



ISO/IEC 14165-432

Edition 1.0 2022-03

# INTERNATIONAL STANDARD



Information technology – Fibre channel –  
Part 432: Security Protocols – 2 (FC-SP-2)  
*STANDARD PREVIEW*  
(standards.iteh.ai)

[ISO/IEC 14165-432:2022](#)

<https://standards.iteh.ai/catalog/standards/sist/fcbefaf5-c0cb-475b-ad82-11ffb62cc7eb/iso-iec-14165-432-2022>





## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2022 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 Secretariat  
3, rue de Varembé  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://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](https://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 It also gives information on projects, replaced and withdrawn publications.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](https://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](https://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](mailto:sales@iec.ch).

#### IEC Products & Services Portal - [products.iec.ch](https://products.iec.ch)

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

#### Electropedia - [www.electropedia.org](https://www.electropedia.org)

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

## ISO/IEC 14165-432:2022

<https://standards.iteh.ai/catalog/standards/sist/fcbefaf5-c0cb-475b-ad82-11ffb62cc7eb/iso-iec-14165-432-2022>



ISO/IEC 14165-432

Edition 1.0 2022-03

# INTERNATIONAL STANDARD



---

iTeh STANDARD PREVIEW  
Information technology – Fibre channel –  
Part 432: Security Protocols – 2 (FC-SP-2)  
(standards.iteh.ai)

[ISO/IEC 14165-432:2022](#)

<https://standards.iteh.ai/catalog/standards/sist/fcbefaf5-c0cb-475b-ad82-11ffb62cc7eb/iso-iec-14165-432-2022>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

---

ICS 35.200

ISBN 978-2-8322-1084-0

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

<b>Contents</b>	<b>Page</b>
<b>FOREWORD .....</b>	<b>15</b>
<b>9 INTRODUCTION .....</b>	<b>17</b>
<b>1 Scope .....</b>	<b>18</b>
<b>2 Normative references .....</b>	<b>19</b>
<b>3 Terms, definitions, symbols, abbreviated terms, and conventions .....</b>	<b>23</b>
3.1 Terms and definitions .....	23
3.2 Symbols and abbreviated terms .....	30
3.3 Editorial conventions .....	31
3.4 Keywords .....	32
3.5 T10 Vendor ID .....	33
3.6 Sorting .....	33
3.6.1 Sorting alphabetic keys .....	33
3.6.2 Sorting numeric keys .....	34
3.7 Terminate communication .....	34
3.8 State machine notation .....	35
3.9 Using numbers in hash functions and concatenation functions .....	35
<b>4 Structure and Concepts .....</b>	<b>37</b>
4.1 Overview .....	37
4.2 FC-SP-2 Compliance .....	37
4.3 Fabric Security Architecture .....	37
4.4 Authentication Infrastructure .....	37
4.5 Authentication .....	38
4.6 Security Associations .....	39
4.7 Cryptographic Integrity and Confidentiality .....	39
4.7.1 Overview .....	39
4.7.2 ESP_Header Processing .....	40
4.7.3 CT_Authentication Processing .....	41
4.8 Authorization (Access Control) .....	43
4.8.1 Policy Definition .....	43
4.8.2 Policy Enforcement .....	43
4.8.3 Policy Distribution .....	44
4.8.4 Policy Check .....	44
4.9 Name Format .....	44
<b>5 Authentication Protocols .....</b>	<b>45</b>
5.1 Overview .....	45
5.2 Authentication Messages Structure .....	46
5.2.1 Overview .....	46
5.2.2 SW_ILS Authentication Messages .....	47
5.2.3 ELS Authentication Messages .....	48
5.2.4 Fields Common to All AUTH Messages .....	49
5.2.5 Vendor Specific Messages .....	50
5.3 Authentication Messages Common to Authentication Protocols .....	50
5.3.1 Overview .....	50
5.3.2 AUTH_Negotiate Message .....	51
5.3.3 Names used in Authentication .....	52
5.3.4 Hash Functions .....	53
5.3.5 Diffie-Hellman Groups .....	53
5.3.6 Accepting an AUTH_Negotiate Message .....	54

