ISO/IEC/IEEE 8802-21:2018-04 (E)

Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 21: Media independent services framework

Contents

1. Overview 16
   1.1 Scope 16
   1.2 Purpose 16
   1.3 General 16
   1.4 Assumptions 18
   1.5 Media independence 18

2. Normative references 19

3. Definitions 22

4. Abbreviations and acronyms 26

5. General architecture 31
   5.1 Introduction 31
   5.2 General design principles 33
   5.3 MISF service overview 33
   5.4 Media independent service reference framework 36
   5.5 MISF reference models for link-layer technologies 38
   5.6 Service access points (SAPs) 44
   5.7 MIS protocol 46

6. MISF services 48
   6.1 General 48
   6.2 Service management 48
   6.3 Media independent event service 50
   6.4 Media independent command service 54
   6.5 Media independent information service 58

7. Service access point (SAPs) and primitives 70
   7.1 Introduction 70
   7.2 SAPs 71
   7.3 MIS_LINK_SAP primitives 73
   7.4 MIS_SAP primitive 85
   7.5 MIS_NET_SAP primitive 136

8. Media independent service protocol 138
   8.1 Introduction 138
   8.2 MIS protocol description 138
   8.3 MIS protocol identifier 150
   8.4 MIS protocol frame format 152
   8.5 Message parameter TLV encoding 159
   8.6 MIS protocol messages 159

9. MIS protocol protection 179
   9.1 Protection established through MIS (D)TLS 179
   9.2 Key establishment through an MIS service access authentication 180
   9.3 MIS message protection mechanisms for EAP-generated SAs 189
   9.4 Common procedures 196
   9.5 Group manipulation for group addressed messages 197
   9.6 Group addressed message protection 223

10. Proactive authentication 231
10.1 Media-specific proactive authentication 232
10.2 Bundling media access authentication with MIS service access authentication 233

Annex A (informative) Bibliography 236

Annex B (normative) Quality of service mapping 237
B.1 Generic IEEE 802.21 QoS flow diagram 238
B.2 Generic IEEE 802.21 QoS parameter mappings 239
B.3 Deriving generic IEEE 802.21 QoS parameters 241

Annex C (normative) Mapping media independent service (MIS) messages to reference points 244

Annex D (normative) Media-specific mapping for service access points (SAPs) 245
D.1 MIS_LINK_SAP mapping to specific technologies 245
D.2 Mapping from MIS_LINK_SAP to media-specific SAPs 247

Annex E (normative) Data type definitions 249
E.1 General 249
E.2 Basic data types 249
E.3 Derived data types 251

Annex F (normative) Information element identifiers 282

Annex G (normative) Media independent information service (MIIS) basic schema 283

Annex H (informative) Making user extensions to media independent information service (MIIS) schema 284

Annex I (normative) IEEE 802.21 management information base (MIB) 285
I.1 Parameters requiring MIB definition 285
I.2 IEEE 802.21 MIB definition 286

Annex J (informative) Example media independent service (MIS) message fragmentation 287
J.1 Example of original MIS message fragmentation 287
J.2 Calculation of securityOverhead when there is an MIS security association (SA) 287

Annex K (normative) Media independent service (MIS) protocol message code assignments 290

Annex L (normative) Protocol implementation conformance statement (PICS) proforma 294
L.1 Introduction 294
L.2 Scope 294
L.3 Conformance 294
L.4 Instructions 294
L.5 Identification of the implementation 297
L.6 Identification of the protocol 297
L.7 Identification of corrigenda to the protocol 297
L.8 PICS proforma tables 297

Annex M (informative) Authentication and key distribution procedures 303
M.1 Media independent service (MIS) service access authentication 303
M.2 Push key distribution 305
M.3 Proactive authentication 306
M.4 Optimized pull key distribution 307
M.5 Termination phase 308

Annex N (informative) Protection through transport protocols 309
N.1 Protection through layer 2 309
N.2 Protection through internet protocol security (IPsec) 309

Annex O (informative) Examples of fragmented group key block (GKB) operation 310

Annex P (normative) Use of Bloom Filter for certificate revocation 312
P.1 Calculating Bloom Filter output for revoked certificates 312
P.2 Certificate revocation check 312
P.3 False positive case 312

