ISO/IEC 14165-432

Edition 1.0 2022-03

INTERNATIONAL STANDARD

colour inside

Information technology – Fibre channel – Part 432: Security Protocols – 2 (FC-SP-2)



ISO/IEC 14165-432:2022-03(en)



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
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC Products & Services Portal - 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
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

Edition 1.0 2022-03

INTERNATIONAL STANDARD

colour inside

Information technology – Fibre channel – Part 432: Security Protocols – 2 (FC-SP-2)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.200

ISBN 978-2-8322-1084-0

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

Contents **Page**

FOREWORD **15**

9 INTRODUCTION **17**

1 Scope **18**

2 Normative references **19**

3 Terms, definitions, symbols, abbreviated terms, and conventions **23**
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

4 Structure and Concepts **37**
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

5 Authentication Protocols **45**
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

6 Security Association Management Protocol 105
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

7 Fabric Policies 149
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

8 Combinations of Security Protocols 208
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

Annex A: FC-SP-2 Compliance Summary (normative) . . . 249

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

Annex B: KMIP Profile for FC-SP-2 EAP-GPSK (Normative) . . . 272

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

Annex C: Random Number Generation and Secret Storage

(informative) 276
C.1 Random Number Generator 276
C.2 Secret Storage 276

Annex D: RADIUS Deployment (informative) 277
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

Annex E: Examples of Proposals Negotiation for the SA Management Protocol (informative) 288

Annex F: Guidelines for Mapping Access Control Requirements to Fabric Policies (informative) 289

Annex G: Pre FC-SP-2 Fabric Policy Implementations (informative) 290
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 – FCAP Nonce 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

Table D.7 – Mathematical Notation for RADIUS Authentication. 283
Table G.1 – Security Request Payload. 296
Table G.2 – Security Command Code 296
Table G.3 – Version Stamp Format 297
Table G.4 – Certificate Download Object 297
Table G.5 – Security Policy Set Object. 298
Table G.6 – Security Policy Object 299
Table G.7 – Type Value 299
Table G.8 – Policy Type Value 300
Table G.9 – Policy Member Object. 300
Table G.10 – Member Type Value 301
Table G.11 – Download Accept Payload Format 301
Table G.12 – Request Response Code values 302
Table G.13 – Request Reason Code values 302
Table G.14 – Fabric Binding Membership List Entry 303
Table G.15 – Fabric Configuration Data Requests. 304
Table G.16 – EFMD Request Payload 304
Table G.17 – Operation Field Values 305
Table G.18 – Fabric Binding Operation Membership Data. 305
Table G.19 – EFMD Accept Payload 306
Table G.20 – EFMD Reason Codes Additions 306
Table G.21 – ESA Request Payload 307
Table G.22 – ESA Accept Payload. 308
Table G.23 – QSA Request Payload 309

INFORMATION TECHNOLOGY – FIBRE CHANNEL –

Part 432: Security Protocols - 2 (FC-SP-2)

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.

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 and ISO National bodies.

3. IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and 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 and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.

5. IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO 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 document.

7. No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National 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, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.

8. Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.

9. Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 14165-432 has been prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on Voting
JTC1-SC25/2999/CDV	JTC1-SC25/3029/RVC

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, available at www.iec.ch/members_experts/refdocs and www.iso.org/directives

A list of all parts in the ISO/IEC 14165 series, published under the general title *Information technology – Fibre Channel*, can be found on the IEC and ISO websites.

IMPORTANT – The "colour inside" logo on the cover page of this document 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

This standard describes the protocols used to implement security in a Fibre Channel Fabric. This standard includes the definition of protocols to authenticate Fibre Channel entities, protocols to set up session keys, protocols to negotiate the parameters required to ensure frame-by-frame integrity and confidentiality, and protocols to establish and distribute policies across a Fibre Channel Fabric.

INFORMATION TECHNOLOGY – FIBRE CHANNEL –

Part 432: Security Protocols - 2 (FC-SP-2)

1 Scope

This part of 14165 is one of the Fibre Channel family of standards. This standard describes the protocols used to implement security in a Fibre Channel Fabric. This standard includes the definition of protocols to authenticate Fibre Channel entities, protocols to set up session keys, protocols to negotiate the parameters required to ensure frame-by-frame integrity and confidentiality, and protocols to establish and distribute policies across a Fibre Channel Fabric.

