

ISO/IEC 9594-2:2005-12 (E)

Information technology - Open Systems Interconnection - The Directory: Models

Contents

Page

Reference number INTERNATIONAL STANDARD 9594-2 Fifth edition 2005-12-15 Information technology -- Open Systems Interconnection -- The Directory: Models Technologies de l'information -- Interconnexion de systèmes ouverts (OSI) -- L'annuaire: Les modèles

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

2.3 Other references 3

3 Definitions 3

3.1 Communication Definitions 3

3.2 Basic directory definitions 3

3.3 Distributed operation definitions 3

3.4 Replication definitions 3

4 Abbreviations 4

5 Conventions 5

SECTION 2 - OVERVIEW OF THE DIRECTORY MODELS 6

6 Directory Models 6

6.1 Definitions 6

6.2 The Directory and its users 6

6.3 Directory and DSA Information Models 7

6.4 Directory Administrative Authority Model 8

SECTION 3 - MODEL OF DIRECTORY USER INFORMATION 10

7 Directory Information Base 10

7.1 Definitions 10

7.2 Objects 11

7.3 Directory entries 11

7.4 The Directory Information Tree (DIT) 11

8	Directory entries	12
8.1	Definitions	12
8.2	Overall structure	14
8.3	Object classes	15
8.4	Attribute Types	16
8.5	Attribute Values	17
8.6	Attribute Type Hierarchies	17
8.7	Friend attributes	18
8.8	Contexts	18
8.9	Matching rules	19
8.10	Entry collections	22
8.11	Compound entries and families of entries	23
9	Names	24
9.1	Definitions	24
9.2	Names in general	24
9.3	Relative Distinguished Names	25
9.4	Name matching	26
9.5	Names returned during operations	27
9.6	Names held as attribute values or used as parameters	27
9.7	Distinguished Names	27
9.8	Alias Names	28
10	Hierarchical groups	29
10.1	Definitions	29
10.2	Hierarchical relationship	29
10.3	Sequential ordering of a hierarchical group	30
SECTION 4 - DIRECTORY ADMINISTRATIVE MODEL		31
11	Directory Administrative Authority model	31
11.1	Definitions	31
11.2	Overview	31
11.3	Policy	32
11.4	Specific administrative authorities	32
11.5	Administrative areas and administrative points	33
11.6	DIT Domain policies	35
11.7	DMD policies	35
SECTION 5 - MODEL OF DIRECTORY ADMINISTRATIVE AND OPERATIONAL INFORMATION		37
12	Model of Directory Administrative and Operational Information	37
12.1	Definitions	37
12.2	Overview	37
12.3	Subtrees	38
12.4	Operational attributes	41
12.5	Entries	41
12.6	Subentries	41
12.7	Information model for collective attributes	43
12.8	Information model for context defaults	43
SECTION 6 - THE DIRECTORY SCHEMA		45
13	Directory Schema	45
13.1	Definitions	45
13.2	Overview	45
13.3	Object class definition	47
13.4	Attribute type definition	49
13.5	Matching rule definition	52
13.6	Relaxations and tightenings	54
13.7	DIT structure definition	60

13.8	DIT content rule definition	62
13.9	Context type definition	64
13.10	DIT Context Use definition	65
13.11	Friends definition	66
14	Directory System Schema	66
14.1	Overview	66
14.2	System schema supporting the administrative and operational information model	67
14.3	System schema supporting the administrative model	67
14.4	System schema supporting general administrative and operational requirements	68
14.5	System schema supporting access control	70
14.6	System schema supporting the collective attribute model	70
14.7	System schema supporting context assertion defaults	71
14.8	System schema supporting the service administration model	71
14.9	System schema supporting hierarchical groups	72
14.10	Maintenance of system schema	73
14.11	System schema for first-level subordinates	73
15	Directory schema administration	73
15.1	Overview	73
15.2	Policy objects	73
15.3	Policy parameters	74
15.4	Policy procedures	74
15.5	Subschema modification procedures	74
15.6	Entry addition and modification procedures	75
15.7	Subschema policy attributes	75
SECTION 7 - DIRECTORY SERVICE ADMINISTRATION		81
16	Service Administration Model	81
16.1	Definitions	81
16.2	Service-type/user-class model	81
16.3	Service-specific administrative areas	82
16.4	Introduction to search-rules	83
16.5	Subfilters	83
16.6	Filter requirements	84
16.7	Attribute information selection based on search-rules	84
16.8	Access control aspects of search-rules	85
16.9	Contexts aspects of search-rules	85
16.10	Search-rule specification	85
16.11	Matching restriction definition	93
16.12	Search-validation function	93
SECTION 8 - SECURITY		95
17	Security model	95
17.1	Definitions	95
17.2	Security policies	95
17.3	Protection of Directory operations	96
18	Basic Access Control	97
18.1	Scope and application	97
18.2	Basic Access Control model	97
18.3	Access control administrative areas	100
18.4	Representation of Access Control Information	102
18.5	The ACI operational attributes	107
18.6	Protecting the ACI	108
18.7	Access control and Directory operations	108
18.8	Access Control Decision Function	108
18.9	Simplified Access Control	110
19	Rule-based Access Control	110