5.3.7 AUTH_Reject Message .....	54
5.3.8 AUTH_Done Message .....	57
5.4 DH-CHAP Protocol .....	58
5.4.1 Protocol Operations .....	58
5.4.2 AUTH_Negotiate DH-CHAP Parameters .....	60
5.4.3 DHCHAP_Challenge Message .....	61
5.4.4 DHCHAP_Reply Message .....	62
5.4.5 DHCHAP_Success Message .....	64
5.4.6 Key Generation for the Security Association Management Protocol .....	65
5.4.7 Reuse of Diffie-Hellman Exponential .....	65
5.4.8 DH-CHAP Security Considerations .....	65
5.5 FCAP Protocol .....	67
5.5.1 Protocol Operations .....	67
5.5.2 AUTH_Negotiate FCAP Parameters .....	70
5.5.3 FCAP_Request Message .....	71
5.5.4 FCAP_Acknowledge Message .....	74
5.5.5 FCAP_Confirm Message .....	76
5.5.6 Key Generation for the Security Association Management Protocol .....	76
5.5.7 Reuse of Diffie-Hellman Exponential .....	77
5.6 FCPAP Protocol .....	78
5.6.1 Protocol Operations .....	78
5.6.2 AUTH_Negotiate FCPAP Parameters .....	81
5.6.3 FCPAP_Init Message .....	82
5.6.4 FCPAP_Accept Message .....	83
5.6.5 FCPAP_Complete Message .....	83
5.6.6 Key Generation for the Security Association Management Protocol .....	84
5.6.7 Reuse of Diffie-Hellman Exponential .....	84
5.7 FCEAP Protocol .....	85
5.7.1 Protocol Operations .....	85
5.7.2 AUTH_Negotiate FCEAP Parameters .....	85
5.7.3 FCEAP_Request Message .....	86
5.7.4 FCEAP_Response Message .....	86
5.7.5 FCEAP_Success Message .....	87
5.7.6 FCEAP_Failure Message .....	87
5.7.7 AUTH_Reject Use .....	88
5.7.8 AUTH_ELS and AUTH_ILS Size Requirements .....	88
5.7.9 Supported EAP Methods .....	89
5.7.10 Key Generation for the Security Association Management Protocol .....	89
5.8 AUTH_ILS Specification .....	90
5.8.1 Overview .....	90
5.8.2 AUTH_ILS Request Sequence .....	91
5.8.3 AUTH_ILS Reply Sequence .....	92
5.9 B_AUTH_ILS Specification .....	92
5.9.1 Overview .....	92
5.9.2 B_AUTH_ILS Request Sequence .....	94
5.9.3 B_AUTH_ILS Reply Sequence .....	95
5.10 AUTH_ELS Specification .....	95
5.10.1 Overview .....	95
5.10.2 AUTH_ELS Request Sequence .....	97
5.10.3 AUTH_ELS Reply Sequence .....	98
5.10.4 AUTH_ELS Fragmentation .....	98
5.10.5 Authentication and Login .....	102
5.11 Re-Authentication .....	103
5.12 Timeouts .....	104

<b>6 Security Association Management Protocol .....</b>	<b>105</b>
6.1 Overview .....	105
6.1.1 General .....	105
6.1.2 IKE_SA_Init Overview .....	107
6.1.3 IKE_Auth Overview .....	107
6.1.4 IKE_Create_Child_SA Overview .....	108
6.2 SA Management Messages .....	108
6.2.1 General Structure .....	108
6.2.2 IKE_Header Payload .....	109
6.2.3 Chaining Header .....	110
6.2.4 AUTH_Reject Message Use .....	112
6.3 IKE_SA_Init Message .....	112
6.3.1 Overview .....	112
6.3.2 Security_Association Payload .....	113
6.3.3 Key_Exchange Payload .....	124
6.3.4 Nonce Payload .....	124
6.4 IKE_Auth Message .....	124
6.4.1 Overview .....	124
6.4.2 Encrypted Payload .....	126
6.4.3 Identification Payload .....	127
6.4.4 Authentication Payload .....	128
6.4.5 Traffic Selector Payload .....	128
6.4.6 Certificate Payload .....	130
6.4.7 Certificate Request Payload .....	131
6.5 IKE_Create_Child_SA Message .....	133
6.6 IKE_Informational Message .....	134
6.6.1 Overview .....	134
6.6.2 Notify Payload .....	136
6.6.3 Delete Payload .....	139
6.6.4 Vendor_ID Payload .....	140
6.7 Interaction with the Authentication Protocols .....	141
6.7.1 Overview .....	141
6.7.2 Concatenation of Authentication and SA Management Transactions .....	141
6.7.3 SA Management Transaction as Authentication Transaction .....	143
6.8 IKEv2 Protocol Details .....	144
6.8.1 Use of Retransmission Timers .....	144
6.8.2 Use of Sequence Numbers for Message_IDs .....	144
6.8.3 Overlapping Requests .....	145
6.8.4 State Synchronization and Connection Timeouts .....	145
6.8.5 Cookies and Anti-Clogging Protection .....	145
6.8.6 Cryptographic Algorithms Negotiation .....	145
6.8.7 Rekeying .....	145
6.8.8 Traffic Selector Negotiation .....	145
6.8.9 Nonces .....	146
6.8.10 Reuse of Diffie-Hellman Exponential .....	146
6.8.11 Generating Keying Material .....	146
6.8.12 Generating Keying Material for the IKE_SA .....	146
6.8.13 Authentication of the IKE_SA .....	146
6.8.14 Generating Keying Material for Child_SAs .....	147
6.8.15 Rekeying IKE_SAs using the IKE_Create_Child_SA exchange .....	147
6.8.16 IKE_Informational Messages outside of an IKE_SA .....	147
6.8.17 Error Handling .....	147
6.8.18 Conformance Requirements .....	147
6.8.19 Rekeying IKE_SAs when Refreshing Authentication .....	148

