

# ISO/IEC 9594-8:2005-12 (E)

## Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

---

### Contents

Page

Reference number INTERNATIONAL STANDARD 9594-8 Fifth edition 2005-12-15 Information technology -- Open Systems Interconnection -- The Directory: Public- key and attribute certificate frameworks Technologies de l'information -- Interconnexion de systèmes ouverts (OSI) -- L'annuaire: Cadre général des certificats de clé publique et d'attribut

PDF disclaimer This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area. Adobe is a trademark of Adobe Systems Incorporated. Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below. electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester. ISO copyright office Case postale 56 · CH-1211 Geneva 20 Tel. + 41 22 749 01 11 Fax + 41 22 749 09 47 E-mail copyright@iso.org Web www.iso.org Published by ISO in 2006 Published in Switzerland CONTENTS 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

3 Definitions ..... 3

3.1 OSI Reference Model security architecture definitions ..... 3

3.2 Directory model definitions ..... 3

3.3 Definitions ..... 4

4 Abbreviations ..... 6

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 ..... 15

7.2 Public-key certificate creation ..... 15

7.3 Certificate Validity ..... 16

7.4 Repudiation of a digital signing ..... 18

8 Public-key certificate and CRL extensions ..... 19

8.1 Policy handling ..... 19

8.1.1 Certificate policy ..... 19

8.1.2 Cross-certification ..... 20

8.1.3	Policy mapping .....	21
8.1.4	Certification path processing .....	21
8.1.5	Self-issued certificates .....	22
8.2	Key and policy information extensions .....	22
8.2.1	Requirements .....	22
8.2.2	Public-key certificate and CRL extension fields .....	23
8.3	Subject and issuer information extensions .....	28
8.3.1	Requirements .....	28
8.3.2	Certificate and CRL extension fields .....	28
8.4	Certification path constraint extensions .....	30
8.4.1	Requirements .....	30
8.4.2	Certificate extension fields .....	30
8.5	Basic CRL extensions .....	34
8.5.1	Requirements .....	34
8.5.2	CRL and CRL entry extension fields .....	35
8.6	CRL distribution points and delta-CRL extensions .....	43
8.6.1	Requirements .....	43
8.6.2	CRL distribution point and delta-CRL extension fields .....	44
9	Delta CRL relationship to base .....	49
10	Certification path processing procedure .....	50
10.1	Path processing inputs .....	50
10.2	Path processing outputs .....	51
10.3	Path processing variables .....	51
10.4	Initialization step .....	51
10.5	Certificate processing .....	52
10.5.1	Basic certificate checks .....	52
10.5.2	Processing intermediate certificates .....	52
10.5.3	Explicit policy indicator processing .....	53
10.5.4	Final processing .....	54
11	PKI directory schema .....	54
11.1	PKI directory object classes and name forms .....	54
11.1.1	PKI user object class .....	54
11.1.2	PKI CA object class .....	54
11.1.3	CRL distribution points object class and name form .....	54
11.1.4	Delta CRL object class .....	55
11.1.5	Certificate Policy & CPS object class .....	55
11.1.6	PKI certificate path object class .....	55
11.2	PKI directory attributes .....	55
11.2.1	User certificate attribute .....	55
11.2.2	CA certificate attribute .....	55
11.2.3	Cross-certificate pair attribute .....	56
11.2.4	Certificate revocation list attribute .....	56
11.2.5	Authority revocation list attribute .....	56
11.2.6	Delta revocation list attribute .....	56
11.2.7	Supported algorithms attribute .....	56
11.2.8	Certification practice statement attribute .....	57
11.2.9	Certificate policy attribute .....	57
11.2.10	PKI path attribute .....	57
11.3	PKI directory matching rules .....	58
11.3.1	Certificate exact match .....	58
11.3.2	Certificate match .....	58
11.3.3	Certificate pair exact match .....	59
11.3.4	Certificate pair match .....	59
11.3.5	Certificate list exact match .....	60
11.3.6	Certificate list match .....	60
11.3.7	Algorithm identifier match .....	61
11.3.8	Policy match .....	61
11.3.9	PKI path match .....	61
11.3.10	Enhanced certificate match .....	61