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.

ANSI INCITS 305-1998 (R2008), *SCSI Enclosures Services (SES).* Available at https://webstore.ansi.org/Standards/INCITS/INCITS3051998R2018

ANSI INCITS 305-1998/AM1-2000 (R2008), *SCSI Enclosures Services (SES) - Amendment 1.* Available at https://webstore.ansi.org/Standards/INCITS/INCITS3051998AM12000R2018

ANSI INCITS 461-2010, *Fibre Channel - Switch Fabric - 5 (FC-SW-5).* Available at https://webstore.ansi.org/Standards/INCITS/INCITS4612010

ANSI INCITS 463-2010, *Fibre Channel - Generic Services - 6 (FC-GS-6).* Available at https://webstore.ansi.org/Standards/INCITS/INCITS4632010

ANSI INCITS 470-2011, *Fibre Channel - Framing and Signaling - 3 (FC-FS-3).* Available at https://webstore.ansi.org/Standards/INCITS/INCITS4702011

ANSI INCITS 477-2011, *Fibre Channel - Link Services - 2 (FC-LS-2).* Available at https://webstore.ansi.org/Standards/INCITS/INCITS4772011

ANSI INCITS 487-2018, *Fibre Channel - Link Services - 3 (FC-LS-3).* Available at https://webstore.ansi.org/Standards/INCITS/INCITS4872018

INCITS TR-49-2012, *Fibre Channel - Device Attach - 2 (FC-DA-2).* Available at https://webstore.ansi.org/Standards/INCITS/INCITSTR492012R2017

RFC 1321, *The MD5 Message-Digest Algorithm*, April 1992. Available at http://www.ietf.org/rfc/rfc1321.txt

RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, August 1996. Available at http://www.ietf.org/rfc/rfc1994.txt

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*, February 1997. Available at http://www.ietf.org/rfc/rfc2104.txt

RFC 2246, *The TLS Protocol Version 1.0*, January 1999. Available at http://www.ietf.org/rfc/rfc2246.txt

RFC 2401, *Security Architecture for the Internet Protocol*, November 1998. Available at http://www.ietf.org/rfc/rfc2401.txt

RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH,* November 1998. Available at http://www.ietf.org/rfc/rfc2403.txt

RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH,* November 1998. Available at http://www.ietf.org/rfc/rfc2404.txt

RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec,* November 1998. Available at http://www.ietf.org/rfc/rfc2410.txt

RFC 2434, *Guidelines for Writing an IANA Considerations Section in RFCs,* October 1998. Available at http://www.ietf.org/rfc/rfc2434.txt

RFC 2437, PKCS #1: *RSA Cryptography Specifications Version 2,* October 1998. Available at http://www.ietf.org/rfc/rfc2437.txt

RFC 2451, *The ESP CBC-Mode Cipher Algorithms,* November 1998. Available at http://www.ietf.org/rfc/rfc2451.txt

RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,* June 1999. Available at http://www.ietf.org/rfc/rfc2560.txt

RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1*, June 1999. Available at http://www.ietf.org/rfc/rfc2616.txt

RFC 2631, *Diffie-Hellman Key Agreement Method,* June 1999. Available at http://www.ietf.org/rfc/rfc2631.txt

RFC 2865, *Remote Authentication Dial In User Service (RADIUS),* June 2000. Available at http://www.ietf.org/rfc/rfc2865.txt

RFC 2945, *The SRP Authentication and Key Exchange System*, September 2000. Available at http://www.ietf.org/rfc/rfc2945.txt

RFC 3279, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* April 2002. Available at http://www.ietf.org/rfc/rfc3279.txt

RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE),* May 2003. Available at http://www.ietf.org/rfc/rfc3526.txt

RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec,* September 2003. Available at http://www.ietf.org/rfc/rfc3602.txt

RFC 3686, *Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP),* January 2004. Available at http://www.ietf.org/rfc/rfc3686.txt

RFC 3723, *Securing Block Storage Protocols over IP,* April 2004. Available at http://www.ietf.org/rfc/rfc3723.txt

RFC 3748, *Extensible Authentication Protocol (EAP),* June 2004. Available at http://www.ietf.org/rfc/rfc3748.txt

RFC 3852, *Cryptographic Message Syntax (CMS),* July 2004. Available at http://www.ietf.org/rfc/rfc3852.txt

RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*, January 2005. Available at http://www.ietf.org/rfc/rfc3986.txt

RFC 4072, *Diameter Extensible Authentication Protocol (EAP) Application,* August 2005. Available at http://www.ietf.org/rfc/rfc4072.txt

RFC 4086, *Randomness Requirements for Security,* June 2005. Available at http://www.ietf.org/rfc/rfc4086.txt

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP),* June 2005. Available at http://www.ietf.org/rfc/rfc4106.txt

RFC 4303, *IP Encapsulating Security Payload (ESP),* December 2005. Available at http://www.ietf.org/rfc/rfc4303.txt

RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE),* February 2006. Available at http://www.ietf.org/rfc/rfc4434.txt

RFC 4543, *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH,* May 2006. Available at http://www.ietf.org/rfc/rfc4543.txt

RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*, April 2006. Available at http://www.ietf.org/rfc/rfc4346.txt

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008. Available at http://www.ietf.org/rfc/rfc5246.txt

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* May 2008. Available at http://www.ietf.org/rfc/rfc5280.txt

RFC 5433, *Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method,* February 2009. Available at http://www.ietf.org/rfc/rfc5433.txt

RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2),* September 2010. Available at http://www.ietf.org/rfc/rfc5996.txt

RFC 6614, *TLS encryption for RADIUS,* May 2012. Available at http://www.ietf.org/rfc/rfc6614.txt

RFC 6818, *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* January 2013. Available at http://www.ietf.org/rfc/rfc6818.txt

SRP-6, *Improvements and Refinements to the Secure Remote Password Protocol,* Submission to the IEEE P1363 Working Group, Oct 2002. Available at http://srp.stanford.edu

X.509v3, ITU-T Recommendation X.509 (1997 E), *Information Technology - Open Systems Interconnection - The Directory: Authentication Framework,* June 1997. Available at https://www.itu.int/ITU-T/recommendations

X.501, ITU-T Recommendation X.501, *Information Technology - Open Systems Interconnection - The Directory: Models,* 1993. Available at https://www.itu.int/ITU-T/recommendations

FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* May 2001. Available at https://csrc.nist.gov/publications/detail/fips/140/2/final

FIPS PUB 180-4, Secure Hash Standard (SHS), March 2012. Available at https://csrc.nist.gov/publications/detail/fips/180/4/final

FIPS PUB 197, *Advanced Encryption Standard (AES),* November 2001. Available at https://csrc.nist.gov/publications/detail/fips/197/final

FIPS PUB 198, *The Keyed-Hash Message Authentication Code (HMAC),* March 2002. Available at https://csrc.nist.gov/csrc/media/publications/fips/198/archive/2002-03-06/documents/fips-198a.pdf

NIST SP 800-57 Part 3, *Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance*, December 2009. Available at https://csrc.nist.gov/publications/detail/sp/800-57-part-3/archive/2009-12-28

NIST SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths,* January 2011. Available at https://csrc.nist.gov/publications/detail/sp/800-131a/archive/2011-01-13

KMIP Spec, *Key Management Interoperability Protocol Specification Version 1.0*, June 2010. Available at http://docs.oasis-open.org/kmip/ug/v1.0/kmip-ug-1.0.pdf

KMIP Profiles, *Key Management Interoperability Protocol Profiles Version 1.0*, June 2010. Available at http://docs.oasis-open.org/kmip/profiles/v1.0/cs01/kmip-profiles-1.0-cs-01.pdf

3 Terms, definitions, symbols, abbreviated terms, and conventions

3.1 Terms and definitions

For the purposes of this document the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org

- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
Access Control
security service that prevents unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

3.1.2
address identifier
address value used to identify source (S_ID) or destination (D_ID) of a frame

Note 1 to entry: See FC-FS-3.

3.1.3
Anti-replay
security service that prevents processing of duplicate frames

3.1.4
Ascending order
sorting order in which each entry is positioned in accord with the value of its key(s) to precede all entries with keys of greater value

3.1.5
Authentication
process that verifies an identity

3.1.6
Authentication Initiator
entity initiating an Authentication Transaction

3.1.7
Authentication Protocol
protocol to perform Authentication

3.1.8
Authentication Responder
responding entity in an Authentication Transaction

3.1.9
Authentication Transaction
instance of an Authentication Protocol

3.1.10
Authorization
process that verifies that an entity is permitted to perform an action

3.1.11
Autonomous Switch
Switch that retains its own per Switch Policy Objects, all Fabric-wide Policy Objects, and all Node to Node (Zoning) information (see 4.8.1)

3.1.12
B_Port
Fabric inter-element port used to connect Bridge devices with E_Ports on a Switch

Note 1 to entry: The B_Port provides a subset of the E_port functionality.

