

ISO/IEC 9594-8:2017-05 (E)

Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate framework s

CONTENTS

	<i>Page</i>
1 Scope	1
2 Normative references.....	1
2.1 Identical Recommendations International Standards	1
2.2 Paired Recommendations International Standards equivalent in technical content.....	2
2.3 Recommendations	2
2.4 Other references	2
3 Definitions	2
3.1 OSI Reference Model security architecture definitions.....	2
3.2 Baseline identity management terms and definitions	3
3.3 Directory model definitions	3
3.4 Access control framework definitions.....	3
3.5 Public-key and attribute certificate definitions.....	3
4 Abbreviations	7
5 Conventions.....	8
6 Frameworks overview	8
6.1 Digital signatures	9
6.2 Public-key cryptography and cryptographic algorithms.....	10
6.3 Distinguished encoding of basic encoding rules	11
6.4 Applying distinguished encoding.....	12
6.5 Using repositories.....	12
7 Public keys and public-key certificates	13
7.1 Introduction	13
7.2 Public-key certificate.....	13
7.3 Public-key certificate extensions.....	15
7.4 Types of public-key certificates	16
7.5 Trust anchor	16
7.6 Entity relationship	17
7.7 Certification path.....	18
7.8 Generation of key pairs	19
7.9 Public-key certificate creation.....	19
7.10 Certificate revocation list	20
7.11 Uniqueness of names.....	22
7.12 Indirect CRLs	22
7.13 Repudiation of a digital signing	24
8 Trust models.....	24
8.1 Three-cornered trust model	24
8.2 Four cornered trust model	25
9 Public-key certificate and CRL extensions.....	26
9.1 Policy handling.....	26
9.2 Key and policy information extensions	29
9.3 Subject and issuer information extensions	35
9.4 Certification path constraint extensions	37
9.5 Basic CRL extensions	41
9.6 CRL distribution points and delta CRL extensions	49
10 Delta CRL relationship to base.....	53

11	Authorization and validation lists.....	55
11.1	Authorization and validation list concept.....	55
11.2	The authorizer	55
11.3	Authorization and validation list syntax.....	55
11.4	Authorization and validation restrictions	57
12	Certification path processing procedure	57
12.1	Path processing inputs.....	57
12.2	Path processing outputs.....	58
12.3	Path processing variables	59
12.4	Initialization step.....	59
12.5	Public-key certificate processing.....	59
13	PKI directory schema	62
13.1	PKI directory object classes and name forms.....	62
13.2	PKI directory attributes	63
13.3	PKI directory matching rules	66
13.4	PKI directory syntax definitions.....	71
14	Attribute certificates	73
14.1	Attribute certificate structure.....	73
14.2	Delegation paths.....	76
14.3	Attribute certificate revocation lists	76
15	Attribute authority, source of authority and certification authority relationship	77
15.1	Privilege in attribute certificates.....	79
15.2	Privilege in public-key certificates.....	79
16	PMI models	79
16.1	General model	79
16.2	Control model.....	81
16.3	Delegation model	81
16.4	Group assignment model.....	82
16.5	Roles model.....	83
16.6	Recognition of Authority Model	84
16.7	XML privilege information attribute.....	88
16.8	Permission attribute and matching rule	89
17	Attribute certificate and attribute certificate revocation list extensions	89
17.1	Basic privilege management extensions.....	90
17.2	Privilege revocation extensions.....	93
17.3	Source of authority extensions	95
17.4	Role extensions	97
17.5	Delegation extensions	98
17.6	Recognition of authority extensions.....	103
17.7	Use of basic CRL extension for ACRLs	105
18	Delegation path processing procedure.....	109
18.1	Basic processing procedure	109
18.2	Role processing procedure	110
18.3	Delegation processing procedure	110
19	PMI directory schema.....	112
19.1	PMI directory object classes	113
19.2	PMI directory attributes	114
19.3	PMI general directory matching rules	116

20	Protocol support for public-key and privilege management infrastructures	118
20.1	General syntax.....	118
20.2	Wrapping of non-encrypted protocol data units.....	118
20.3	Wrapping of encrypted protocol data unit.....	119
20.4	Check of PKI-PMI-Wrapper protocol elements.....	121
20.5	PKI-PMI-Wrapper error codes.....	122
21	Authorization and validation list management	123
21.1	General	123
21.2	Defined protocol data unit (PDU) types.....	123
21.3	Checking of received PDU.....	123
21.4	Authorization and validation management protocol	124
21.5	Certification authority subscription protocol.....	130
22	Trust broker protocol.....	137
	Annex A – Public-key and attribute certificate frameworks.....	140
	Annex B – Reference definition of cryptographic algorithms	176
	Annex C – Certificate extension attribute types	182
	C.1 Certificate extension attribute concept	182
	C.2 Formal specification for certificate extension attribute types.....	182
	Annex D – External ASN.1 modules.....	190
	Annex E – CRL generation and processing rules	199
	E.1 Introduction	199
	E.2 Determine parameters for CRLs.....	200
	E.3 Determine CRLs required	201
	E.4 Obtain CRLs.....	202
	E.5 Process CRLs	202
	Annex F – Examples of delta CRL issuance.....	206
	Annex G – Privilege policy and privilege attribute definition examples	208
	G.1 Introduction	208
	G.2 Sample syntaxes	208
	G.3 Privilege attribute example.....	212
	Annex H – An introduction to public key cryptography ²⁾	213
	Annex I – Examples of use of certification path constraints	215
	I.1 Example 1: Use of basic constraints.....	215
	I.2 Example 2: Use of policy mapping and policy constraints	215
	I.3 Use of name constraints extension	215
	Annex J – Guidance on determining for which policies a certification path is valid.....	224
	J.1 Certification path valid for a user-specified policy required	224
	J.2 Certification path valid for any policy required	225
	J.3 Certification path valid regardless of policy	225
	J.4 Certification path valid for a user-specific policy desired, but not required	225
	Annex K – Key usage certificate extension issues	226
	Annex L – Deprecated extensions	227
	L.1 CRL scope extension.....	227
	Annex M – Directory concepts.....	230
	M.1 Scope.....	230
	M.2 Basic directory concepts.....	230
	M.3 Directory schema	230
	M.4 Directory distinguished names	231
	M.5 Subtrees	231

Annex N – Considerations on strong authentication	232
N.1 Introduction	232
N.2 One-way authentication.....	233
N.3 Two-way authentication	233
N.4 Three-way authentication.....	234
N.5 Five-way authentication (initiated by A).....	235
N.6 Five-way authentication (initiated by B).....	236
Annex O – Alphabetical list of information item definitions	238
Annex P – Amendments and corrigenda	241
Bibliography	242