

# ISO/IEC/IEEE 8802-1X:2021-12 (E)

## Telecommunications and exchange between information technology systems - Requirements for local and metropolitan area networks - Part 1X: Port-based network access control

---

### Contents

Page

1.	Overview.....	16
1.1	Scope.....	16
1.2	Purpose.....	16
1.3	Introduction.....	16
1.4	Provisions of this standard.....	17
2.	Normative references.....	19
3.	Definitions.....	21
4.	Acronyms and abbreviations.....	26
5.	Conformance.....	28
5.1	Requirements terminology.....	28
5.2	Protocol Implementation Conformance Statement.....	28
5.3	Conformant systems and system components.....	29
5.4	PAE requirements.....	29
5.5	PAE options.....	30
5.6	Supplicant requirements.....	30
5.7	Supplicant options.....	30
5.8	Authenticator requirements.....	30
5.9	Authenticator options.....	30
5.10	MKA requirements.....	31
5.11	MKA options.....	31
5.12	Virtual port requirements.....	32
5.13	Virtual port options.....	33
5.14	Announcement transmission requirements.....	33
5.15	Announcement transmission options.....	33
5.16	Announcement reception requirements.....	33
5.17	Announcement reception options.....	33
5.18	Requirements for SNMP access to the PAE MIB.....	34
5.19	Options for SNMP access to the PAE MIB.....	34
5.20	PAC requirements.....	34
5.21	System recommendations.....	34
5.22	Prohibitions.....	34
5.23	Requirement for YANG data model of a PAE.....	34
5.24	Options for YANG data model of a PAE.....	34
6.	Principles of port-based network access control operation.....	36
6.1	Port-based network access control architecture.....	37
6.2	Key hierarchy.....	38
6.3	Port Access Entity (PAE).....	43
6.4	Port Access Controller (PAC).....	46
6.5	Link aggregation.....	48
6.6	Use of this standard by IEEE Std 802.11.....	49
7.	Port-based network access control applications.....	50
7.1	Host access with physically secure LANs.....	50
7.2	Infrastructure support with physically secure LANs.....	53
7.3	Host access with MACsec and point-to-point LANs.....	55

7.4	Use with MACsec to support infrastructure LANs .....	56
7.5	Host access with MACsec and a multi-access LAN.....	58
7.6	Group host access with MACsec .....	61
7.7	Use with MACsec to support virtual shared media infrastructure LANs.....	62
8.	Authentication using EAP .....	65
8.1	PACP Overview.....	66
8.2	Example EAP exchanges .....	67
8.3	PAE higher layer interface.....	68
8.4	PAE Client interface .....	69
8.5	EAPOL transmit and receive .....	71
8.6	Supplicant and Authenticator PAE timers .....	71
8.7	Supplicant PACP state machine, variables, and procedures.....	72
8.8	Supplicant PAE counters .....	72
8.9	Authenticator PACP state machine, variables, and procedures.....	73
8.10	Authenticator PAE counters .....	74
8.11	EAP methods .....	75
9.	MACsec Key Agreement protocol (MKA) .....	77
9.1	Protocol design requirements.....	78
9.2	Protocol support requirements .....	79
9.3	MKA key hierarchy .....	79
9.4	MKA transport.....	82
9.5	Key server election .....	85
9.6	Use of MACsec.....	86
9.7	Cipher suite selection.....	87
9.8	SAK generation, distribution, and selection .....	88
9.9	SA assignment .....	90
9.10	SAK installation and use.....	90
9.11	Connectivity change detection.....	92
9.12	CA formation and group CAK distribution .....	92
9.13	Secure announcements.....	93
9.14	MKA participant creation and deletion .....	93
9.15	MKA participant timer values .....	94
9.16	MKA management.....	95
9.17	MKA SAK distribution examples.....	97
9.18	In-service upgrades .....	98
9.19	In-service upgrade examples .....	102
10.	Network announcements.....	105
10.1	Announcement information .....	105
10.2	Making and requesting announcements.....	108
10.3	Receiving announcements .....	110
10.4	Managing announcements .....	110
11.	EAPOL PDUs .....	112
11.1	EAPOL PDU transmission, addressing, and protocol identification.....	112
11.2	Representation and encoding of octets .....	115
11.3	Common EAPOL PDU structure.....	115
11.4	Validation of received EAPOL PDUs .....	116
11.5	EAPOL protocol version handling .....	117
11.6	EAPOL-Start.....	118