Note 2 to entry: See FC-SW-5.

3.1.13

Bridge
device that encapsulates/de-encapsulates Fibre Channel frames within another protocol

Note 1 to entry: See FC-FS-2.

3.1.14
Certificate
data structure that cryptographically binds an identity to a public key

3.1.15
Certificate Revocation List
list of revoked Certificates issued by a specific CA

3.1.16
Certification Authority
organization or a function that creates, issues and manages Certificates

3.1.17
Child_SA
Security Association used to protect FC-2 frames or CT_IUs

Note 1 to entry: Its parent is an IKE_SA.

3.1.18
Client Switch
Switch that retains its per Switch Policy Objects, all Fabric-wide Policy Objects and the subset of the Node to Node (Zoning) information relevant for its operations (see 4.8.1)

3.1.19
Compliance Element
subset of the features defined in this standard

Note 1 to entry: See Annex A.

3.1.20
Confidentiality
security service that protects data from unauthorized disclosure

3.1.21
Cryptographic Integrity
security service that ensures integrity by using cryptographic techniques

3.1.22
Data Origin Authentication
security service that verifies the identity of the claimed source of data

3.1.23
E_Port
Fabric “Expansion” Port that attaches to another Interconnect_Port to create an Inter-Switch Link

Note 1 to entry: See FC-SW-5.

3.1.24
Encryption
security mechanism used to transform data from an intelligible form (plaintext) into an unintelligible form (ciphertext), in order to provide confidentiality

Note 1 to entry: The inverse transformation process is called decryption.

3.1.25
entity
something that may communicate using a Fibre Channel topology and has an identity that distinguishes it for the purpose of applying the security features specified in this standard

3.1.26
Ephemeral key
nonce used as an intermediate key within a cryptographic protocol

3.1.27
ESP_Header
optional Header defined in FC-FS-3

3.1.28
Exchange
unit of protocol activity that transfers information between a specific Originator Nx_Port and specific Responder Nx_Port using one or more related non-concurrent Sequences that may flow in the same or opposite directions

Note 1 to entry: See FC-FS-3.

3.1.29
exchange (noun)
pair of related messages one of which is a response to the other one (used in clause 6)

3.1.30
Fabric
entity that interconnects Nx_Ports attached to it and is capable of routing frames by using the D_ID information in a FC-2 frame header

Note 1 to entry: See FC-FS-3.

3.1.31
F_Port
Link Control Facility within the Fabric that attaches to an N_Port through a link

Note 1 to entry: An F_Port is addressable by the N_Port attached to it, with a common well-known address identifier (FFFFFEh).

Note 2 to entry: See FC-FS-3.

3.1.32
F_Port_Name
Name_Identifier associated with an F_Port

Note 1 to entry: See FC-FS-3.

3.1.33
FC-SP Compliance
set of Compliance Elements that are required to be implemented in order to claim compliance with this standard

Note 1 to entry: See 4.2.

3.1.34
FC-SP Zoning
variant of zoning defined in this standard (see 7.6)

3.1.35
Fx_Port
Switch port capable of operating as an F_Port or FL_Port

Note 1 to entry: See FC-FS-3.

3.1.36
IKE_SA
Security Association used to protect the messages used by the FC SA management protocol, in order to negotiate Child_SAs

3.1.37
Integrity
service that enables detection of modifications to data

3.1.38
Internet Key Exchange
security protocol used for the management of Security Associations in IP networks

Note 1 to entry: The FC SA Management protocol is based on version 2 of IKE, called IKEv2.

3.1.39
Key
value that controls the operation of a cryptographic algorithm

3.1.40
Local Fx_Port
Fx_Port to which an Nx_Port is directly attached by a link or an Arbitrated Loop

Note 1 to entry: See FC-FS-3.

3.1.41
Log (noun)
one or more collections of information concerning events or conditions that have occurred and may be of interest to security administrator(s)

Note 1 to entry: The mechanism used to maintain a log or logs is vendor specific.