List of Figures

Figure 1—MIS services and their initiations 18
Figure 2—Group communication functional entities 32
Figure 3—MISF communication model 37
Figure 4—General MISF reference model and SAPs 39
Figure 5—Types of MISF relationships 40
Figure 6—MIS reference model for IEEE 802.3 41
Figure 7—MIS reference model for IEEE 802.11 42
Figure 8—MIS reference model for IEEE 802.16 42
Figure 9—MIS reference model for 3GPP systems 43
Figure 10—MIS reference model for 3GPP2 systems 44
Figure 11—Relationship between different MISF SAPs 45
Figure 12—Link events and MIS events 51
Figure 13—Remote MIS events 51
Figure 14—MIS events subscription and flow 52
Figure 15—Link commands and MIS commands 55
Figure 16—Remote MIS command 56
Figure 17—Command service flow 57
Figure 18—Depicting a list of neighboring networks with information elements 63
Figure 19—TLV representation of information elements 64
Figure 20—MIIS information flow 70
Figure 21—State machines interactions 140
Figure 22—Transaction timers state machine 145
Figure 23—Transaction source state machine 146
Figure 24—Transaction destination state machine 147
Figure 25—ACK requestor state machine 148
Figure 26—ACK responder state machine 149
Figure 27—MIS protocol general frame format 152
Figure 28—MIS protocol header format 152
Figure 29—Protected MIS frame format 154
Figure 30—MIS PDU during TLS handshake 155
Figure 31—MIS PDU in existence of MIS SA by TLS 155
Figure 32—MIS PDU protected by an EAP-generated MIS SA 156
Figure 33—MIS PDU upon Transport Address Change 156
Figure 34—MIS PDU protected by a GKB-generated MIS SA with a signature TLV 156
Figure 35—MIS PDU protected by digital signature only 157
Figure 36—Fragmented MIS protocol frame format 157
Figure 37—Protected fragmented MIS protocol frame format 158
Figure 38—Message parameter TLV encoding 159
Figure 39—The TLV encoding for the vendor-specific TLV (Type = 111) 159
Figure 40—Protocol stack of service access authentication (with an EAP server) 180
Figure 41—Main stages with MN initiated EAP execution 182
Figure 42—Main stages with PoS initiated EAP execution 183
Figure 43—Main stages with MN initiated ERP execution 184
Figure 44—Main stages with PoS initiated ERP execution (1) 185
Figure 45—Main stages with PoS initiated ERP execution (2) 186
Figure 46—MIS Key Hierarchy 188
Figure 47—MIS PDU protection procedure 191
Figure 48—AES-CCM nonce construction 192
Figure 49—Format of *B0* 192
Figure 50—Format of counter *Ctr(i)* 193
Figure 51—Security TLV for AES-CCM 193
Figure 52—Security TLV for AES CBC and HMAC-SHA1-96 195
Figure 53—Security TLV for HMAC-SHA1-96 195
Figure 54—Security TLV for AES-CMAC 196

Figure 55—Sending and receiving protected MIS PDU 197
Figure 56—A group of management tree of depth 3 199
Figure 57—Three complete subtrees for the group with nodes 000, 001, 010, 011, 101, and 111 200
Figure 58—GKB for the group with nodes 000, 001, 010, 011, 101, and 111 202
Figure 59—Flow diagram of the verify group code generation 203
Figure 60—Flow diagram of the group key wrapping 204
Figure 61—Selection of *master group key unwrapping* or *no group key procedures* 205
Figure 62—Flow diagram of the group key unwrapping 205
Figure 63—Flow diagram of *no group key data procedure* 206
Figure 64—Flow diagram of the *master group key unwrapping procedure 1* 207
Figure 65—Flow diagram of the *master group key unwrapping procedure 2* 209
Figure 66—Flow diagram of the *master group key unwrapping procedure 3* 210
Figure 67—Example of group manipulation distribution using multicast mechanisms 213
Figure 68—Summary of steps performed by MIS user of PoS with group manager 215
Figure 69—Summary of steps performed by MIS user of PoS with group manager (continued from Figure 68) 216
Figure 70—Flow diagram of CreateCompleteSubtree and CreateCompleteSubtreeFragments procedure 217
Figure 71—Summary of steps performed by MISF of PoS with group manager 219
Figure 72—Summary of steps performed by the recipient MISF 222
Figure 73—Key derivation example 223
Figure 74—MIS PDU protection procedure with the GKB-generated MIS SA 225
Figure 75—Format of *B0* with associated data 226
Figure 76—Signing with confidentiality 228
Figure 77—Signing without confidentiality 228
Figure 78—Signature verification with confidentiality 229
Figure 79—Signature verification without confidentiality 229
Figure 80—Protocol stack for MIS supported proactive authentication 232
Figure 81—Protocol stack for MIS supported optimized pull key distribution with two points of service 232
Figure 82—Key hierarchy for bundle case 235
Figure B.1—An example flow for setting application QoS requirements 239
Figure E.1—Encoding example of a LIST with two LINK_ID elements 250
Figure J.1—MIS fragmentation example for Maximum Transmission Unit (MTU) of 1500 octets 287
Figure J.2—Example of protected MIS fragment message 289
Figure M.1—Mobile initiated access authentication phase 303
Figure M.2—Network initiated access authentication phase 304
Figure M.3—Push key distribution 305
Figure M.4—Proactive authentication 306
Figure M.5—Optimized pull key distribution 307
Figure M.6—Mobile node (MN) initiated termination phase 308
Figure O.1—Example of fragmented complete subtrees with Subgroup Ranges 311
Figure P.1—Bloom Filter example (k = 3, m = 32) 312

