

# ISO/IEC 9594-2:2014-03 (E)

## Information technology - Open Systems Interconnection - The Directory - Part 2: Models

---

<b>Contents</b>		<b>Page</b>
1	Scope .....	1
2	Normative references .....	2
2.1	Identical Recommendations   International Standards .....	2
2.2	Paired Recommendations   International Standards equivalent in technical content.....	2
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
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.....	7
7	Directory Information Base .....	9
7.1	Definitions.....	9
7.2	Objects .....	10
7.3	Directory entries.....	10
7.4	Directory Information Tree (DIT).....	10
8	Directory entries .....	11
8.1	Definitions.....	11
8.2	Overall structure.....	13
8.3	Object classes .....	14
8.4	Attribute types.....	16
8.5	Attribute values .....	16
8.6	Attribute type hierarchies.....	16
8.7	Friend attributes .....	17
8.8	Contexts .....	17
8.9	Matching rules.....	18
8.10	Entry collections.....	21
8.11	Compound entries and families of entries .....	22
9	Names.....	23
9.1	Definitions.....	23
9.2	Names in general.....	23
9.3	Relative distinguished name.....	23
9.4	Name matching .....	24
9.5	Distinguished names .....	24
9.6	Alias names .....	25
10	Hierarchical groups .....	25
10.1	Definitions.....	25
10.2	Hierarchical relationship .....	26
10.3	Sequential ordering of a hierarchical group .....	27

11	Directory Administrative Authority model .....	28
	11.1 Definitions.....	28
	11.2 Overview.....	28
	11.3 Policy .....	29
	11.4 Specific administrative authorities .....	29
	11.5 Administrative areas and administrative points .....	30
	11.6 DIT Domain policies.....	32
	11.7 DMD policies.....	32
12	Model of Directory Administrative and Operational Information.....	34
	12.1 Definitions.....	34
	12.2 Overview .....	34
	12.3 Subtrees.....	35
	12.4 Operational attributes .....	37
	12.5 Entries .....	38
	12.6 Subentries.....	38
	12.7 Information model for collective attributes.....	39
	12.8 Information model for context defaults.....	40
13	Directory Schema .....	41
	13.1 Definitions.....	41
	13.2 Overview .....	41
	13.3 Object class definition.....	43
	13.4 Attribute type definition.....	45
	13.5 Matching rule definition.....	48
	13.6 Relaxation and tightening.....	50
	13.7 DIT structure definition.....	56
	13.8 DIT content rule definition.....	59
	13.9 Context type definition.....	60
	13.10 DIT Context Use definition.....	62
	13.11 Friends definition .....	62
	13.12 Syntax definitions.....	63
14	Directory System Schema .....	63
	14.1 Overview .....	63
	14.2 System schema supporting the administrative and operational information model .....	64
	14.3 System schema supporting the administrative model.....	64
	14.4 System schema supporting general administrative and operational requirements .....	65
	14.5 System schema supporting access control.....	67
	14.6 System schema supporting the collective attribute model.....	67
	14.7 System schema supporting context assertion defaults.....	68
	14.8 System schema supporting the service administration model .....	68
	14.9 System schema supporting password administration .....	69
	14.10 System schema supporting hierarchical groups .....	70
	14.11 Maintenance of system schema.....	70
	14.12 System schema for first-level subordinates.....	71
15	Directory schema administration.....	71
	15.1 Overview.....	71
	15.2 Policy objects .....	71
	15.3 Policy parameters .....	72
	15.4 Policy procedures .....	72
	15.5 Subschema modification procedures.....	72
	15.6 Entry addition and modification procedures .....	73
	15.7 Subschema policy attributes.....	73

