

# ISO/IEC/IEEE 8802-1X:2013-12 (E)

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

---

Contents	Page
1. Overview.....	1
1.1 Scope.....	1
1.2 Purpose.....	1
1.3 Introduction.....	2
1.4 Provisions of this standard.....	2
2. Normative references.....	4
3. Definitions.....	6
4. Acronyms and abbreviations.....	10
5. Conformance.....	12
5.1 Requirements terminology.....	12
5.2 Protocol Implementation Conformance Statement.....	12
5.3 Conformant systems and system components.....	13
5.4 PAE requirements.....	13
5.5 PAE options.....	14
5.6 Supplicant requirements.....	14
5.7 Supplicant options.....	14
5.8 Authenticator requirements.....	14
5.9 Authenticator options.....	14
5.10 MKA requirements.....	15
5.11 MKA options.....	15
5.12 Virtual port requirements.....	16
5.13 Virtual port options.....	16
5.14 Announcement transmission requirements.....	16
5.15 Announcement transmission options.....	17
5.16 Announcement reception requirements.....	17
5.17 Announcement reception options.....	17
5.18 Requirements for SNMP access to the PAE MIB.....	17
5.19 Options for SNMP access to the PAE MIB.....	17
5.20 PAC requirements.....	17
5.21 System recommendations.....	18
5.22 Prohibitions.....	18
6. Principles of port-based network access control operation.....	19
6.1 Port-based network access control architecture.....	19
6.2 Key hierarchy.....	21
6.3 Port Access Entity (PAE).....	25
6.4 Port Access Controller (PAC).....	29
6.5 Link aggregation.....	31
6.6 Use of this standard by IEEE Std 802.11.....	32

7.	Port-based network access control applications .....	33
7.1	Host access with physically secure LANs .....	33
7.2	Infrastructure support with physically secure LANs .....	36
7.3	Host access with MACsec and point-to-point LANs.....	38
7.4	Use with MACsec to support infrastructure LANs .....	39
7.5	Host access with MACsec and a multi-access LAN.....	41
7.6	Group host access with MACsec .....	44
7.7	Use with MACsec to support virtual shared media infrastructure LANs.....	45
8.	Authentication using EAP .....	48
8.1	PACP Overview.....	49
8.2	Example EAP exchanges .....	50
8.3	PAE higher layer interface.....	51
8.4	PAE Client interface .....	52
8.5	EAPOL transmit and receive .....	54
8.6	Supplicant and Authenticator PAE timers .....	54
8.7	Supplicant PACP state machine, variables, and procedures.....	55
8.8	Supplicant PAE counters .....	55
8.9	Authenticator PACP state machine, variables, and procedures.....	57
8.10	Authenticator PAE counters .....	58
8.11	EAP methods .....	58
9.	MACsec Key Agreement protocol (MKA) .....	60
9.1	Protocol design requirements.....	61
9.2	Protocol support requirements.....	62
9.3	MKA key hierarchy .....	62
9.4	MKA transport.....	64
9.5	Key server election .....	67
9.6	Use of MACsec.....	68
9.7	Cipher suite selection.....	69
9.8	SAK generation, distribution, and selection .....	69
9.9	SA assignment .....	71
9.10	SAK installation and use.....	72
9.11	Connectivity change detection.....	73
9.12	CA formation and group CAK distribution .....	73
9.13	Secure announcements.....	74
9.14	MKA participant creation and deletion .....	74
9.15	MKA participant timer values .....	75
9.16	MKA management.....	76
9.17	MKA SAK distribution examples.....	78
10.	Network announcements.....	80
10.1	Announcement information .....	80
10.2	Making and requesting announcements.....	83
10.3	Receiving announcements .....	85
10.4	Managing announcements .....	85
11.	EAPOL PDUs.....	87
11.1	EAPOL PDU transmission, addressing, and protocol identification.....	87
11.2	Representation and encoding of octets .....	89
11.3	Common EAPOL PDU structure.....	90
11.4	Validation of received EAPOL PDUs .....	91
11.5	EAPOL protocol version handling .....	92
11.6	EAPOL-Start.....	93
11.7	EAPOL-Logoff.....	94
11.8	EAPOL-EAP.....	94
11.9	EAPOL-Key.....	94
11.10	EAPOL-Encapsulated-ASF-Alert.....	95

11.11	EAPOL-MKA .....	95
11.12	EAPOL-Announcement .....	104
11.13	EAPOL-Announcement-Req .....	109
12.	PAE operation .....	110
12.1	Model of operation .....	110
12.2	KaY interfaces .....	112
12.3	CP state machine interfaces .....	114
12.4	CP state machine .....	114
12.5	Logon Process .....	116
12.6	CAK cache .....	118
12.7	Virtual port creation and deletion .....	119
12.8	EAPOL Transmit and Receive Process .....	120
12.9	PAE management .....	123
13.	PAE MIB .....	126
13.1	The Internet Standard Management Framework .....	126
13.2	Structure of the MIB .....	126
13.3	Relationship to other MIBs .....	126
13.4	Security considerations .....	134
13.5	Definitions for PAE MIB .....	135
Annex A	(normative) PICS proforma .....	181
A.1	Introduction .....	181
A.2	Abbreviations and special symbols .....	181
A.3	Instructions for completing the PICS proforma .....	182
A.4	PICS proforma for IEEE 802.1X .....	184
A.5	Major capabilities and options .....	185
A.7	Supplicant requirements and options .....	186
A.6	PAE requirements and options .....	186
A.8	Authenticator requirements and options .....	187
A.9	MKA requirements and options .....	188
A.12	Management and remote management .....	189
A.10	Announcement transmission requirements .....	189
A.11	Announcement reception requirements .....	189
A.13	Virtual ports .....	190
A.14	PAC .....	190
Annex B	(informative) Bibliography .....	191
Annex C	(normative) State diagram notation .....	193
Annex D	(normative) Basic architectural concepts and terms .....	195
D.1	Protocol entities, peers, layers, services, and clients .....	195
D.2	Service interface primitives, parameters, and frames .....	195
D.3	Layer management interfaces .....	196
D.4	Service access points, interface stacks, and ports .....	196
D.5	Media independent protocols and shims .....	197
D.6	MAC Service clients .....	197
D.7	Stations and systems .....	198
D.8	Connectionless connectivity and connectivity associations .....	198

Annex E (informative) IEEE 802.1X EAP and RADIUS usage guidelines.....	199
E.1    EAP Session-Id .....	199
E.2    RADIUS Attributes for IEEE 802 Networks.....	199
Annex F (informative) Support for 'Wake-on-LAN' protocols .....	200
Annex G (informative) Unsecured multi-access LANs.....	201
Annex H (informative) Test vectors .....	203
H.1    KDF .....	203
H.2    CAK Key Derivation .....	203
H.3    CKN Derivation .....	204
H.4    KEK Derivation .....	204
H.5    ICK Derivation .....	204
H.6    SAK Derivation .....	205
Annex K (informative) KGG'rkv'qh'r ct vkr cpw.....	208