19.1	Scope and application	110
19.2	Rule-based Access Control model	110
19.3	Access control administrative areas	111
19.4	Security Label	111
19.5	Clearance	113
19.6	Access Control and Directory operations	113
19.7	Access Control Decision Function	114
19.8	Use of Rule-based and Basic Access Control	114
20	Data Integrity in Storage	114
20.1	Introduction	114
20.2	Protection of an Entry or Selected Attribute Types	114
20.3	Context for Protection of a Single Attribute Value	116
SECTION 9 - DSA MODELS		117
21	DSA Models	117
21.1	Definitions	117
21.2	Directory Functional Model	117
21.3	Directory Distribution Model	118
SECTION 10 - DSA INFORMATION MODEL		120
22	Knowledge	120
22.1	Definitions	120
22.2	Introduction	120
22.3	Knowledge References	121
22.4	Minimum Knowledge	123
22.5	First Level DSAs	124
23	Basic Elements of the DSA Information Model	124
23.1	Definitions	124
23.2	Introduction	125
23.3	DSA-Specific Entries and their Names	125
23.4	Basic Elements	127
24	Representation of DSA Information	128
24.1	Representation of Directory User and Operational Information	128
24.2	Representation of Knowledge References	129
24.3	Representation of Names and Naming Contexts	136
SECTION 11 - DSA OPERATIONAL FRAMEWORK		138
25	Overview	138
25.1	Definitions	138
25.2	Introduction	138
26	Operational bindings	138
26.1	General	138
26.2	Application of the operational framework	139
26.3	States of cooperation	140
27	Operational binding specification and management	141
27.1	Operational binding type specification	141
27.2	Operational binding management	142
27.3	Operational binding specification templates	143
28	Operations for operational binding management	145
28.1	Application-context definition	145
28.2	Establish Operational Binding operation	145
28.3	Modify Operational Binding operation	147
28.4	Terminate Operational Binding operation	148

28.5	Operational Binding Error	149
28.6	Operational Binding Management Bind and Unbind	150
Annex A - Object identifier usage		152
Annex B - Information Framework in ASN.1		155
Annex C - SubSchema Administration Schema in ASN.1		165
Annex D - Service Administration in ASN.1		169
Annex E - Basic Access Control in ASN.1		173
Annex F - DSA Operational Attribute Types in ASN.1		177
Annex G - Operational Binding Management in ASN.1		180
Annex H - Enhanced security		184
Annex I - The Mathematics of Trees		187
Annex J - Name Design Criteria		188
Annex K - Examples of various aspects of schema		190
K.1	Example of an attribute hierarchy	190
K.2	Example of a subtree specification	190
K.3	Schema specification	191
K.4	DIT content rules	192
K.5	DIT context use	193
Annex L - Overview of basic access control permissions		194
L.1	Introduction	194
L.2	Permissions required for operations	194
L.3	Permissions affecting error	195
L.4	Entry level permissions	195
L.5	Entry level permissions	196
Annex M - Examples of access control		198
M.1	Introduction	198
M.2	Design principles for Basic Access Control	198
M.3	Introduction to example	198
M.4	Policy affecting the definition of specific and inner areas	199
M.5	Policy affecting the definition of DACDs	201
M.6	Policy expressed in prescriptiveACI attributes	204
M.7	Policy expressed in subentryACI attributes	209
M.8	Policy expressed in entryACI attributes	210
M.9	ACDF examples	211
M.10	Rule-based Access Control	213
Annex N - DSE type combinations		214
Annex O - Modelling of knowledge		216
Annex P - Names held as attribute values or used as parameters		221
Annex Q - Subfilters		222
Annex R - Compound entry name patterns and their use		223

Annex S - Naming concepts and considerations	225
S.1 History tells us	225
S.2 A new look at name resolution	225
Annex T - Alphabetical index of definitions	232
Annex U - Amendments and corrigenda	234