11.7	EAPOL-Logoff .....	119
11.8	EAPOL-EAP.....	119
11.9	EAPOL-Key.....	119
11.10	EAPOL-Encapsulated-ASF-Alert.....	120
11.11	EAPOL-MKA .....	120
11.12	EAPOL-Announcement.....	130
11.13	EAPOL-Announcement-Req .....	136
12.	PAE operation.....	137
12.1	Model of operation.....	137
12.2	KaY interfaces .....	139
12.3	CP state machine interfaces .....	141
12.4	CP state machine.....	142
12.5	Logon Process.....	142
12.6	CAK cache.....	146
12.7	Virtual port creation and deletion .....	147
12.8	EAPOL Transmit and Receive Process .....	148
12.9	PAE management .....	150
13.	PAE MIB .....	153
13.1	The Internet Standard Management Framework .....	153
13.2	Structure of the MIB .....	153
13.3	Relationship to other MIBs.....	153
13.4	Security considerations .....	162
13.5	Definitions for PAE MIB.....	162
14.	YANG Data Model.....	212
14.1	PAE management using YANG .....	212
14.2	Security considerations .....	213
14.3	802.1X YANG model structure .....	214
14.4	Relationship to other YANG data models .....	215
14.5	Definition of the IEEE 802.1X YANG data model .....	229
14.6	YANG data model use in network access control applications.....	261
Annex A	(normative) PICS proforma.....	266
A.1	Introduction.....	266
A.2	Abbreviations and special symbols.....	266
A.3	Instructions for completing the PICS proforma.....	267
A.4	PICS proforma for IEEE 802.1X .....	269
A.5	Major capabilities and options .....	270
A.6	PAE requirements and options .....	270
A.7	Supplicant requirements and options .....	271
A.8	Authenticator requirements and options .....	271
A.9	MKA requirements and options.....	271
A.12	Management and remote management .....	273
A.13	Virtual ports .....	273
A.10	Announcement transmission requirements .....	273
A.11	Announcement reception requirements .....	273
A.14	PAC.....	274
A.15	YANG requirements and options .....	274

Annex B (informative) Bibliography.....	275
Annex C (normative) State diagram notation.....	278
Annex D (informative) IEEE 802.1X EAP and RADIUS usage guidelines .....	280
D.1 EAP Session-Id.....	280
D.2 RADIUS Attributes for IEEE 802 Networks.....	280
Annex E (informative) Support for ‘Wake-on-LAN’ protocols.....	281
Annex F (informative) Unsecured multi-access LANs .....	282
Annex G (informative) Test vectors .....	284
G.1 KDF .....	284
G.2 CAK Key Derivation .....	285
G.3 CKN Derivation .....	285
G.4 KEK Derivation .....	286
G.5 ICK Derivation .....	286
G.6 SAK Derivation .....	287

## Figures

Figure 6-1	Port-based network access control processes.....	37
Figure 6-2	Port-based network access control with MACsec.....	38
Figure 6-3	MKA key hierarchy .....	39
Figure 6-4	Use of pairwise CAKs to distribute group SAKs .....	39
Figure 6-5	Network access control with MACsec and a multi-access LAN .....	46
Figure 6-6	-Port Access Controller.....	47
Figure 6-7	-PACs and Link Aggregation in an interface stack.....	49
Figure 6-8	SecYs and Link Aggregation in an interface stack.....	49
Figure 7-1	Network access control with a physically secure point-to-point LAN .....	50
Figure 7-2	Network access control with a physically secure point-to-point LAN .....	51
Figure 7-3	Network access controlled VLAN-aware Bridge Port with PAC.....	52
Figure 7-4	Selective relay to a physically secured unauthenticated port.....	53
Figure 7-5	Network infrastructure with a physically secure point-to-point LAN .....	54
Figure 7-6	Network access control with MACsec and a point-to-point LAN.....	55
Figure 7-7	Network access control with MACsec and a point-to-point LAN.....	56
Figure 7-8	Point-to-point LAN within a secured network.....	56
Figure 7-9	Shared media LAN within a secured network .....	57
Figure 7-10	Network access control within the network infrastructure .....	57
Figure 7-11	Network access control with MACsec and a multi-access LAN .....	58
Figure 7-12	Network access control with MACsec and a multi-access LAN .....	59
Figure 7-13	Secure and unsecured connectivity on a multi-access LAN .....	60
Figure 7-14	Group host access.....	61
Figure 7-15	Multipoint connectivity across a Provider Bridged Network .....	62
Figure 7-16	Internal organization of the MAC sublayer in a Provider Bridged Network.....	63
Figure 7-17	Secure PBN transit and access with priority selection.....	64
Figure 7-18	Secure PBN transit and with priority selection.....	64
Figure 8-1	PAEs, PACP, EAP Messages, and EAPOL PDUs .....	66
Figure 8-2	Authenticator-initiated EAP-TLS (success).....	68
Figure 8-3	Supplicant-initiated EAP exchange .....	68
Figure 8-4	PAE state machines and interfaces .....	70
Figure 8-5	PAE Timer state machines .....	72
Figure 8-6	Supplicant PACP state machine.....	73
Figure 8-7	Authenticator PACP state machine.....	74
Figure 11-1	Common EAPOL PDU structure .....	115
Figure 11-2	EAPOL Start-PDU (Protocol Version $\leq 2$ ).....	118
Figure 11-3	EAPOL Start-PDU (Protocol Version $\geq 3$ ).....	118
Figure 11-4	EAPOL-EAP Packet Body with EAP packet format.....	119
Figure 11-5	EAPOL-Key Packet Body with Key Descriptor format .....	119
Figure 11-7	MKPDU—Parameter set encoding.....	121
Figure 11-6	EAPOL-MKA Packet Body with MKPDU format.....	121
Figure 11-8	Basic Parameter Set .....	125
Figure 11-9	Live Peer List and Potential Peer List parameter sets.....	125
Figure 11-11	Distributed SAK parameter set (GCM-AES-128) .....	126
Figure 11-10	MACsec SAK Use parameter set.....	126
Figure 11-12	Distributed SAK parameter set (other MACsec Cipher Suites) .....	127
Figure 11-13	Distributed CAK parameter set.....	127
Figure 11-14	KMD parameter set.....	127
Figure 11-15	Announcement parameter set.....	128
Figure 11-16	XPN parameter set .....	128
Figure 11-17	ICV Indicator .....	128
Figure 11-18	EAPOL-Announcement .....	130
Figure 11-19	EAPOL-Announcement TLV format.....	130