<b>SECTION 3 - ATTRIBUTE CERTIFICATE FRAMEWORK .....</b>	<b>62</b>	
<b>12</b>	<b>Attribute Certificates .....</b>	<b>63</b>
12.1	Attribute certificate structure .....	63
12.2	Attribute certificate paths .....	65
<b>13</b>	<b>Attribute Authority, SOA and Certification Authority relationship .....</b>	<b>65</b>
13.1	Privilege in attribute certificates .....	66
13.2	Privilege in public-key certificates .....	67
<b>14</b>	<b>PMI models .....</b>	<b>67</b>
14.1	General model .....	67
14.1.1	PMI in access control context .....	68
14.1.2	PMI in a non-repudiation context .....	69
14.2	Control model .....	69
14.3	Delegation model .....	69
14.4	Roles model .....	70
14.4.1	Role attribute .....	71
14.5	XML privilege information attribute .....	71
<b>15</b>	<b>Privilege management certificate extensions .....</b>	<b>73</b>
15.1	Basic privilege management extensions .....	73
15.1.1	Requirements .....	73
15.1.2	Basic privilege management extension fields .....	73
15.2	Privilege revocation extensions .....	76
15.2.1	Requirements .....	76
15.2.2	Privilege revocation extension fields .....	76
15.3	Source of Authority extensions .....	76
15.3.1	Requirements .....	76
15.3.2	SOA extension fields .....	77
15.4	Role extensions .....	78
15.4.1	Requirements .....	78
15.4.2	Role extension fields .....	78
15.5	Delegation extensions .....	80
15.5.1	Requirements .....	80
15.5.2	Delegation extension fields .....	80
<b>16</b>	<b>Privilege path processing procedure .....</b>	<b>84</b>
16.1	Basic processing procedure .....	84
16.2	Role processing procedure .....	85
16.3	Delegation processing procedure .....	85
16.3.1	Verify integrity of domination rule .....	85
16.3.2	Establish valid delegation path .....	86
16.3.3	Verify privilege delegation .....	86
16.3.4	Pass/fail determination .....	86
<b>17</b>	<b>PMI directory schema .....</b>	<b>86</b>
17.1	PMI directory object classes .....	86
17.1.1	PMI user object class .....	86
17.1.2	PMI AA object class .....	87
17.1.3	PMI SOA object class .....	87
17.1.4	Attribute certificate CRL distribution point object class .....	87
17.1.5	PMI delegation path .....	87
17.1.6	Privilege policy object class .....	87
17.1.7	Protected privilege policy object class .....	87
17.2	PMI Directory attributes .....	88
17.2.1	Attribute certificate attribute .....	88
17.2.2	AA certificate attribute .....	88
17.2.3	Attribute descriptor certificate attribute .....	88
17.2.4	Attribute certificate revocation list attribute .....	88
17.2.5	AA certificate revocation list attribute .....	88

17.2.6	Delegation path attribute .....	88
17.2.7	Privilege policy attribute .....	89
17.2.8	Protected privilege policy attribute .....	89
17.2.9	XML Protected privilege policy attribute .....	89
17.3	PMI general directory matching rules .....	89
17.3.1	Attribute certificate exact match .....	89
17.3.2	Attribute certificate match .....	89
17.3.3	Holder issuer match .....	90
17.3.4	Delegation path match .....	90
<b>SECTION 4 - DIRECTORY USE OF PUBLIC-KEY &amp; ATTRIBUTE CERTIFICATE FRAMEWORKS .....</b>		<b>90</b>
18	Directory authentication .....	90
18.1	Simple authentication procedure .....	91
18.1.1	Generation of protected identifying information .....	91
18.1.2	Procedure for protected simple authentication .....	92
18.1.3	User Password attribute type .....	93
18.2	Strong Authentication .....	93
18.2.1	Obtaining public-key certificates from the directory .....	93
18.2.2	Strong authentication procedures .....	96
19	Access control .....	99
20	Protection of Directory operations .....	99
<b>Annex A - Public-Key and Attribute Certificate Frameworks .....</b>		<b>100</b>
-- A.1	Authentication framework module .....	100
-- A.2	Certificate extensions module .....	105
-- A.3	Attribute Certificate Framework module .....	114
<b>Annex B - CRL generation and processing rules .....</b>		<b>122</b>
B.1	Introduction .....	122
B.1.1	CRL types .....	122
B.1.2	CRL processing .....	123
B.2	Determine parameters for CRLs .....	123
B.3	Determine CRLs required .....	124
B.3.1	End-entity with critical CRL DP .....	124
B.3.2	End-entity with no critical CRL DP .....	124
B.3.3	CA with critical CRL DP .....	124
B.3.4	CA with no critical CRL DP .....	125
B.4	Obtain CRLs .....	125
B.5	Process CRLs .....	125
B.5.1	Validate base CRL scope .....	125
B.5.2	Validate delta CRL scope .....	127
B.5.3	Validity and currency checks on the base CRL .....	128
B.5.4	Validity and checks on the delta CRL .....	128
<b>Annex C - Examples of delta CRL issuance .....</b>		<b>129</b>
<b>Annex D - Privilege policy and privilege attribute definition examples .....</b>		<b>131</b>
D.1	Introduction .....	131
D.2	Sample syntaxes .....	131
D.2.1	First example .....	131
D.2.2	Second example .....	133
D.3	Privilege attribute example .....	134
<b>Annex E - An introduction to public key cryptography .....</b>		<b>136</b>

<b>Annex F - Reference definition of algorithm object identifiers .....</b>	<b>138</b>
<b>Annex G - Examples of use of certification path constraints .....</b>	<b>139</b>
<b>G.1 Example 1: Use of basic constraints .....</b>	<b>139</b>
<b>G.2 Example 2: Use of policy mapping and policy constraints .....</b>	<b>139</b>
<b>G.3 Use of Name Constraints Extension .....</b>	<b>139</b>
<b>G.3.1 Examples of Certificate Format with Name Constraints Extension .....</b>	<b>139</b>
<b>G.3.2 Examples of Certificate Handling with Name Constraint Extension .....</b>	<b>143</b>
<b>Annex H - Guidance on determining for which policies a certification path is valid .....</b>	<b>156</b>
<b>H.1 Certification path valid for a user-specified policy required .....</b>	<b>156</b>
<b>H.2 Certification path valid for any policy required .....</b>	<b>157</b>
<b>H.3 Certification path valid regardless of policy .....</b>	<b>157</b>
<b>H.4 Certification path valid for a user-specific policy desired, but not required .....</b>	<b>157</b>
<b>Annex I - Key usage certificate extension issues .....</b>	<b>158</b>
<b>Annex J - Alphabetical list of information item definitions .....</b>	<b>159</b>
<b>Annex K - Amendments and corrigenda .....</b>	<b>162</b>