<b>7 Fabric Policies .....</b>	<b>149</b>
7.1 Policies Definition .....	149
7.1.1 Overview .....	149
7.1.2 Names used to define Policies .....	151
7.1.3 Policy Summary Object .....	153
7.1.4 Switch Membership List Object .....	154
7.1.5 Node Membership List Object .....	159
7.1.6 Switch Connectivity Object .....	163
7.1.7 IP Management List Object .....	164
7.1.8 Attribute Object .....	168
7.2 Policies Enforcement .....	170
7.2.1 Overview .....	170
7.2.2 Switch-to-Switch Connections .....	170
7.2.3 Switch-to-Node Connections .....	171
7.2.4 In-Band Management Access to a Switch .....	172
7.2.5 IP Management Access to a Switch .....	173
7.2.6 Direct Management Access to a Switch .....	174
7.2.7 Authentication Enforcement .....	175
7.3 Policies Management .....	175
7.3.1 Management Interface .....	175
7.3.2 Fabric Distribution .....	177
7.3.3 Relationship between Security Policy Server Requests and Fabric Actions ..	180
7.3.4 Policy Objects Support .....	180
7.3.5 Optional Data .....	184
7.3.6 Detailed Management Specification .....	185
7.4 Policies Check .....	193
7.4.1 Overview .....	193
7.4.2 CPS Request Sequence .....	193
7.4.3 CPS Reply Sequence .....	194
7.5 Policy Summation ELSs .....	194
7.5.1 Overview .....	194
7.5.2 Fabric Change Notification Specification .....	194
7.6 Zoning Policies .....	195
7.6.1 Overview .....	195
7.6.2 Management Requests .....	195
7.6.3 Fabric Operations .....	198
7.6.4 Zoning Ordering Rules .....	204
7.6.5 The Client-Server Protocol .....	205
<b>8 Combinations of Security Protocols .....</b>	<b>208</b>
8.1 Entity Authentication Overview .....	208
8.2 Terminology .....	208
8.3 Scope of Security Relationships .....	209
8.3.1 N_Port_ID Virtualization .....	209
8.3.2 Nx_Port Entity to a Fabric Entity .....	209
8.3.3 Nx_Port Entity to Nx_Port Entity .....	210
8.4 Entity Authentication Model .....	210
8.5 Abstract Services for Entity Authentication .....	212
8.5.1 Overview .....	212
8.5.2 Authentication Service .....	212
8.5.3 Security Service .....	213
8.5.4 FC-2 Service .....	213
8.6 Nx_Port to Fabric Authentication (NFA) State Machine .....	218
8.6.1 Overview .....	218

8.6.2 NFA States .....	219
8.6.3 NFA Events .....	220
8.6.4 NFA Transitions .....	220
8.7 Fabric from Nx_Port Authentication (FNA) State Machine .....	226
8.7.1 Overview .....	226
8.7.2 FNA States .....	227
8.7.3 FNA Events .....	228
8.7.4 FNA Transitions .....	228
8.8 Nx_Port to Nx_Port Authentication (NNA) State Machine .....	236
8.8.1 Overview .....	236
8.8.2 NNA States .....	237
8.8.3 NNA Events .....	238
8.8.4 NNA Transitions .....	238
8.9 Additional Security State Machines .....	245
8.9.1 E_Port to E_Port Security Checks .....	245
8.9.2 B_Port Security Checks .....	246
8.9.3 Switch Security Checks with Virtual Fabrics .....	246
8.9.4 N_Port Security Checks with Virtual Fabrics .....	248
8.10 Impact on Other Standards .....	248
<b>Annex A: FC-SP-2 Compliance Summary (normative) .....</b>	<b>249</b>
A.1 Compliance Elements .....	249
A.1.1 Overview .....	249
A.1.2 FC-SP-2 Compliance .....	250
A.1.3 Conventions .....	250
A.2 Authentication Compliance Elements .....	251
A.2.1 AUTH-A .....	251
A.2.2 AUTH-B1 .....	252
A.2.3 AUTH-B2 .....	253
A.2.4 AUTH-B3 .....	254
A.3 SA Management Compliance Elements .....	255
A.3.1 Algorithms Support .....	255
A.3.2 SA-A .....	257
A.3.3 SA-B .....	258
A.3.4 SA-C1 .....	261
A.3.5 SA-C2 .....	263
A.3.6 SA-C3 .....	265
A.4 Policy Compliance Elements .....	267
A.4.1 POL-A1 .....	267
A.4.2 POL-A2 .....	268
A.4.3 POL-A3 .....	269
A.4.4 POL-B3 .....	270
<b>Annex B: KMIP Profile for FC-SP-2 EAP-GPSK (Normative) .....</b>	<b>272</b>
B.1 Overview .....	272
B.2 General .....	272
B.3 KMIP profile specification .....	272
B.3.1 FC-SP-2 EAP-GPSK Profile .....	272
B.3.2 FC-SP-2 EAP-GPSK Authentication Suite .....	272
B.3.3 FC-SP-2 EAP/GPSK Key Foundry and Server Conformance Clause .....	274
<b>Annex C: Random Number Generation and Secret Storage</b>	

