ISO/IEC 9594-2:2008-12 (E)

Information technology_- Open Systems Interconnection_- The Directory: Models

CONTENTS

Page

Foreword viii
Introduction ix

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 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 4
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 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 Names 23
9.4 Name matching 25
9.5 Names returned during operations 25
9.6 Names held as attribute values or used as parameters 25
9.7 Distinguished Names 26
9.8 Alias Names 27
10 Hierarchical groups 27
10.1 Definitions 27
10.2 Hierarchical relationship 28
10.3 Sequential ordering of a hierarchical group 28

Page

SECTION 4 – DIRECTORY ADMINISTRATIVE MODEL 30

11 Directory Administrative Authority model 30
11.1 Definitions 30
11.2 Overview 30
11.3 Policy 31
11.4 Specific administrative authorities 31
11.5 Administrative areas and administrative points 32
11.6 DIT Domain policies 34
11.7 DMD policies 34

SECTION 5 – MODEL OF DIRECTORY ADMINISTRATIVE AND OPERATIONAL INFORMATION 36

12 Model of Directory Administrative and Operational Information 36
12.1 Definitions 36
12.2 Overview 36
12.3 Subtrees 37
12.4 Operational attributes 39
12.5 Entries 40
12.6 Subentries 40
12.7 Information model for collective attributes 41
12.8 Information model for context defaults 42

SECTION 6 – THE DIRECTORY SCHEMA 43

13 Directory Schema 43
13.1 Definitions 43
13.2 Overview 43
13.3 Object class definition 45
13.4 Attribute type definition 46
13.5 Matching rule definition 49
13.6 Relaxations and tightenings 51
13.7 DIT structure definition 57
13.8 DIT content rule definition 59
13.9 Context type definition 61
13.10 DIT Context Use definition 62
13.11 Friends definition 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 hierarchical groups 68
14.10 Maintenance of system schema 69
14.11 System schema for first-level subordinates 70

15 Directory schema administration 70
15.1 Overview 70
15.2 Policy objects 70
15.3 Policy parameters 70
15.4 Policy procedures 71
15.5 Subschema modification procedures 71
15.6 Entry addition and modification procedures 72
15.7 Subschema policy attributes 72

Page

SECTION 7 – DIRECTORY SERVICE ADMINISTRATION 78

16 Service Administration Model 78
16.1 Definitions 78
16.2 Service-type/user-class model 78
16.3 Service-specific administrative areas 79
16.4 Introduction to search-rules 80
16.5 Subfilters 80
16.6 Filter requirements 81
16.7 Attribute information selection based on search-rules 81
16.8 Access control aspects of search-rules 81
16.9 Contexts aspects of search-rules 82
16.10 Search-rule specification 82
16.11 Matching restriction definition 90
16.12 Search-validation function 90

SECTION 8 – SECURITY 91

17 Security model 91
17.1 Definitions 91
17.2 Security policies 91
17.3 Protection of Directory operations 92

18 Basic Access Control 93
18.1 Scope and application 93
18.2 Basic Access Control model 93
18.3 Access control administrative areas 95
18.4 Representation of Access Control Information 98
18.5 ACI operational attributes 103
18.6 Protecting the ACI 104
18.7 Access control and Directory operations 104
18.8 Access Control Decision Function 104
18.9 Simplified Access Control 106

19 Rule-based Access Control 106
19.1 Scope and application 106
19.2 Rule-based Access Control model 107
19.3 Access control administrative areas 107
19.4 Security Label 107
19.5 Clearance 109
19.6 Access Control and Directory operations 109
19.7 Access Control Decision Function 110
19.8 Use of Rule-based and Basic Access Control 110

20 Data Integrity in Storage 110
20.1 Introduction 110
20.2 Protection of an Entry or Selected Attribute Types 110
20.3 Context for Protection of a Single Attribute Value 112

SECTION 9 – DSA MODELS 113

21 DSA Models 113
21.1 Definitions 113
21.2 Directory Functional Model 113
21.3 Directory Distribution Model 114

Page

SECTION 10 – DSA INFORMATION MODEL 116

22 Knowledge 116
22.1 Definitions 116
22.2 Introduction 116
22.3 Knowledge References 117
22.4 Minimum Knowledge 119
22.5 First Level DSAs 120

23 Basic Elements of the DSA Information Model 120
23.1 Definitions 120
23.2 Introduction 120
23.3 DSA Specific Entries and their Names 121
23.4 Basic Elements 122

24 Representation of DSA Information 124
24.1 Representation of Directory User and Operational Information 124
24.2 Representation of Knowledge References 125
24.3 Representation of Names and Naming Contexts 131

SECTION 11 – DSA OPERATIONAL FRAMEWORK 133

25 Overview 133
25.1 Definitions 133
25.2 Introduction 133

26 Operational bindings 133
26.1 General 133
26.2 Application of the operational framework 134
26.3 States of cooperation 135

27 Operational binding specification and management 136
27.1 Operational binding type specification 136
27.2 Operational binding management 137
27.3 Operational binding specification templates 137

28 Operations for operational binding management 139
28.1 Application-context definition 139
28.2 Establish Operational Binding operation 140
28.3 Modify Operational Binding operation 142
28.4 Terminate Operational Binding operation 143
28.5 Operational Binding Error 144
28.6 Operational Binding Management Bind and Unbind 145

Annex A – Object identifier usage 146

Annex B – Information Framework in ASN.1 149

Annex C – SubSchema Administration Schema in ASN.1 159

Annex D – Service Administration in ASN.1 163

Annex E – Basic Access Control in ASN.1 167

Annex F – DSA Operational Attribute Types in ASN.1 171

Annex G – Operational Binding Management in ASN.1 174

Annex H – Enhanced security 178

Annex I – The Mathematics of Trees 181

Annex J – Name Design Criteria 182

Page

Annex K – Examples of various aspects of schema 184
K.1 Example of an attribute hierarchy 184
K.2 Example of a subtree specification 184
K.3 Schema specification 185
K.4 DIT content rules 186
K.5 DIT context use 187
Annex L – Overview of basic access control permissions 188
L.1 Introduction 188
L.2 Permissions required for operations 188
L.3 Permissions affecting error 189
L.4 Entry level permissions 189
L.5 Entry level permissions 190
Annex M – Examples of access control 192
M.1 Introduction 192
M.2 Design principles for Basic Access Control 192
M.3 Introduction to example 192
M.4 Policy affecting the definition of specific and inner areas 193
M.5 Policy affecting the definition of DACDs 195
M.6 Policy expressed in prescriptiveACI attributes 197
M.7 Policy expressed in subentryACI attributes 202
M.8 Policy expressed in entryACI attributes 203
M.9 ACDF examples 204
M.10 Rule-based Access Control 206
Annex N – DSE type combinations 207
Annex O – Modelling of knowledge 209
Annex P – Names held as attribute values or used as parameters 214
Annex Q – Subfilters 215
Annex R – Compound entry name patterns and their use 216
Annex S – Naming concepts and considerations 218
S.1 History tells us … 218
S.2 A new look at name resolution 218
Annex T – Alphabetical index of definitions 224
Annex U – Amendments and corrigenda 226