Note 2 to entry: A log may contain sensitive security information and should be appropriately protected.

3.1.42
Log (verb)
to insert information about a specific event or condition into a log

3.1.43
Name_Identifier
64-bit identifier, with a 60-bit value preceded by a 4-bit Network_Address_Authority Identifier, used to identify entities in Fibre Channel

Note 1 to entry: See FC-FS-3.

3.1.44
Node
collection of one or more Nx_Ports controlled by a level above FC-2

Note 1 to entry: See FC-FS-3.

3.1.45
Node_Name
Name_Identifier associated with a Node

Note 1 to entry: See FC-FS-3.

3.1.46
Nonce
unpredictable random value used only for a single instance or invocation of a cryptographic algorithm or protocol

3.1.47
N_Port
hardware entity that includes a Link Control Facility but not Arbitrated Loop functions associated with Arbitrated Loop topology, and has the ability to act as an Originator, a Responder, or both

Note 1 to entry: Well-known addresses are considered to be N_Ports.

Note 2 to entry: See FC-FS-3.

3.1.48
N_Port_Name
Name_Identifier associated with an Nx_Port

Note 1 to entry: See FC-FS-3.

3.1.49
Nx_Port
port capable of operating as an N_Port or Public NL_Port, but not as a Private NL_Port

Note 1 to entry: See FC-FS-3.

3.1.50
Online Certificate Status Protocol
protocol for online verification of Certificate validity

Note 1 to entry: See RFC 2560.

3.1.51
Password
user generated value known to a limited group of entities

Note 1 to entry: Password based Security Protocols use an entity's knowledge of a password to establish security properties and privileges for that entity.

3.1.52
Perfect Forward Secrecy
security service that ensures that the compromise of a single key does not enable access to data protected by other keys

3.1.53
Printable ASCII characters
ASCII characters in the range 20h through 7Eh

3.1.54
Private Key
in asymmetric cryptography the element of a public-private key pair that shall be kept secret

3.1.55
Public Key
in asymmetric cryptography the element of a public-private key pair that may be made public

3.1.56
RADIUS Server
entity providing the security services defined in RFC 2865

3.1.57
Root Certificate
Certificate for a key that a Certification Authority uses to sign the Certificates that it issues

3.1.58
Secret
value known to a limited group of entities and generated with sufficient randomness to be computationally intractable to guess

Note 1 to entry: Secret based Security Protocols use an entity's knowledge of a secret to establish security properties and privileges for that entity.

3.1.59
SA_Initiator
entity initiating an SA Management Transaction

3.1.60
SA Management Protocol
protocol to perform management of Security Associations

3.1.61
SA Management Transaction
instance of a SA Management Protocol

3.1.62
SA Proposal
Proposal
set of security parameters proposed to a peer in the process of negotiating an SA

3.1.63
SA_Responder
responding entity in an SA Management Transaction

3.1.64
Salt
random value associated with a password to increase the difficulty of cryptographic attacks

3.1.65
Security Association
uni-directional logical connection created by the SA Management protocol to provide security processing

Note 1 to entry: All traffic belonging to an SA has the same security processing applied to it.

3.1.66
Security Association Database
database maintaining Security Associations

3.1.67
Security Parameters Index
value used by a receiver to identify the SA to which an incoming frame, CT_IU or FC SA message belongs

3.1.68
security relationship
relationship based on shared state among two or more entities that allows the communication among them to be protected by one or more security services

3.1.69
Server Switch
Switch that retains all Policy Objects and all Node to Node (Zoning) information (see 4.8.1)

3.1.70
Switch
member of the Fabric collective

Note 1 to entry: See FC-SW-5.

3.1.71
Switch_Name
Name_Identifier that identifies a Switch or a Bridge device for identification purposes

Note 1 to entry: See FC-SW-5.

3.1.72
T10 Vendor ID
character string that uniquely identifies a vendor (see 3.5).

3.1.73
well-known address
set of address identifiers defined to access Fabric and other functions (e.g., a name server)

Note 1 to entry: See FC-FS-3.

3.1.74
word
when used to indicate a size, 32 contiguous bits

3.2 Symbols and abbreviated terms

Abbreviations, acronyms, and symbols applicable to this standard are listed. Definitions of several of these items are included in 3.1.

