ISO/IEC 9594-2:2020-11 (E)

Information technology - Open systems interconnection - Part 2: The Directory: Models

Contents

		Page
SECTION 1 – GENERAL		1
1	Scope	1
2	References	2
	2.1 Normative references	2
	2.2 Non-normative 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	7
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	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 26
SECTION 4 – DIRECTORY ADMINISTRATIVE MODEL 28
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
SECTION 5 – MODEL OF DIRECTORY ADMINISTRATIVE AND OPERATIONAL INFORMATION 34
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 37
12.6 Subentries 38
12.7 Information model for collective attributes 39
12.8 Information model for context defaults 40
SECTION 6 – THE DIRECTORY SCHEMA 41
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 61
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 63
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 67
14.8 System schema supporting the service administration model 68
14.9 System schema supporting password administration 68
14.10 System schema supporting hierarchical groups 69
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 71
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
SECTION 7 – DIRECTORY SERVICE ADMINISTRATION 79
16 Service Administration Model 79

16.1 Definitions 79
16.2 Service-type/user-class model 79
16.3 Service-specific administrative areas 80
16.4 Introduction to search-rules 81
16.5 Subfilters 81
16.6 Filter requirements 82
16.7 Attribute information selection based on search-rules 82
16.8 Access control aspects of search-rules 83
16.9 Contexts aspects of search-rules 83
16.10 Search-rule specification 83
16.11 Matching restriction definition 91
16.12 Search-validation function 91
SECTION 8 – SECURITY 93
17 Security model 93
17.1 Definitions 93
17.2 Security policies 93
17.3 Protection of Directory operations 94
18 Basic Access Control 95
18.1 Scope and application 95
18.2 Basic Access Control model 95
18.3 Access control administrative areas 98
18.4 Representation of Access Control Information 100
18.5 ACI operational attributes 105
18.6 Protecting the ACI 106
18.7 Access control and Directory operations 106
18.8 Access Control Decision Function 106
18.9 Simplified Access Control 108
19 Rule-based Access Control 108
19.1 Scope and application 108
19.2 Rule-based Access Control model 108
19.3 Access control administrative areas 109
19.4 Security Label 109
19.5 Clearance 110
19.6 Access Control and Directory operations 111
19.7 Access Control Decision Function 111
19.8 Use of Rule-based and Basic Access Control 112
20 Data Integrity in Storage 112
20.1 Introduction 112
20.2 Protection of an Entry or Selected Attribute Types 112
20.3 Context for Protection of a Single Attribute Value 114
SECTION 9 – DSA MODELS 115
21 DSA Models 115
21.1 Definitions 115
21.2 Directory Functional Model 115
21.3 Directory Distribution Model 116
SECTION 10 – DSA INFORMATION MODEL 118
22 Knowledge 118
22.1 Definitions 118
22.2 Introduction 118
22.3 Knowledge References 119
22.4 Minimum Knowledge 121
22.5 First Level DSAs 121
22.6 Knowledge references to LDAP servers 122

23 Basic Elements of the DSA Information Model 122
23.1 Definitions 122
23.2 Introduction 122
23.3 DSA Specific Entries and their Names 123
23.4 Basic Elements 124
24 Representation of DSA Information 125
24.1 Representation of Directory User and Operational Information 126
24.2 Representation of Knowledge References 126
24.3 Representation of Names and Naming Contexts 133
SECTION 11 – DSA OPERATIONAL FRAMEWORK 135
25 Overview 135
25.1 Definitions 135
25.2 Introduction 135
26 Operational bindings 135
26.1 General 135
26.2 Application of the operational framework 136
26.3 States of cooperation 137
27 Operational binding specification and management 138
27.1 Operational binding type specification 138
27.2 Operational binding management 139
27.3 Operational binding specification templates 139
28 Operations for operational binding management 141
28.1 Application-context definition 141
28.2 Establish Operational Binding operation 142
28.3 Modify Operational Binding operation 145
28.4 Terminate Operational Binding operation 147
28.5 Operational Binding Error 148
28.6 Operational Binding Management Bind and Unbind 149
SECTION 12 – INTERWORKING WITH LDAP 151
29 Overview 151
29.1 Definitions 151
29.2 Introduction 151
30 LDAP interworking model 151
30.1 LDAP interworking scenarios 151
30.2 Overview of bound DSA handling LDAP operations 152
30.3 General LDAP requestor characteristics 152
30.4 LDAP extension mechanisms 153
31 LDAP specific system schema 153
31.1 Operational Attribute types from IETF RFC 4512 153
Annex A – Object identifier usage 156
Annex B – Information framework in ASN.1 159
Annex C – Subschema administration in ASN.1 170
Annex D – Service administration in ASN.1 175
Annex E – Basic Access Control in ASN.1 179
Annex F – DSA operational attribute types in ASN.1 183
Annex G – Operational binding management in ASN.1 186
Annex H – Enhanced security in ASN.1 191
Annex I – LDAP system schema 194
Annex J – The mathematics of trees 196
Annex K – Name design criteria 197

Annex L – Examples of various aspects of schema 199
L.1 Example of an attribute hierarchy 199
L.2 Example of a subtree specification 199
L.3 Schema specification 200
L.4 DIT content rules 201
L.5 DIT context use 202
Annex M – Overview of basic access control permissions 203
M.1 Introduction 203
M.2 Permissions required for operations 203
M.3 Permissions affecting error 204
M.4 Entry level permissions 204
M.5 Entry level permissions 205
Annex N – Examples of access control 206
N.1 Introduction 206
N.2 Design principles for Basic Access Control 206
N.3 Introduction to example 207
N.4 Policy affecting the definition of specific and inner areas 208
N.5 Policy affecting the definition of Directory Access Control Domains (DACDs) 209
N.6 Policy expressed in prescriptiveACI attributes 212
N.7 Policy expressed in subentryACI attributes 216
N.8 Policy expressed in entryACI attributes 217
N.9 ACDF examples 218
N.10 Rule-based access control 220
Annex O – DSE type combinations 221
Annex P – Modelling of knowledge 223
Annex Q – Subfilters 227
Annex R – Compound entry name patterns and their use 228
Annex S – Naming concepts and considerations 230
S.1 History tells us …. 230
S.2 A new look at name resolution 230
Annex T – Alphabetical index of definitions 236
Annex U – Amendments and corrigenda 238