<b>(informative) .....</b>	<b>276</b>
C.1 Random Number Generator .....	276
C.2 Secret Storage .....	276
<b>Annex D: RADIUS Deployment</b>	
<b>(informative) .....</b>	<b>277</b>
D.1 Overview .....	277
D.2 RADIUS Servers .....	277
D.2.1 Overview .....	277
D.2.2 Digest Algorithm .....	278
D.3 RADIUS Messages .....	278
D.3.1 Message Types .....	278
D.3.2 Radius Attributes .....	279
D.4 RADIUS Authentication .....	282
D.4.1 RADIUS Authentication Method .....	282
D.4.2 RADIUS Authentication with NULL DH algorithm .....	283
D.4.3 Bidirectional Authentication with RADIUS .....	285
D.4.4 RADIUS Authentication with DH option .....	286
<b>Annex E: Examples of Proposals Negotiation for the SA Management Protocol</b>	
<b>(informative) .....</b>	<b>288</b>
<b>Annex F: Guidelines for Mapping Access Control Requirements to Fabric Policies</b>	
<b>(informative) .....</b>	<b>289</b>
<b>Annex G: Pre FC-SP-2 Fabric Policy Implementations</b>	
<b>(informative) .....</b>	<b>290</b>
G.1 Overview .....	290
G.2 Fabric Management Policy Set .....	290
G.2.1 Fabric Management Policy Set Overview .....	290
G.2.2 FMPS Hierarchy Model .....	290
G.2.3 Policy Description .....	290
G.2.4 Policy Distribution .....	291
G.2.5 Signature, Version Stamp, and Timestamp .....	291
G.2.6 FMPS Object Structure .....	292
G.2.7 Fabric Initialization And Fabric Join Procedures .....	292
G.2.8 FMPS Payload Format .....	295
G.3 Fabric Binding .....	302
G.3.1 Fabric Binding Overview .....	302
G.3.2 Joining Switches .....	303
G.3.3 Managing User-Initiated Change Requests .....	303
G.3.4 Fabric Binding Objects .....	303
G.3.5 Fabric Binding Commands .....	303
G.3.6 Exchange Fabric Membership Data (EFMD) .....	304
G.3.7 Exchange Security Attributes (ESA) .....	306
G.3.8 Query Security Attributes (QSA) Version 1 .....	308

Figure	Page
Figure 1 – State machine example . . . . .	35
Figure 2 – Relationship between Authentication Protocols and Security Associations . . . . .	38
Figure 3 – Logical Model for Integrity and Confidentiality Protection with ESP_Header . . . . .	40
Figure 4 – Logical Model for Integrity and Confidentiality Protection with CT_Authentication . . . . .	42
Figure 5 – A Generic Authentication Transaction . . . . .	45
Figure 6 – Example of AUTH_Reject . . . . .	55
Figure 7 – A DH-CHAP Protocol Transaction Example . . . . .	58
Figure 8 – A FCAP Protocol Transaction Example . . . . .	68
Figure 9 – A FCPAP Protocol Transaction Example . . . . .	79
Figure 10 – A FCEAP Protocol Transaction Example . . . . .	85
Figure 11 – A Failing FCEAP Protocol Transaction Example . . . . .	88
Figure 12 – FC-2 AUTH_ILS Mapping Example for the E_Port to E_Port Case . . . . .	91
Figure 13 – Usage of B_AUTH_ILS . . . . .	93
Figure 14 – FC-2 B_AUTH_ILS Mapping Example . . . . .	94
Figure 15 – FC-2 AUTH_ELS Mapping Example for the Nx_Port to Nx_Port Case . . . . .	97
Figure 16 – AUTH_ELS Fragmentation Process . . . . .	99
Figure 17 – Use of the Sequence Number Bit Example . . . . .	100
Figure 18 – FC-2 Authentication Mapping with AUTH_ELS Fragmentation Example . . . . .	101
Figure 19 – An SA Management Transaction Example . . . . .	105
Figure 20 – An IKE_SA_Init exchange . . . . .	113
Figure 21 – An IKE_Auth exchange . . . . .	125
Figure 22 – An IKE_Create_Child_SA exchange . . . . .	133
Figure 23 – An IKE_Informational exchange . . . . .	135
Figure 24 – Concatenation of Authentication and SA Management Transactions . . . . .	143
Figure 25 – An IKEv2-AUTH Transaction . . . . .	144
Figure 26 – Policy Data Structures . . . . .	149
Figure 27 – Policy Management Model . . . . .	176
Figure 28 – Entity Authentication Standard Perspective . . . . .	209
Figure 29 – Entity Authentication Model for an Nx_Port (Informative) . . . . .	211
Figure 30 – NFA State Machine . . . . .	219
Figure 31 – FNA State Machine . . . . .	227
Figure 32 – NNA State Machine . . . . .	237
Figure 33 – State P17:Security Checks . . . . .	245
Figure 34 – State P24(k):Security Checks . . . . .	247
Figure D.1 – Unidirectional Authentication with RADIUS . . . . .	284
Figure D.2 – Bidirectional Authentication with RADIUS . . . . .	285
Figure D.3 – DH-CHAP Authentication with RADIUS . . . . .	287