=	is equal to
#	number
||	concatenation symbol (e.g., A || B represents the concatenation of A and B)
ACA	Acquire Change Authorization SW_ILS (see FC-SW-5)
AES	Advanced Encryption Standard (see FIPS PUB 197)
CA	Certification Authority
CHAP	Challenge Handshake Authentication Protocol (see RFC 1994)
CRL	Certificate Revocation List
CT	Common Transport (see FC-GS-6)
CT_IU	Common Transport Information Unit (see FC-GS-6)
DH	Diffie-Hellman
DH-CHAP	Diffie-Hellman augmented CHAP
D_ID	Destination address identifier (see FC-FS-3)
ELS	Extended Link Service (see FC-LS-2)
HMAC	Keyed-Hashing for Message Authentication (see RFC 2104)
IANA	Internet Assigned Numbers Authority (see RFC 2434)
ICV	Integrity Check Value
IKEv2	Internet Key Exchange (IKEv2) Protocol (see RFC 5996)
IP	Internet Protocol (see RFC 791 and RFC 2460)

ISO International Organization for Standardization
ITU International Telecommunication Union
LS_ACC Link Service Accept (see FC-LS-2)
LS_RJT Link Service Reject (see FC-LS-2)
MAC Message Authentication Code
MD5 Message Digest 5 (see RFC 1321)
mod The modulus function
OCSP Online Certificate Status Protocol
OID Object Identifier (see RFC 5280)
prf Pseudo Random Function
RADIUS Remote Authentication Dial In User Service (see RFC 2865)
RCA Remove Change Authorization SW_ILS (see FC-SW-5)
SA Security Association
SADB Security Association Database
SHA-1 Secure Hash Algorithm (see ANSI X9.30.2-1997)
SFC Stage Fabric Configuration SW_ILS (see FC-SW-5)
SPI Security Parameter Index
SSB Server Session Begin CT Request (see FC-GS-6)
SSE Server Session End CT Request (see FC-GS-6)
SW_ILS Switch Internal Link Service (see FC-SW-5)
SW_ACC Switch Fabric Link Service Accept (see FC-SW-5)
SW_RJT Switch Fabric Link Service Reject (see FC-SW-5)
S_ID Source address identifier (see FC-FS-3)
SRP Secure Remote Password (see RFC 2945)
T_ID Transaction Identifier
TCP Transmission Control Protocol (see RFC 793)
UDP User Datagram Protocol (see RFC 768)
UFC Update Fabric Configuration SW_ILS (see FC-SW-5)
UTC Universal Time Code

3.3 Editorial conventions

In this standard, a number of conditions, mechanisms, sequences, parameters, events, states, or similar terms are printed with the first letter of each word in uppercase and the rest lowercase (e.g., Exchange, Class). Any lowercase uses of these words have the normal technical English meanings.

Lists sequenced by letters (e.g., a-red, b-blue, c-green) show no priority relationship between the listed items. Numbered lists (e.g., 1-red, 2-blue, 3-green) show a priority ordering between the listed items.

The ISO convention of numbering is used (i.e., the thousands and higher multiples are separated by a space and a comma is used as the decimal point.) A comparison of the American and ISO conventions is shown in table 1.

Table 1 – ISO and American conventions

ISO	American
0,6	0.6
1 000	1,000
1 323 462,9	1,323,462.9

In case of any conflict between figure, table, and text, the text, then tables, and finally figures take precedence.

In all of the figures, tables, and text of this document, the most significant bit of a binary quantity is shown on the left side.

When the value of a bit or field is not relevant, x or xx appears in place of a specific value.

Unless stated otherwise, numbers that are not immediately followed by lower-case b or h are decimal values, numbers immediately followed by lower-case b (xxb) are binary values, and numbers or upper case letters immediately followed by lower-case h (xxh) are hexadecimal values.

A numeric range is indicated by listing the two extremes separated by ".." (e.g., "1 .. 6" indicates the range from 1 to 6, including 1 and 6).

Optional parameters are enclosed in square brackets (e.g., [X] indicates that X is an optional parameter), except in the clause 7 policy enforcement definitions, where square brackets enclose restricted identifiers (e.g., [N(α)] indicates a restriction on access for the Switch with Node_Name α. See table 141 for additional examples).

