ISO/IEC 9594-8:2014-03 (E)

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

Contents

		Page
1	Scope	1
2	Normative references	2
2.1	Identical Recommendations | International Standards	2
2.2	Paired Recommendations | International Standards equivalent in technical content	3
2.3	Recommendations	3
2.4	Other references	3
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	4
3.4	Access control framework definitions	4
3.5	Public-key and attribute certificate definitions	4
4	Abbreviations	7
5	Conventions	8
6	Frameworks overview	8
6.1	Digital signatures	9
6.2	Formal definitions for public-key cryptography	10
6.3	Distinguished encoding of Basic Encoding Rules	10
6.4	Applying distinguished encoding	11
7	Public-keys and public-key certificates	11
7.1	Introduction	11
7.2	Public-key certificate	12
7.3	Public-key certificate extensions	14
7.4	Types of public-key certificates	15
7.5	Trust anchor	15
7.6	Entity relationship	16
7.7	Certification path	16
7.8	Generation of key pairs	18
7.9	Public-key certificate creation	18
7.10	Certificate revocation list	18
7.11	Repudiation of a digital signing	21
8	Public-key certificate and CRL extensions	22
8.1	Policy handling	22
8.2	Key and policy information extensions	25
8.3	Subject and issuer information extensions	31
8.4	Certification path constraint extensions	33
8.5	Basic CRL extensions	37
8.6	CRL distribution points and delta-CRL extensions	46
9	Delta CRL relationship to base	52

10 Certification path processing procedure 53
10.1 Path processing inputs 53
10.2 Path processing outputs 54
10.3 Path processing variables 54
10.4 Initialization step 55
10.5 Certificate processing 55
11 PKI directory schema 57
11.1 PKI directory object classes and name forms 57
11.2 PKI directory attributes 59
11.3 PKI directory matching rules 61
11.4 PKI directory syntax definitions 66
12 Attribute Certificates 68
12.1 Attribute certificate structure 69
12.2 Attribute certification paths 71
13 Attribute Authority, SOA and Certification Authority relationship 71
13.1 Privilege in attribute certificates 73
13.2 Privilege in public-key certificates 73
14 PMI models 73
14.1 General model 73
14.2 Control model 75
14.3 Delegation model 76
14.4 Group assignment model 76
14.5 Roles model 77
14.6 Recognition of Authority Model 78
14.7 XML privilege information attribute 82
14.8 Permission attribute and matching rule 83
15 Privilege management certificate extensions 83
15.1 Basic privilege management extensions 84
15.2 Privilege revocation extensions 87
15.3 Source of Authority extensions 87
15.4 Role extensions 90
15.5 Delegation extensions 91
15.6 Recognition of Authority Extensions 95
16 Privilege path processing procedure 98
16.1 Basic processing procedure 98
16.2 Role processing procedure 99
16.3 Delegation processing procedure 99
17 PMI directory schema 102
17.1 PMI directory object classes 102
17.2 PMI Directory attributes 103
17.3 PMI general directory matching rules 105
18 Directory authentication 107
18.1 Simple authentication procedure 107
18.2 Password policy 109
18.3 Strong Authentication 119
19 Access control 122
20 Protection of Directory operations 122

Annex A – Public-Key and Attribute Certificate Frameworks 123
Annex B – Reference definition of algorithm object identifiers 153
Annex C – CRL generation and processing rules 154
C.1 Introduction 154
C.2 Determine parameters for CRLs 155
C.3 Determine CRLs required 156
C.4 Obtain CRLs 157
C.5 Process CRLs 157
Annex D – Examples of delta CRL issuance 161
Annex E – Privilege policy and privilege attribute definition examples 163
E.1 Introduction 163
E.2 Sample syntaxes 163
E.3 Privilege attribute example 167
Annex F – An introduction to public key cryptography[2)] 168
Annex G – Examples of use of certification path constraints 170
G.1 Example 1: Use of basic constraints 170
G.2 Example 2: Use of policy mapping and policy constraints 170
G.3 Use of Name Constraints Extension 170
Annex H – Guidance on determining for which policies a certification path is valid 179
H.1 Certification path valid for a user-specified policy required 179
H.2 Certification path valid for any policy required 180
H.3 Certification path valid regardless of policy 180
H.4 Certification path valid for a user-specific policy desired, but not required 180
Annex I – Key usage certificate extension issues 181
Annex J – External ASN.1 modules 182
Annex K – Use of Protected Passwords for Bind operations 190
Annex L – Examples of password hashing algorithms 191
L.1 Null Hashing method 191
L.2 MD5 method 191
L.3 SHA-1 method 191
Annex M – Alphabetical list of information item definitions 192
Annex N – Amendments and corrigenda 195