ISO/IEC 9594-8:2008-12 (E)

Information technology_- Open Systems Interconnection_- The Directory: Public-key and attribute certificate frameworks

CONTENTS

Page

Foreword vi
Introduction vii

SECTION 1 – GENERAL 1
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 Other references 3
3 Definitions 3
3.1 OSI Reference Model security architecture definitions 3
3.2 Directory model definitions 3
3.3 Access control framework definitions 4
3.4 Definitions 4
4 Abbreviations 7
5 Conventions 7
6 Frameworks overview 8
6.1 Digital signatures 9
SECTION 2 – PUBLIC-KEY CERTIFICATE FRAMEWORK 11
7 Public-keys and public-key certificates 11
7.1 Generation of key pairs 16
7.2 Public-key certificate creation 16
7.3 Certificate Validity 16
7.4 Repudiation of a digital signing 19
8 Public-key certificate and CRL extensions 19
8.1 Policy handling 20
8.2 Key and policy information extensions 23
8.3 Subject and issuer information extensions 29
8.4 Certification path constraint extensions 31
8.5 Basic CRL extensions 35
8.6 CRL distribution points and delta-CRL extensions 44
9 Delta CRL relationship to base 49
10 Certification path processing procedure 50
10.1 Path processing inputs 51
10.2 Path processing outputs 51
10.3 Path processing variables 52
10.4 Initialization step 52
10.5 Certificate processing 52
11 PKI directory schema 55
11.1 PKI directory object classes and name forms 55
11.2 PKI directory attributes 56
11.3 PKI directory matching rules 58
SECTION 3 – ATTRIBUTE CERTIFICATE FRAMEWORK 63
12 Attribute Certificates 64
12.1 Attribute certificate structure 64
12.2 Attribute certificate paths 66
13 Attribute Authority, SOA and Certification Authority relationship 66
13.1 Privilege in attribute certificates 68
13.2 Privilege in public-key certificates 68

Page

14 PMI models ... 68
14.1 General model ... 68
14.2 Control model ... 70
14.3 Delegation model ... 71
14.4 Group assignment model ... 72
14.5 Roles model ... 72
14.6 Recognition of Authority Model ... 74
14.7 XML privilege information attribute ... 77
14.8 Permission attribute and matching rule ... 78
15 Privilege management certificate extensions ... 78
15.1 Basic privilege management extensions ... 79
15.2 Privilege revocation extensions ... 82
15.3 Source of Authority extensions ... 82
15.4 Role extensions ... 85
15.5 Delegation extensions ... 86
15.6 Recognition of Authority Extensions ... 90
16 Privilege path processing procedure ... 92
16.1 Basic processing procedure ... 93
16.2 Role processing procedure ... 94
16.3 Delegation processing procedure ... 94
17 PMI directory schema ... 96
17.1 PMI directory object classes ... 96
17.2 PMI Directory attributes ... 98
17.3 PMI general directory matching rules ... 99
18 Directory authentication ... 101
18.1 Simple authentication procedure ... 101
18.2 Strong Authentication ... 103
19 Access control ... 109
20 Protection of Directory operations ... 110
Annex A – Public-Key and Attribute Certificate Frameworks ... 111
Annex B – CRL generation and processing rules ... 133
B.1 Introduction ... 133
B.2 Determine parameters for CRLs ... 134
B.3 Determine CRLs required ... 135
B.4 Obtain CRLs ... 136
B.5 Process CRLs ... 136
Annex C – Examples of delta CRL issuance ... 140
Annex D – Privilege policy and privilege attribute definition examples ... 142
D.1 Introduction ... 142
D.2 Sample syntaxes ... 142
D.3 Privilege attribute example ... 146
Annex E – An introduction to public key cryptography ... 147
Annex F – Reference definition of algorithm object identifiers ... 149
Annex G – Examples of use of certification path constraints ... 150
G.1 Example 1: Use of basic constraints ... 150
G.2 Example 2: Use of policy mapping and policy constraints ... 150
G.3 Use of Name Constraints Extension ... 150
Annex H – Guidance on determining for which policies a certification path is valid ... 159
H.1 Certification path valid for a user-specified policy required ... 159
H.2 Certification path valid for any policy required ... 160
H.3 Certification path valid regardless of policy ... 160
H.4 Certification path valid for a user-specific policy desired, but not required ... 160

Page

Annex I – Key usage certificate extension issues 161
Annex J – External ASN.1 modules 162
Annex K – Use of Protected Passwords for Bind operations 169
Annex L – Alphabetical list of information item definitions 170
Annex M – Amendments and corrigenda 173