The notation SK { ... } is used in clause 6 to indicate encrypted and integrity protected IKE Payloads (see 6.1.2).

3.4 Keywords

3.4.1 expected: A keyword used to describe the behavior of the hardware or software in the design models assumed by this standard. Other hardware and software design models may also be implemented.

3.4.2 ignored: When speaking of a bit, byte, word, field, or code value, this keyword indicates that the object is unused. The contents or value of an ignored bit, byte, word, field or code value shall not be examined by the receiving device and may be set to any value by the transmitting device. When speaking of a protocol step or event, this keyword indicates that the recipient of the protocol step or event shall take no action.

3.4.3 invalid: A keyword used to describe an illegal or unsupported bit, byte, word, field or code value. Receipt of an invalid bit, byte, word, field or code value shall be reported as an error.

3.4.4 Invocable: A keyword referring to a feature or parameter that is required to be implemented by an entity to which a request may be sent, but it is not required to be used by a requesting entity.

3.4.5 mandatory: A keyword indicating an item that is required to be implemented as defined in this standard.

3.4.6 may: A keyword that indicates flexibility of choice with no implied preference (equivalent to "may or may not").

3.4.7 may not: A keyword that indicates flexibility of choice with no implied preference (equivalent to "may or may not").

3.4.8 obsolete: A keyword indicating that an item was defined in prior Fibre Channel standards but has been removed from this standard.

3.4.9 optional: A keyword that describes features that are not required to be implemented by this standard. However, if any optional feature defined by this standard is implemented, then it shall be implemented as defined in this standard.

3.4.10 prohibited: A keyword referring to a feature that shall not be used between entities compliant with this standard.

3.4.11 reserved: A keyword referring to bits, bytes, words, fields and code values that are set aside for future standardization. A reserved bit, byte, word or field shall be set to zero, or in accordance with a future extension to this standard. Recipients are not required to check reserved bits, bytes, words or fields for zero values. Receipt of reserved code values in defined fields shall be reported as error.

3.4.12 restricted: A keyword referring to bits, bytes, words, and fields that are set aside for use in other Fibre Channel standards. A restricted bit, byte, word, or field shall be treated as a reserved bit, byte, word or field for the purposes of the requirements defined in this standard.

3.4.13 shall: A keyword indicating a mandatory requirement. Designers are required to implement all such mandatory requirements to ensure interoperability with other products that conform to this standard.

3.4.14 should: A keyword indicating flexibility of choice with a strongly preferred alternative; equivalent to the phrase “it is strongly recommended”.

3.4.15 x or **xx:** The value of the bit or field is not relevant.

3.5 T10 Vendor ID

A T10 Vendor ID shall be a string of one to eight characters that is recorded in an informal list of Vendor IDs maintained by INCITS Technical Committee T10 (see http://www.t10.org).

A field described as containing a T10 Vendor ID shall contain the first character of the T10 Vendor ID in the first byte of the field, and successive characters of the T10 Vendor ID in successive bytes of the field. Any bytes of the field not filled by characters of the T10 Vendor ID shall be filled with ASCII space characters (20h).

3.6 Sorting

3.6.1 Sorting alphabetic keys

An alphabetic key is an ordered series of bytes containing printable ASCII characters. Alphabetic keys are sorted by comparison of the values in their corresponding bytes (i.e., bytes at the same offset within the key):

a) one alphabetic key is equal to another alphabetic key if the two keys are the same length and each byte of the one is equal to the corresponding byte of the other; and

b) one alphabetic key is greater than another alphabetic key if:

   A) the first byte of the one alphabetic key in which the two keys differ is greater than the corresponding byte in the other alphabetic key; or

   B) there are no corresponding bytes of the two alphabetic keys that differ, but the one alphabetic key is longer than the other alphabetic key.

NOTE 1 – Unlike dictionary sorting, alphabetic key sorting compares the actual ASCII values of alphabetic characters of different case (i.e., a lower case character is not equal to its corresponding upper case character).

3.6.2 Sorting numeric keys

A numeric key is an unsigned integer of arbitrary size. Numeric keys are sorted by numeric comparison of their values.

