ISO/IEC 9594-8:2020-11 (E)

Information technology - Open systems interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks

Contents

			Page
SECTION 1 – General			1
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		3
	3.1	OSI Reference Model security architecture definitions	3
	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	12
	6.4	Applying distinguished encoding	12
	6.5	Using repositories	13
SECTION 2 – PUBLIC-KEY CERTIFICATE FRAMEWORK			14
7	Public keys and public-key certificates		14
	7.1	Introduction	14
	7.2	Public-key certificate	14
	7.3	Public-key certificate extensions	17
	7.4	Types of public-key certificates	18
	7.5	Trust anchor	18
	7.6	Entity relationship	19
	7.7	Certification path	19
	7.8	Generation of key pairs	21
	7.9	Public-key certificate creation	21
	7.10	Certificate revocation list	22
	7.11	Uniqueness of names	25
	7.12	Indirect CRLs	25
	7.13	Repudiation of a digital signing	26
8	Trust models		27
	8.1	Three-cornered trust model	27
	8.2	Four cornered trust model	27
9	Public-key certificate and CRL extensions		28
	9.1	Policy handling	29
	9.2	Key and policy information extensions	31
	9.3	Subject and issuer information extensions	38
	9.4	Certification path constraint extensions	41
	9.5	Basic CRL extensions	45

9.6 CRL distribution points and delta CRL extensions 52
9.7 Authorization and validation list extensions 57
9.8 Alternative cryptographic algorithms and digital signature extensions 58
10 Delta CRL relationship to base 59
11 Authorization and validation lists 60
11.1 Authorization and validation list concept 60
11.2 The authorizer 60
11.3 Authorization and validation list syntax 61
11.4 Multiple cryptographic algorithms for authorization and validation list 62
12 Certification path processing procedure 63
12.1 Path processing inputs 63
12.2 Path processing outputs 63
12.3 Path processing variables 64
12.4 Initialization step 64
12.5 Public-key certificate processing 65
13 PKI directory schema 67
13.1 PKI directory object classes and name forms 67
13.2 PKI directory attributes 68
13.3 PKI directory matching rules 72
13.4 PKI directory syntax definitions 77
SECTION 3 – ATTRIBUTE CERTIFICATE FRAMEWORK 80
14 Attribute certificates 80
14.1 General 80
14.2 Attribute certificate syntax 81
14.3 Multiple cryptographic algorithms for attribute certificates 83
14.4 Delegation paths 83
14.5 Attribute certificate revocation lists 84
15 Attribute authority, source of authority and certification authority relationship 86
15.1 Privilege in attribute certificates 87
15.2 Privilege in public-key certificates 87
16 PMI models 87
16.1 General model 87
16.2 Control model 89
16.3 Delegation model 90
16.4 Group assignment model 90
16.5 Roles model 91
16.6 Recognition of Authority Model 93
16.7 XML privilege information attribute 96
16.8 Permission attribute and matching rule 97
17 Attribute certificate and attribute certificate revocation list extensions 97
17.1 Basic privilege management extensions 98
17.2 Privilege revocation extensions 101
17.3 Source of authority extensions 107
17.4 Role extensions 109
17.5 Delegation extensions 110
17.6 Recognition of authority extensions 114
17.7 Use of alternative digital signature algorithm and digital signature extensions 117
18 Delegation path processing procedure 118
18.1 Basic processing procedure 118
18.2 Role processing procedure 119
18.3 Delegation processing procedure 119
19 PMI directory schema 121
19.1 PMI directory object classes 121
19.2 PMI directory attributes 123
19.3 PMI general directory matching rules 125
Annex A – Public-key and attribute certificate frameworks 127
Annex B – Reference definition of cryptographic algorithms 155
Annex C Certificate extension attribute types 162

C.1 Certificate extension attribute concept 162
C.2 Formal specification for certificate extension attribute types 162
Annex D – External ASN.1 modules 171
Annex E – CRL generation and processing rules 180
E.1 Introduction 180
E.2 Determine parameters for CRLs 181
E.3 Determine CRLs required 182
E.4 Obtain CRLs 183
E.5 Process CRLs 183
Annex F – Examples of delta CRL issuance 187
Annex G – Privilege policy and privilege attribute definition examples 189
G.1 Introduction 189
G.2 Sample syntaxes 189
G.3 Privilege attribute example 193
Annex H – An introduction to public key cryptography[2)] 194
Annex I – Examples of use of certification path constraints 196
I.1 Example 1: Use of basic constraints 196
I.2 Example 2: Use of policy mapping and policy constraints 196
I.3 Use of name constraints extension 196
Annex J – Guidance on determining for which policies a certification path is valid 205
J.1 Certification path valid for a user-specified policy required 205
J.2 Certification path valid for any policy required 206
J.3 Certification path valid regardless of policy 206
J.4 Certification path valid for a user-specific policy desired, but not required 206
Annex K – Key usage certificate extension issues 207
Annex L – Deprecated extensions 208
L.1 CRL scope extension 208
Annex M – Directory concepts 211
M.1 Scope 211
M.2 The directory attribute concept 211
M.3 Basic directory concepts 211
M.4 Subtrees 212
M.5 Directory distinguished names 212
M.6 Directory schema 213
Annex N – Considerations on strong authentication 214
N.1 Introduction 214
N.2 One-way authentication 215
N.3 Two-way authentication 215
N.4 Three-way authentication 216
N.5 Five-way authentication (initiated by A) 217
N.6 Five-way authentication (initiated by B) 218
Annex O – Alphabetical list of information item definitions 220
Annex P – Amendments and corrigenda 223
Bibliography 224