Table	Page
Table 1 – ISO and American conventions . . . . .	31
Table 2 – Name Format . . . . .	44
Table 3 – AUTH_ILS Message Format . . . . .	47
Table 4 – AUTH_ILS Flags . . . . .	47
Table 5 – B_AUTH_ILS Message Format . . . . .	48
Table 6 – AUTH_ELS Message Format . . . . .	48
Table 7 – AUTH_ELS Flags . . . . .	48
Table 8 – AUTH Message Codes . . . . .	49
Table 9 – Vendor Specific Message Payload Format . . . . .	50
Table 10 – AUTH_Negotiate Message Payload . . . . .	51
Table 11 – Authentication Protocol Identifiers . . . . .	52
Table 12 – AUTH_Negotiate Vendor Specific Protocol Parameters . . . . .	52
Table 13 – Names used in Authentication . . . . .	52
Table 14 – Hash Functions Identifiers . . . . .	53
Table 15 – Diffie-Hellman Group Identifiers . . . . .	53
Table 16 – AUTH_Reject Message Payload . . . . .	55
Table 17 – AUTH_Reject Reason Codes . . . . .	55
Table 18 – AUTH_Reject Reason Code Explanations . . . . .	56
Table 19 – Error Conditions . . . . .	56
Table 20 – Mathematical Notation for DH-CHAP . . . . .	59
Table 21 – AUTH_Negotiate DH-CHAP Protocol Parameters . . . . .	60
Table 22 – AUTH_Negotiate DH-CHAP Parameter Format . . . . .	60
Table 23 – AUTH_Negotiate DH-CHAP Parameter Tags . . . . .	60
Table 24 – DHCHAP_Challenge Message Payload . . . . .	61
Table 25 – DHCHAP_Reply Message Payload . . . . .	63
Table 26 – DHCHAP_Success Message Payload . . . . .	64
Table 27 – Mathematical Notation for FCAP . . . . .	67
Table 28 – AUTH_Negotiate FCAP Protocol Parameters . . . . .	70
Table 29 – AUTH_Negotiate FCAP Parameter Format . . . . .	70
Table 30 – AUTH_Negotiate FCAP Parameter Tags . . . . .	70
Table 31 – FCAP_Request Message Payload . . . . .	71
Table 32 – FCAP_Certificate Format . . . . .	72
Table 33 – Certificate Formats . . . . .	72
Table 34 – FCAP usage of X.509v3 Certificate fields . . . . .	72
Table 35 – FCAPNonce Format . . . . .	74
Table 36 – Nonce Formats . . . . .	74
Table 37 – FCAP_Acknowledge Message Payload . . . . .	74
Table 38 – FCAP_Signature Format . . . . .	75
Table 39 – Signature Formats . . . . .	75
Table 40 – FCAP_Confirm Message Payload . . . . .	76
Table 41 – Mathematical Notation for FCPAP . . . . .	78
Table 42 – AUTH_Negotiate FCPAP Protocol Parameters . . . . .	81
Table 43 – AUTH_Negotiate FCPAP Parameter Format . . . . .	81
Table 44 – AUTH_Negotiate FCPAP Parameter Tags . . . . .	81
Table 45 – FCPAP_Init Message Payload . . . . .	82
Table 46 – FCPAP_Accept Message Payload . . . . .	83
Table 47 – FCPAP_Complete Message Payload . . . . .	83
Table 48 – FCEAP_Request Message Payload . . . . .	86
Table 49 – FCEAP_Response Message Payload . . . . .	86
Table 50 – FCEAP_Success Message Payload . . . . .	87
Table 51 – FCEAP_Failure Message Payload . . . . .	87
Table 52 – Supported EAP Methods . . . . .	89