List of Tables

Table 1—Summary of reference points 38
Table 2—MIS protocol Ethernet type 47
Table 3—Service management primitives 49
Table 4—Link events 53
Table 5—MIS events 54
Table 6—Link commands 58
Table 7—MIS commands 58
Table 8—Information element containers 60
Table 9—Information elements 61
Table 10—Information element namespace 64
Table 11—IE_CONTAINER_LIST_OF_NETWORKS definition 65
Table 12—IE_CONTAINER_NETWORKS definition 66
Table 13—IE_CONTAINER_POA definition 67
Table 14—MIS_LINK_SAP primitives 71
Table 15—MIS_NET_SAP primitive 71
Table 16—MIS_SAP primitives 72
Table 17—State machine symbols 141
Table 18—Inter-state-machine variables 142
Table 19—Exported state machine variables 142
Table 20—State Machines to be searched for incoming message 143
Table 21—State Machines to be searched for outgoing message 143
Table 22—Description of MIS protocol header fields 153
Table 23—Valid combination of S-bit and security-related TLVs 154
Table 24—Cryptographic algorithms 188
Table 25—Ciphersuites 189
Table 26—Device key assignments for recipients through a depth-3 group management tree 199
Table 27—Group ciphersuites 230
Table 28—Group key distribution ciphersuites 231
Table B.1—QoS parameter mapping for IEEE 802.11 240
Table B.2—QoS parameter mapping for IEEE 802.16 and 3GPP2 241
Table B.3—QoS parameter mapping for 3GPP 241
Table C.1—Mapping MIS messages to reference points 244
Table D.1—MIS_Link_SAP/IEEE 802.16 primitives mapping 245
Table D.2—MIS_LINK_SAP/IEEE 802.11/IEEE 802.3/IEEE 802.1Q primitives mapping 246
Table D.3—MIS_LINK_SAP/3GPP/3GPP2 primitives mapping 247
Table E.1—Basic data types 249
Table E.2—General data types 251
Table E.3—Data types for address 252
Table E.4—Data types for links 253
Table E.5—Link actions 261
Table E.6—Link action attributes 261
Table E.7—Link down reason code 262
Table E.8—Link going down reason code 262
Table E.9—Data types for QoS 263
Table E.10—Data types for location 263
Table E.11—Value field format of PoA location information (geospatial location) 264
Table E.12—Data types for IP configuration 265
Table E.13—Data types for information elements 265
Table E.14—Network type and subtype representation 270
Table E.15—Data types for binary query 272
Table E.16—Data type for RDF query 273
Table E.17—Data type for binary information query response 273
Table E.18—Data type for RDF information query response 273
Table E.19—Data type for MISF identification 274
Table E.20—Data type for MIS capabilities 274
Table E.21—Data type for MIS registration 276
Table E.22—Data type for handover operations 277
Table E.23—Data type for MIS_NET_SAP primitives 277
Table E.24—Data type for security 277
Table E.25—Delivery types for delivery of control messages 281
Table F.1—Information element identifier values 282
Table J.1—Protection overhead for EAP-generated SAs 288
Table K.1—AID assignments 290
Table K.2—Type values for TLV encoding 291