... 84
Table 31 — COMPLIANCE DESCRIPTOR TYPE field ... 84
Table 32 — FIPS 140 compliance descriptor ... 85
Table 33 — RELATED STANDARD field ... 85
Table 34 — SECURITY PROTOCOL SPECIFIC field for the SA creation capabilities ... 87
Table 35 — Supported device server capabilities formats parameter data ... 87
Table 36 — IKEv2-SCSI device server capabilities parameter data ... 88
Table 37 — SECURITY PROTOCOL SPECIFIC field as defined by the IKEv2-SCSI SECURITY PROTOCOL IN command ... 89
Table 38 — SECURITY PROTOCOL SPECIFIC field as defined by the IKEv2-SCSI SECURITY PROTOCOL OUT command ... 90
Table 39 — IKEv2-SCSI SECURITY PROTOCOL OUT command and SECURITY PROTOCOL IN command parameter data ... 91
Table 40 — IKEv2-SCSI header checking of SAIs ... 93
Table 41 — NEXT PAYLOAD field ... 94
Table 42 — MESSAGE ID field ... 95
Table 43 — Next payload values in SECURITY PROTOCOL OUT/IN parameter data ... 96
Table 44 — IKEv2-SCSI payload format ... 98
Table 45 — Key Exchange payload format ... 100
Table 46 — Identification payload format ... 101
Table 47 — ID TYPE field ... 101
Table 48 — Certificate payload format ... 102
Table 49 — CERTIFICATE ENCODING field ... 102
Table 50 — Certificate Request payload format ... 103
Table 51 — Authentication payload format ... 104
Table 52 — Nonce payload format ... 106

Table 53 — Notify payload format 107
Table 54 — Delete payload format 108
Table 55 — Encrypted payload format 110
Table 56 — Plaintext format for Encrypted payload CIPHERTEXT field 112
Table 57 — IKEv2-SCSI SA Creation Capabilities payload format 115
Table 58 — IKEv2-SCSI SA Cryptographic Algorithms payload format 116
Table 59 — IKEv2-SCSI SAUT Cryptographic Algorithms payload format 118
Table 60 — IKEv2-SCSI Timeout Values payload format 119
Table 61 — IKEv2-SCSI cryptographic algorithm descriptor format 120
Table 62 — ALGORITHM TYPE field 121
Table 63 — ENCR IKEv2-SCSI cryptographic algorithm descriptor format 122
Table 64 — ENCR ALGORITHM IDENTIFIER field 123
Table 65 — PRF IKEv2-SCSI cryptographic algorithm descriptor format 124
Table 66 — PRF ALGORITHM IDENTIFIER field 125
Table 67 — INTEG IKEv2-SCSI cryptographic algorithm descriptor format 126
Table 68 — INTEG ALGORITHM IDENTIFIER field 126
Table 69 — D-H IKEv2-SCSI cryptographic algorithm descriptor format 127
Table 70 — D-H ALGORITHM IDENTIFIER field 128
Table 71 — SA_AUTH_OUT and SA_AUTH_IN IKEv2-SCSI cryptographic algorithm descriptor format 129
Table 72 — SA_AUTH_OUT and SA_AUTH_IN ALGORITHM IDENTIFIER field 130
Table 73 — IKEv2-SCSI command order processing requirements on a single I_T_L nexus 132
Table 74 — IKEv2-SCSI parameter error categories 133
Table 75 — IKEv2 Notify payload error translations for IKEv2-SCSI 135
Table B.1 — IKE payload names shorthand 141

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.

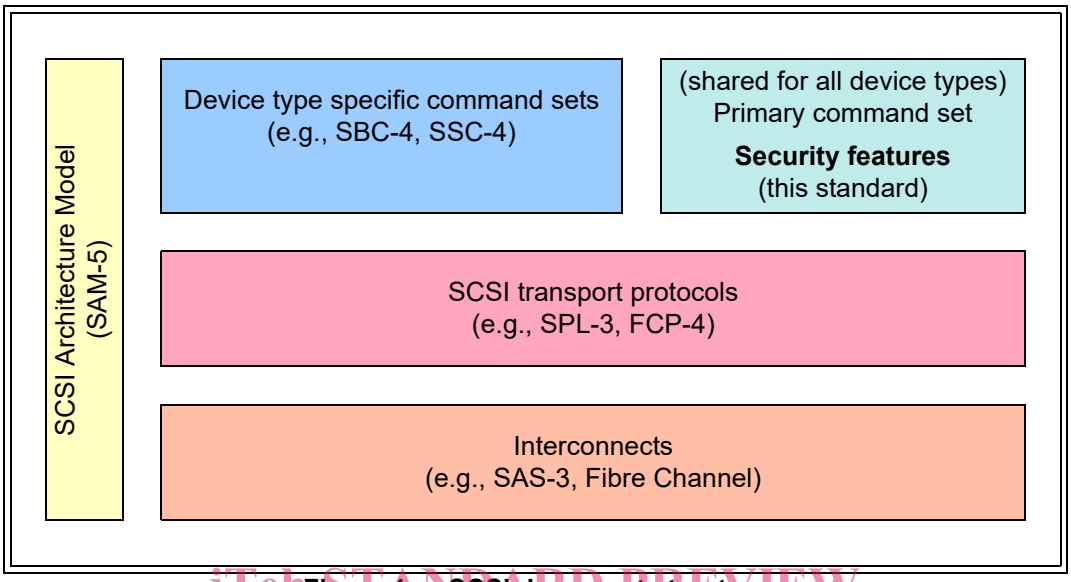

Figure 1 — SCSI document structure

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/.