Table 53 – AUTH_ILS SW_RJT Reasons .....	92
Table 54 – AUTH_ILS SW_ACC Payload .....	92
Table 55 – B_AUTH_ILS SW_RJT Reasons .....	95
Table 56 – B_AUTH_ILS SW_ACC Payload .....	95
Table 57 – AUTH_ELS LS_RJT Reasons .....	98
Table 58 – AUTH_ELS LS_ACC Payload .....	98
Table 59 – Security Bit Applicability .....	102
Table 60 – Security Bit usage with FLOGI .....	102
Table 61 – Security Bit usage with PLOGI .....	103
Table 62 – Login LS_RJT Reasons .....	103
Table 63 – IKE Payloads Summary .....	106
Table 64 – IKE_Header Payload Format .....	109
Table 65 – IKE Flags .....	110
Table 66 – Chaining Header Format .....	110
Table 67 – IKE Payload Type Values .....	111
Table 68 – Chaining Flags .....	112
Table 69 – IKE_SA_Init Message Payload .....	113
Table 70 – Examples of Proposals .....	115
Table 71 – Security_Association Payload Format .....	116
Table 72 – Security Protocol Identifiers .....	117
Table 73 – Transforms Definition .....	117
Table 74 – Transform Type Values .....	118
Table 75 – Encryption Algorithms Transform_IDs (Transform Type 1) .....	119
Table 76 – Pseudo-random Functions Transform_IDs (Transform Type 2) .....	119
Table 77 – Integrity Algorithms Transform_IDs (Transform Type 3) .....	120
Table 78 – Diffie-Hellman Group Transform_IDs (Transform Type 4) .....	120
Table 79 – Mandatory Transform Types .....	121
Table 80 – Mandatory and Recommended Transform_IDs .....	121
Table 81 – Transform Attributes Definition .....	123
Table 82 – Attribute Type Values .....	123
Table 83 – Key_Exchange Payload Format .....	124
Table 84 – Nonce Payload Format .....	124
Table 85 – IKE_Auth Message Payload .....	125
Table 86 – IKE Payloads Contained in the IKE_Auth Message .....	126
Table 87 – Encrypted Payload Format .....	126
Table 88 – Identification Payload Format .....	127
Table 89 – Type Identifiers .....	127
Table 90 – Authentication Payload Format .....	128
Table 91 – Authentication Methods .....	128
Table 92 – Traffic Selector Payload Format .....	128
Table 93 – Traffic Selector Definition .....	129
Table 94 – TS Type Identifiers .....	129
Table 95 – Certificate Payload Format .....	130
Table 96 – Certificate Encodings .....	131
Table 97 – Certificate Request Payload Format .....	132
Table 98 – IKE_Create_Child_SA Message Payload .....	134
Table 99 – IKE Payloads Contained in the IKE_Create_Child_SA Message .....	134
Table 100 – IKE_Informational Message Payload .....	135
Table 101 – IKE Payloads Contained in the IKE_Informational Message .....	136
Table 102 – Notify Payload Format .....	136
Table 103 – Notify Message Types - Errors .....	137
Table 104 – Notify Message Types - Status .....	139
Table 105 – Delete Payload Format .....	140
Table 106 – Vendor_ID Payload Format .....	141

Table 107 – Policy Objects . . . . .	150
Table 108 – Names used to define Policies . . . . .	151
Table 109 – Policy Summary Object Format . . . . .	153
Table 110 – Object Flags . . . . .	153
Table 111 – Hash Field Format . . . . .	154
Table 112 – Hash Formats . . . . .	154
Table 113 – Switch Membership List Object Format . . . . .	155
Table 114 – Object Flags . . . . .	155
Table 115 – Switch Entry Field Format . . . . .	156
Table 116 – Basic Switch Attributes Format . . . . .	156
Table 117 – Switch Flags . . . . .	156
Table 118 – Policy Data Role . . . . .	158
Table 119 – Authentication Behavior . . . . .	158
Table 120 – Node Membership List Object Format . . . . .	159
Table 121 – Node Entry Field Format . . . . .	160
Table 122 – Basic Node Attribute Format . . . . .	160
Table 123 – Node Flags . . . . .	160
Table 124 – Common Transport Access Specifier Format . . . . .	161
Table 125 – CT Access Descriptor Format . . . . .	161
Table 126 – CT Access Flags . . . . .	161
Table 127 – Examples of Common Transport Access Specifiers . . . . .	162
Table 128 – Switch Connectivity Object Format . . . . .	163
Table 129 – Port Connectivity Entry Format . . . . .	164
Table 130 – IP Management List Object Format . . . . .	165
Table 131 – IP Management Entry Format . . . . .	165
Table 132 – Basic IP Management Attributes Format . . . . .	166
Table 133 – IP Management Flags . . . . .	166
Table 134 – Well Known Protocols Access Specifier Format . . . . .	166
Table 135 – WKP Access Descriptor Format . . . . .	166
Table 136 – WKP Access Flags . . . . .	167
Table 137 – Examples of Well Known Protocols Access Specifiers . . . . .	168
Table 138 – Attribute Object Format . . . . .	169
Table 139 – Attribute Entry Format . . . . .	169
Table 140 – Attribute Formats . . . . .	169
Table 141 – Notation for Policy Enforcement . . . . .	170
Table 142 – Security Policy Server – Request Command Codes . . . . .	176
Table 143 – ESFC Operations for Fabric Policies . . . . .	177
Table 144 – ESFC Payload for Operation ‘Activate Policy Summary’ . . . . .	177
Table 145 – ESFC Payload for Operation ‘Deactivate Policy Summary’ . . . . .	178
Table 146 – ESFC Payload for Operation ‘Add Policy Object’ . . . . .	178
Table 147 – ESFC Payload for Operation ‘Remove Policy Object’ . . . . .	179
Table 148 – ESFC Payload for Operation ‘Remove All Non-Active Policy Objects’ . . . . .	179
Table 149 – Security Policy Server CT Requests and Fabric Actions . . . . .	180
Table 150 – GPOS Request CT_IU . . . . .	181
Table 151 – Accept CT_IU to a GPOS Request . . . . .	181
Table 152 – Fabric Policy Objects Support Flags . . . . .	182
Table 153 – Switch Policy Objects Support Entry Format . . . . .	182
Table 154 – Switch Policy Objects Support Flags . . . . .	183
Table 155 – ESS Security Policy Server Capability Object Format . . . . .	183
Table 156 – Optional Data Field Format . . . . .	184
Table 157 – Security Object Format . . . . .	184
Table 158 – Security Object Tags . . . . .	184
Table 159 – Vendor Specific Security Object Payload Format . . . . .	185
Table 160 – GPS Request CT_IU . . . . .	185

