

# ISO/IEC 9594-2:2017-05 (E)

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

### CONTENTS

	<i>Page</i>
SECTION 1 – GENERAL.....	1
1 Scope.....	1
2 References.....	2
2.1 Normative references.....	2
2.2 Non-normative reference.....	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.....	4
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.....	9
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.....	22
8.11 Compound entries and families of entries.....	22
9 Names.....	23
9.1 Definitions.....	23
9.2 Names in general.....	24
9.3 Relative distinguished name.....	24
9.4 Name matching.....	25
9.5 Distinguished names.....	25
9.6 Alias names.....	26
10 Hierarchical groups.....	26
10.1 Definitions.....	26
10.2 Hierarchical relationship.....	27
10.3 Sequential ordering of a hierarchical group.....	28

	<i>Page</i>
SECTION 4 – DIRECTORY ADMINISTRATIVE MODEL.....	29
11 Directory Administrative Authority model .....	29
11.1 Definitions.....	29
11.2 Overview.....	29
11.3 Policy .....	30
11.4 Specific administrative authorities .....	30
11.5 Administrative areas and administrative points .....	31
11.6 DIT Domain policies.....	33
11.7 DMD policies.....	33
SECTION 5 – MODEL OF DIRECTORY ADMINISTRATIVE AND OPERATIONAL INFORMATION .....	35
12 Model of Directory Administrative and Operational Information.....	35
12.1 Definitions.....	35
12.2 Overview.....	35
12.3 Subtrees .....	36
12.4 Operational attributes .....	38
12.5 Entries .....	39
12.6 Subentries.....	39
12.7 Information model for collective attributes.....	40
12.8 Information model for context defaults.....	41
SECTION 6 – THE DIRECTORY SCHEMA .....	42
13 Directory Schema .....	42
13.1 Definitions.....	42
13.2 Overview.....	42
13.3 Object class definition.....	44
13.4 Attribute type definition .....	46
13.5 Matching rule definition.....	50
13.6 Relaxation and tightening.....	52
13.7 DIT structure definition.....	58
13.8 DIT content rule definition.....	61
13.9 Context type definition.....	62
13.10 DIT Context Use definition.....	63
13.11 Friends definition .....	64
13.12 Syntax definitions.....	65
14 Directory System Schema .....	65
14.1 Overview.....	65
14.2 System schema supporting the administrative and operational information model .....	66
14.3 System schema supporting the administrative model.....	66
14.4 System schema supporting general administrative and operational requirements .....	67
14.5 System schema supporting access control.....	69
14.6 System schema supporting the collective attribute model.....	70
14.7 System schema supporting context assertion defaults.....	70
14.8 System schema supporting the service administration model .....	70
14.9 System schema supporting password administration .....	71
14.10 System schema supporting hierarchical groups.....	72
14.11 Maintenance of system schema.....	73
14.12 System schema for first-level subordinates.....	73
15 Directory schema administration.....	73
15.1 Overview.....	73
15.2 Policy objects .....	74
15.3 Policy parameters .....	74
15.4 Policy procedures .....	75
15.5 Subschema modification procedures.....	75
15.6 Entry addition and modification procedures .....	75
15.7 Subschema policy attributes.....	76

	<i>Page</i>
SECTION 7 – DIRECTORY SERVICE ADMINISTRATION.....	82
16 Service Administration Model.....	82
16.1 Definitions.....	82
16.2 Service-type/user-class model.....	82
16.3 Service-specific administrative areas .....	83
16.4 Introduction to search-rules.....	84
16.5 Subfilters .....	84
16.6 Filter requirements .....	85
16.7 Attribute information selection based on search-rules .....	85
16.8 Access control aspects of search-rules .....	86
16.9 Contexts aspects of search-rules.....	86
16.10 Search-rule specification .....	86
16.11 Matching restriction definition.....	94
16.12 Search-validation function .....	95
SECTION 8 – SECURITY .....	96
17 Security model.....	96
17.1 Definitions.....	96
17.2 Security policies .....	96
17.3 Protection of Directory operations .....	97
18 Basic Access Control.....	98
18.1 Scope and application.....	98
18.2 Basic Access Control model .....	98
18.3 Access control administrative areas .....	101
18.4 Representation of Access Control Information .....	103
18.5 ACI operational attributes .....	108
18.6 Protecting the ACI.....	109
18.7 Access control and Directory operations.....	109
18.8 Access Control Decision Function.....	110
18.9 Simplified Access Control .....	111
19 Rule-based Access Control.....	111
19.1 Scope and application.....	111
19.2 Rule-based Access Control model .....	112
19.3 Access control administrative areas .....	113
19.4 Security Label .....	113
19.5 Clearance.....	114
19.6 Access Control and Directory operations.....	115
19.7 Access Control Decision Function.....	115
19.8 Use of Rule-based and Basic Access Control .....	115
20 Data Integrity in Storage .....	116
20.1 Introduction .....	116
20.2 Protection of an Entry or Selected Attribute Types.....	116
20.3 Context for Protection of a Single Attribute Value .....	117
SECTION 9 – DSA MODELS .....	119
21 DSA Models .....	119
21.1 Definitions.....	119
21.2 Directory Functional Model .....	119
21.3 Directory Distribution Model.....	120
SECTION 10 – DSA INFORMATION MODEL.....	122
22 Knowledge.....	122
22.1 Definitions.....	122
22.2 Introduction .....	122
22.3 Knowledge References.....	123