Figure 11-20	NID Set TLV format .....	132
Figure 11-21	Access Information TLV format.....	132
Figure 11-22	Access Information TLV format.....	133
Figure 11-23	Key Management Domain TLV format.....	134
Figure 11-24	Organizationally Specific TLV format .....	134
Figure 11-25	Organizationally Specific Set TLV format .....	134
Figure 11-26	EAPOL-Announcement-Req (Protocol Version = 3).....	136
Figure 12-1	PAE state machines—overview and interfaces .....	138
Figure 12-2	CP state machine .....	143
Figure 12-3	PAE management information .....	152
Figure 13-1	Use of the ifStackTable.....	154
Figure 14-1	YANG model structure .....	214
Figure 14-2	YANG object hierarchy with IEEE Std 802.1X .....	214
Figure 14-3	IETF System Management YANG data model .....	216
Figure 14-4	IETF Interface Management YANG data model.....	218
Figure 14-5	Explicit Interface Model of Bridge Port .....	224
Figure 14-6	Augmented Interface Mode of Bridge Port.....	225
Figure 14-7	Bridge Port with LAG Interface stack model .....	225
Figure 14-8	Bridge Port YANG Interface stack model with MACsec.....	226
Figure 14-9	Augmented Interface Model of Bridge Port with MACsec .....	226
Figure 14-10	YANG Interface Model with MACsec and virtual ports.....	227
Figure 14-11	Explicit Interface Model of Bridge Port LAG with MACsec on members .....	227
Figure 14-12	Augmented Interface Model of Bridge Port LAG with MACsec on members .....	228
Figure 14-13	IEEE 802.1X YANG model for host (7.1).....	261
Figure 14-14	IEEE 802.1X YANG model for network access point (7.1).....	262
Figure 14-15	IEEE 802.1X YANG model for network access point (7.3).....	263

## Tables

Table 5-1	System recommendations .....	35
Table 9-1	MKA Algorithm Agility parameter values .....	81
Table 9-2	Key Server Priority values .....	85
Table 9-3	MKA Participant timer values .....	94
Table 10-1	Announcement performance parameters .....	109
Table 11-1	EAPOL group address assignments.....	113
Table 11-2	EAPOL Ethernet Type assignment.....	114
Table 11-3	EAPOL Packet Types .....	116
Table 11-4	EAPOL Packet Type Destination Addressing .....	117
Table 11-5	Descriptor Type value assignments .....	120
Table 11-6	MKA parameters—fixed width encoding.....	122
Table 11-7	MKPDU parameter sets .....	123
Table 11-8	EAPOL-Announcement TLVs .....	131
Table 11-9	Access Information .....	133
Table 13-1	Use of ifGeneralInformationGroup objects .....	154
Table 13-4	PAE managed object cross-reference table .....	155
Table 13-2	Use of ifCounterDiscontinuityGroup Object.....	155
Table 13-3	Use of ifStackGroup2 Objects .....	155
Table 13-5	PAC managed object cross-reference table .....	161
Table 14-1	PAE System cross-reference table.....	217
Table 14-2	PAE cross-reference table.....	219
Table C-1	State machine symbols.....	279