Table 161 – Accept CT_IU to a GPS Request . . . . .	185
Table 162 – APS Request CT_IU . . . . .	186
Table 163 – Accept CT_IU to an APS Request . . . . .	186
Table 164 – DPS Request CT_IU . . . . .	187
Table 165 – Accept CT_IU to a DPS Request . . . . .	187
Table 166 – GPO Request CT_IU . . . . .	187
Table 167 – Accept CT_IU to a GPO Request . . . . .	188
Table 168 – GALN Request CT_IU . . . . .	188
Table 169 – Accept CT_IU to a GALN Request . . . . .	189
Table 170 – GAAO Request CT_IU . . . . .	189
Table 171 – Accept CT_IU to a GAAO Request . . . . .	190
Table 172 – APO Request CT_IU . . . . .	190
Table 173 – Accept CT_IU to an APO Request . . . . .	191
Table 174 – RPO Request CT_IU . . . . .	191
Table 175 – Accept CT_IU to a RPO Request . . . . .	192
Table 176 – RANA Request CT_IU . . . . .	192
Table 177 – Accept CT_IU to a RANA Request . . . . .	193
Table 178 – Check Policy Summary SW_ILS Request Payload . . . . .	193
Table 179 – Check Policy Summary SW_RJT Reasons . . . . .	194
Table 180 – Check Policy Summary SW_ACC Payload . . . . .	194
Table 181 – Fabric Enhanced Zoning Support Flags Additions . . . . .	196
Table 182 – Switch Enhanced Zoning Support Flags Additions . . . . .	196
Table 183 – Fabric Enhanced Zoning Request Flags Additions. . . . .	196
Table 184 – SPCMIT Request Payload . . . . .	197
Table 185 – SPCMIT Accept Payload . . . . .	198
Table 186 – ESS Zone Server Support Flags Additions. . . . .	198
Table 187 – Zoning Check Protocol SW_ILS Request Payload . . . . .	199
Table 188 – Zoning Check Protocol SW_RJT Reasons . . . . .	199
Table 189 – Zoning Check Protocol SW_ACC Payload . . . . .	200
Table 190 – Additional SFC Operation Request Codes . . . . .	200
Table 191 – Payload for the Operation Request ‘FC-SP Activate Zone Set Enhanced’ . . . . .	201
Table 192 – Payload for the Operation Request ‘FC-SP Deactivate Zone Set Enhanced’ . . . . .	202
Table 193 – Payload for the Operation Request ‘FC-SP Distribute Zone Set Database’ . . . . .	202
Table 194 – Payload for the Operation Request ‘FC-SP Activate Zone Set by Name’ . . . . .	203
Table 195 – Payload for the Operation Request ‘FC-SP Set Zoning Policies’ . . . . .	203
Table 196 – Zone Information Request SW_ILS Request Payload . . . . .	206
Table 197 – Zone Information Request SW_RJT Reasons . . . . .	207
Table 198 – Zone Information Request SW_ACC Payload . . . . .	207
Table A.1 – FC-SP-2 Authentication Compliance Elements . . . . .	249
Table A.2 – FC-SP-2 SA Management Compliance Elements . . . . .	249
Table A.3 – FC-SP-2 Policy Compliance Elements . . . . .	249
Table A.4 – Feature Set table terms and definitions . . . . .	250
Table A.5 – Feature Set table key abbreviations . . . . .	250
Table A.6 – Authentication Protocols Support for AUTH-A . . . . .	251
Table A.7 – AUTH Messages Support for AUTH-A . . . . .	251
Table A.8 – Hash Functions Support for AUTH-A . . . . .	251
Table A.9 – DH Groups Support for AUTH-A. . . . .	251
Table A.10 – Authentication Protocols Support for AUTH-B1 . . . . .	252
Table A.11 – AUTH Messages Support for AUTH-B1 . . . . .	252
Table A.12 – Hash Functions Support for AUTH-B1 . . . . .	252
Table A.13 – DH Groups Support for AUTH-B1. . . . .	252
Table A.14 – Authentication Protocols Support for AUTH-B2 . . . . .	253
Table A.15 – AUTH Messages Support for AUTH-B2 . . . . .	253
Table A.16 – Hash Functions Support for AUTH-B2 . . . . .	253