16	Service Administration Model .....	80
	16.1 Definitions.....	80
	16.2 Service-type/user-class model.....	80
	16.3 Service-specific administrative areas .....	81
	16.4 Introduction to search-rules.....	82
	16.5 Subfilters .....	82
	16.6 Filter requirements .....	83
	16.7 Attribute information selection based on search-rules .....	83
	16.8 Access control aspects of search-rules .....	84
	16.9 Contexts aspects of search-rules .....	84
	16.10 Search-rule specification.....	84
	16.11 Matching restriction definition.....	92
	16.12 Search-validation function .....	92
17	Security model.....	94
	17.1 Definitions.....	94
	17.2 Security policies .....	94
	17.3 Protection of Directory operations .....	95
18	Basic Access Control.....	96
	18.1 Scope and application .....	96
	18.2 Basic Access Control model .....	96
	18.3 Access control administrative areas .....	98
	18.4 Representation of Access Control Information .....	101
	18.5 ACI operational attributes .....	106
	18.6 Protecting the ACI.....	107
	18.7 Access control and Directory operations.....	107
	18.8 Access Control Decision Function .....	107
	18.9 Simplified Access Control .....	109
19	Rule-based Access Control.....	109
	19.1 Scope and application .....	109
	19.2 Rule-based Access Control model .....	110
	19.3 Access control administrative areas .....	110
	19.4 Security Label .....	110
	19.5 Clearance.....	112
	19.6 Access Control and Directory operations.....	112
	19.7 Access Control Decision Function .....	113
	19.8 Use of Rule-based and Basic Access Control .....	113
20	Data Integrity in Storage .....	113
	20.1 Introduction.....	113
	20.2 Protection of an Entry or Selected Attribute Types.....	113
	20.3 Context for Protection of a Single Attribute Value .....	115
21	DSA Models.....	116
	21.1 Definitions.....	116
	21.2 Directory Functional Model .....	116
	21.3 Directory Distribution Model.....	117
22	Knowledge .....	119
	22.1 Definitions.....	119
	22.2 Introduction.....	119
	22.3 Knowledge References.....	120
	22.4 Minimum Knowledge .....	122
	22.5 First Level DSAs.....	122
	22.6 Knowledge references to LDAP servers .....	123
23	Basic Elements of the DSA Information Model.....	123
	23.1 Definitions.....	123
	23.2 Introduction.....	123
	23.3 DSA Specific Entries and their Names .....	124
	23.4 Basic Elements.....	125

24	Representation of DSA Information.....	127
	24.1 Representation of Directory User and Operational Information .....	127
	24.2 Representation of Knowledge References.....	127
	24.3 Representation of Names and Naming Contexts.....	134
25	Overview .....	136
	25.1 Definitions.....	136
	25.2 Introduction.....	136
26	Operational bindings .....	136
	26.1 General.....	136
	26.2 Application of the operational framework .....	137
	26.3 States of cooperation .....	138
27	Operational binding specification and management.....	139
	27.1 Operational binding type specification.....	139
	27.2 Operational binding management .....	140
	27.3 Operational binding specification templates .....	140
28	Operations for operational binding management .....	142
	28.1 Application-context definition .....	142
	28.2 Establish Operational Binding operation .....	143
	28.3 Modify Operational Binding operation .....	146
	28.4 Terminate Operational Binding operation.....	148
	28.5 Operational Binding Error.....	149
	28.6 Operational Binding Management Bind and Unbind.....	151
29	Overview .....	152
	29.1 Definitions.....	152
	29.2 Introduction.....	152
30	LDAP interworking model .....	153
	30.1 LDAP interworking scenarios.....	153
	30.2 Overview of bound DSA handling LDAP operations .....	153
	30.3 General LDAP requestor characteristics .....	154
	30.4 LDAP extension mechanisms .....	154
31	LDAP specific system schema .....	154
	31.1 Operational Attribute types from IETF RFC 4512.....	154

Annex A – Object identifier usage .....	157
Annex B – Information framework in ASN.1 .....	161
Annex C – Subschema administration in ASN.1 .....	172
Annex D – Service administration in ASN.1 .....	177
Annex E – Basic Access Control in ASN.1 .....	181
Annex F – DSA operational attribute types in ASN.1 .....	184
Annex G – Operational binding management in ASN.1 .....	187
Annex H – Enhanced security in ASN.1 .....	192
Annex I – LDAP system schema .....	195
Annex J – The mathematics of trees .....	197
Annex K – Name design criteria .....	198
Annex L – Examples of various aspects of schema .....	200
L.1 Example of an attribute hierarchy .....	200
L.2 Example of a subtree specification .....	200
L.3 Schema specification .....	201
L.4 DIT content rules .....	202
L.5 DIT context use .....	203
Annex M – Overview of basic access control permissions .....	204
M.1 Introduction .....	204
M.2 Permissions required for operations .....	204
M.3 Permissions affecting error .....	205
M.4 Entry level permissions .....	205
M.5 Entry level permissions .....	206
Annex N – Examples of access control .....	207
N.1 Introduction .....	207
N.2 Design principles for Basic Access Control .....	207
N.3 Introduction to example .....	208
N.4 Policy affecting the definition of specific and inner areas .....	208
N.5 Policy affecting the definition of Directory Access Control Domains (DACDs) .....	210
N.6 Policy expressed in prescriptiveACI attributes .....	213
N.7 Policy expressed in subentryACI attributes .....	217
N.8 Policy expressed in entryACI attributes .....	218
N.9 ACDF examples .....	219
N.10 Rule-based access control .....	221
Annex O – DSE type combinations .....	222
Annex P – Modelling of knowledge .....	224
Annex Q – Subfilters .....	228
Annex R – Compound entry name patterns and their use .....	229
Annex S – Naming concepts and considerations .....	231
S.1 History tells us .....	231
S.2 A new look at name resolution .....	231
Annex T – Alphabetical index of definitions .....	237
Annex U – Amendments and corrigenda .....	240