	<i>Page</i>	
22.4	Minimum Knowledge .....	125
22.5	First Level DSAs.....	126
22.6	Knowledge references to LDAP servers .....	126
23	Basic Elements of the DSA Information Model.....	126
23.1	Definitions.....	126
23.2	Introduction .....	127
23.3	DSA Specific Entries and their Names .....	127
23.4	Basic Elements .....	129
24	Representation of DSA Information.....	130
24.1	Representation of Directory User and Operational Information .....	130
24.2	Representation of Knowledge References.....	131
24.3	Representation of Names and Naming Contexts.....	138
SECTION 11 – DSA OPERATIONAL FRAMEWORK.....		140
25	Overview .....	140
25.1	Definitions.....	140
25.2	Introduction .....	140
26	Operational bindings .....	140
26.1	General .....	140
26.2	Application of the operational framework .....	141
26.3	States of cooperation .....	142
27	Operational binding specification and management.....	143
27.1	Operational binding type specification.....	143
27.2	Operational binding management .....	144
27.3	Operational binding specification templates .....	145
28	Operations for operational binding management.....	147
28.1	Application-context definition .....	147
28.2	Establish Operational Binding operation.....	147
28.3	Modify Operational Binding operation .....	150
28.4	Terminate Operational Binding operation.....	152
28.5	Operational Binding Error.....	153
28.6	Operational Binding Management Bind and Unbind.....	155
SECTION 12 – INTERWORKING WITH LDAP.....		156
29	Overview .....	156
29.1	Definitions.....	156
29.2	Introduction .....	156
30	LDAP interworking model .....	156
30.1	LDAP interworking scenarios.....	156
30.2	Overview of bound DSA handling LDAP operations .....	157
30.3	General LDAP requestor characteristics .....	157
30.4	LDAP extension mechanisms .....	158
31	LDAP specific system schema .....	158
31.1	Operational Attribute types from IETF RFC 4512.....	158
Annex A – Object identifier usage.....		161
Annex B – Information framework in ASN.1.....		165
Annex C – Subschema administration in ASN.1 .....		177
Annex D – Service administration in ASN.1 .....		182
Annex E – Basic Access Control in ASN.1 .....		186
Annex F – DSA operational attribute types in ASN.1 .....		190
Annex G – Operational binding management in ASN.1 .....		193
Annex H – Enhanced security in ASN.1 .....		198

Annex I – LDAP system schema .....	201
Annex J – The mathematics of trees .....	203
Annex K – Name design criteria .....	204
Annex L – Examples of various aspects of schema .....	206
L.1 Example of an attribute hierarchy .....	206
L.2 Example of a subtree specification .....	206
L.3 Schema specification .....	207
L.4 DIT content rules .....	208
L.5 DIT context use .....	209
Annex M – Overview of basic access control permissions .....	210
M.1 Introduction .....	210
M.2 Permissions required for operations .....	210
M.3 Permissions affecting error .....	211
M.4 Entry level permissions .....	211
M.5 Entry level permissions .....	212
Annex N – Examples of access control .....	213
N.1 Introduction .....	213
N.2 Design principles for Basic Access Control .....	213
N.3 Introduction to example .....	214
N.4 Policy affecting the definition of specific and inner areas .....	215
N.5 Policy affecting the definition of Directory Access Control Domains (DACDs) .....	216
N.6 Policy expressed in prescriptiveACI attributes .....	219
N.7 Policy expressed in subentryACI attributes .....	224
N.8 Policy expressed in entryACI attributes .....	225
N.9 ACDF examples .....	225
N.10 Rule-based access control .....	227
Annex O – DSE type combinations .....	228
Annex P – Modelling of knowledge .....	230
Annex Q – Subfilters .....	235
Annex R – Compound entry name patterns and their use .....	236
Annex S – Naming concepts and considerations .....	238
S.1 History tells us .....	238
S.2 A new look at name resolution .....	238
Annex T – Alphabetical index of definitions .....	244
Annex U – Amendments and corrigenda .....	247