Table A.17 – DH Groups Support for AUTH-B2 . . . . .	253
Table A.18 – Authentication Protocols Support for AUTH-B3. . . . .	254
Table A.19 – AUTH Messages Support for AUTH-B3 . . . . .	254
Table A.20 – Hash Functions Support for AUTH-B3 . . . . .	254
Table A.21 – DH Groups Support for AUTH-B3 . . . . .	254
Table A.22 – Security Protocols Support . . . . .	255
Table A.23 – Encryption Algorithms Support . . . . .	255
Table A.24 – Pseudo Random Functions Support . . . . .	255
Table A.25 – Integrity Algorithms Support . . . . .	256
Table A.26 – SA Management DH Groups Support . . . . .	256
Table A.27 – SA Management Protocol Support for SA-A . . . . .	257
Table A.28 – AUTH Messages Support for SA-A . . . . .	257
Table A.29 – IKEv2 Payloads Support for SA-A . . . . .	257
Table A.30 – SA Management Protocol Support for SA-B . . . . .	258
Table A.31 – AUTH Messages Support for SA-B . . . . .	259
Table A.32 – Authentication Hash Functions Support for SA-B . . . . .	259
Table A.33 – Authentication DH Groups Support for SA-B. . . . .	259
Table A.34 – IKEv2 Payloads Support for SA-B . . . . .	259
Table A.35 – SA Management Protocol Support for SA-C1 . . . . .	261
Table A.36 – AUTH Messages Support for SA-C1 . . . . .	261
Table A.37 – Authentication Hash Functions Support for SA-C1 . . . . .	261
Table A.38 – Authentication DH Groups Support for SA-C1 . . . . .	262
Table A.39 – IKEv2 Payloads Support for SA-C1 . . . . .	262
Table A.40 – SA Management Protocol Support for SA-C2 . . . . .	263
Table A.41 – AUTH Messages Support for SA-C2 . . . . .	263
Table A.42 – Authentication Hash Functions Support for SA-C2 . . . . .	263
Table A.43 – Authentication DH Groups Support for SA-C2 . . . . .	264
Table A.44 – IKEv2 Payloads Support for SA-C2 . . . . .	264
Table A.45 – SA Management Protocol Support for SA-C3 . . . . .	265
Table A.46 – AUTH Messages Support for SA-C3 . . . . .	265
Table A.47 – Authentication Hash Functions Support for SA-C3 . . . . .	265
Table A.48 – Authentication DH Groups Support for SA-C3 . . . . .	266
Table A.49 – IKEv2 Payloads Support for SA-C3 . . . . .	266
Table A.50 – Protocols Support for POL-A1 . . . . .	267
Table A.51 – Policy Objects Support for POL-A1 . . . . .	267
Table A.52 – Switch Flags Support for POL-A1 . . . . .	267
Table A.55 – Protocols Support for POL-A2 . . . . .	268
Table A.53 – Security Policy Server Support for POL-A1 . . . . .	268
Table A.54 – EUFC Operations Support for POL-A1 . . . . .	268
Table A.59 – Protocols Support for POL-A3 . . . . .	269
Table A.56 – Policy Objects Support for POL-A2 . . . . .	269
Table A.57 – Security Policy Server Support for POL-A2 . . . . .	269
Table A.58 – EUFC Operations Support for POL-A2 . . . . .	269
Table A.60 – Protocols Support for POL-B3 . . . . .	270
Table A.61 – Policy Objects Support for POL-B3 . . . . .	270
Table A.62 – Switch Flags Support for POL-B3 . . . . .	270
Table A.63 – Security Policy Server Support for POL-B3 . . . . .	271
Table A.64 – EUFC Operations Support for POL-B3 . . . . .	271
Table D.1 – RADIUS Message Format . . . . .	278
Table D.2 – RADIUS Message Codes . . . . .	278
Table D.3 – User-Name Attribute . . . . .	279
Table D.4 – Binary to UTF-8 Transformation . . . . .	280
Table D.5 – CHAP-Password Attribute . . . . .	281
Table D.6 – CHAP-Challenge Attribute . . . . .	282