3.7 Terminate communication

This standard often uses language of the form “If the Authentication fails the entity shall terminate the communication.” This means that any further communication between the two involved entities is forbidden. More specifically, when an Authentication Transaction occurs in specific states of a state machine, the meaning is as follows:

a) When an Authentication Transaction is performed between E_Ports in state P17a (see 8.9.1) or in state P22 (see 8.9.3), terminate communication means going in state P16 (Invalid Attachment).

b) When an Authentication Transaction is performed between an E_Port and a B_Port in state P19 (see 8.9.2), terminate communication means going in state P16 (Invalid Attachment).

c) When an Authentication Transaction is performed between VE_Ports in state $P24^{(k)}a$ (see 8.9.3), terminate communication means going in state $P26^{(k)}$ (Logical Isolation).

d) When an Authentication Transaction is performed between two Domain Controller addresses (see FC-SW-5), terminate communication means that no further communication occurs between the involved Domain Controller addresses.

e) When an Authentication Transaction is performed between an N_Port or a VN_Port and another N_Port or VN_Port, terminate communication means that no further communication occurs between the two entities.

f) When an Authentication Transaction is performed between an N_Port and an F_Port, terminate communication means that no further communication occurs between the involved FC_Ports (the situation is equivalent to a Fabric Logout).

g) When an Authentication Transaction is performed between a VN_Port and a VF_Port, terminate communication means that no further communication occurs between the involved Virtual FC_Ports (the situation is equivalent to a Fabric Logout in that particular Virtual Fabric).

3.8 State machine notation

State machines in this standard use the style shown in figure 1.

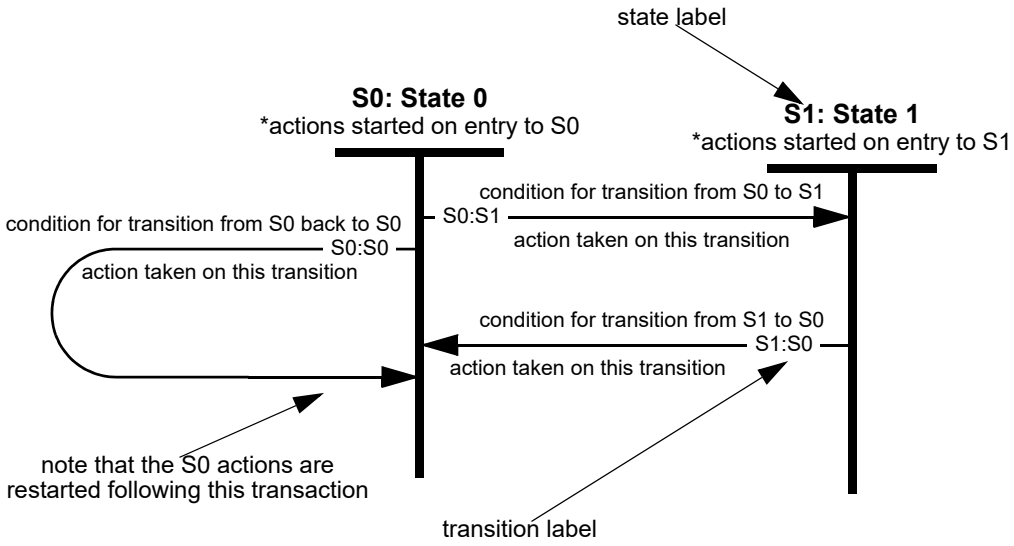


Figure 1 – State machine example

These state machines make three assumptions:

a) Time elapses only within discrete states.

b) State transitions are logically instantaneous, so the only actions taken during a transition are setting flags and variables and sending signals. These actions complete before the next state is entered.

c) Every time a state is entered, the actions of that state are started. This means that a transition that points back to the same state repeats the actions from the beginning. All the actions started upon entry complete before any tests are made to exit the state.

3.9 Using numbers in hash functions and concatenation functions

When a numeric value is used as a bit string argument to a function (e.g., inputs to hash functions and concatenation functions), unless otherwise specified, the numeric value is represented as a bit string as follows:

a) if the numeric value used as a bit string argument to a function is determined by reference to a field with size determined by this standard, its bit string representation is the entire field that contained it; and

b) if the numeric value used as a bit string argument to a function is not determined by reference to a field with size determined by this standard and the numeric value is the output of a function or the result of an arithmetic computation, the bit string representation of the numeric value is the bit string that:

   A) has the same value when interpreted as a binary number; and

B) has as many bits as the shortest bit string that is capable of representing all possible outputs of the function or computation.