Working Implementation Agreements for Open Systems Interconnection Protocols: Part 11 - Directory Services Protocols

Output from the December 1993 (OIW) Open Systems Environment Implementors' Workshop (OIW)

SIG Chair: **Kenneth J. Rossen, SHL Systemhouse**
SIG Editor: **Michael Ransom, NIST**

Foreword

This part of the Working Implementation Agreements was prepared by the Directory Services Special Interest Group (DSSIG) of the Open Systems Environment Implementors' Workshop (OIW). See Part 1 - Workshop Policies and Procedures in the "Draft Working Implementation Agreements Document" for the workshop charter.

Text in this part has been approved by the Plenary of the above mentioned Workshop. This part replaces the previously existing chapter on Directory Services Protocol.

Please refer to the March 1992 Working Document for additional information.

Future changes and additions to this version of these Implementor Agreements will be published as change pages. Deleted and replaced text will be shown as strikeout. New and replacement text will be shown as shaded.

Table of Contents

List of Tables

Part 11 - Directory Services Protocols

Editor's Note - The text in this part of the Implementation Agreements will be significantly reorganized in 1993 due to the alignment and submission by Regional Workshops of International Standardized Profiles ISO/IEC pdiSP 10615 and 10616. The text in these pdISPs, in some cases containing technical changes, will replace substantial segments of the text in this Agreement. In addition, text addressing the forthcoming 1993 edition of the Directory Documents, currently interspersed among sections of this Agreement, will be moved to a new Agreement appearing in Part 28 of this document and expanded. Please refer to later editions of this document for the most recent of these realignments.

0 Introduction

Refer to clause 0 of Stable Agreements.

1 Scope

Refer to clause 1 of Stable Agreements.

2 Normative references

Refer to clause 2 of Stable Agreements.

3 Status

Refer to clause 3 of Stable Agreements.

4 Use of the Directory

This clause will contain introductory text.

4.1 MHS

(TBD)

4.2 FTAM

(TBD)

5 Directory ASEs and Application Contexts

Refer to clause 5 of Stable Agreements.

6 Schema

Refer to clause 6 of Stable Agreements.

6.1 Support of Structures and Naming Rules

Refer to 6.1 of Stable Agreements.

6.2 Support of Object Classes and Subclasses

Refer to 6.2 of Stable Agreements.

6.3 Support of Attribute Types

Refer to 6.3 of Stable Agreements.

6.4 Support of Attribute Syntaxes

Refer to 6.4 of Stable Agreements.

6.5 Naming Contexts

Refer to 6.5 of Stable Agreements.

6.6 Common Profiles

Refer to 6.6 of Stable Agreements.

6.6.1 OIW Directory Common Application Directory Profile

Refer to 6.6.1 of Stable Agreements.

6.6.1.1 Standard Application Specific Attributes and Attribute Sets

Refer to 6.6.1.1 of Stable Agreements.

6.6.1.2 Standard Application Specific Object Classes

Refer to 6.6.1.2 of Stable Agreements.

6.6.2 OIW Directory Strong Authentication Directory Profile

Refer to 6.6.2 of Stable Agreements.

6.6.2.1 Other Profiles Supported

Refer to 6.6.2.1 of Stable Agreements.

6.6.2.2 Standard Application Specific Object Classes

Refer to 6.6.2.2 of Stable Agreements.

6.7 Restrictions on Object Class Definitions

Refer to 6.7 of Stable Agreements.

7 Pragmatic Constraints

Refer to clause 7 of Stable Agreements.

7.1 General Constraints

Refer to 7.1 of Stable Agreements.

7.1.1 Character Sets

Refer to 7.1.1 of Stable Agreements.

7.1.2 DSP APDU Size

Refer to 7.1.2 of Stable Agreements.

7.1.3 Service Control (SC) Considerations

Refer to 7.1.3 of Stable Agreements.

7.1.4 Priority Service Control

Refer to 7.1.4 of Stable Agreements.

7.2 Constraints on Operations

Refer to 7.2 of Stable Agreements.

7.2.1 Filters

Refer to 7.2.1 of Stable Agreements.

7.2.2 Errors

Refer to 7.2.2 of Stable Agreements.

7.2.3 Error Reporting - Detection of Search Loop

Refer to 7.2.3 of Stable Agreements.

7.3 Constraints Relevant to Specific Attribute Types

Refer to 7.3 of Stable Agreements.

8 Conformance

Refer to clause 8 of Stable Agreements.

8.1 DUA Conformance

Refer to 8.1 of Stable Agreements.

8.2 DSA Conformance

Refer to 8.2 of Stable Agreements.

8.3 DSA Conformance Classes

Refer to 8.3 of Stable Agreements.

8.3.1 Conformance Class 0 - Centralized DSA

> **Editor's Note -** The following paragraph is to be added immediately after the existing final paragraph of this clause in the Stable Agreements.

A centralized DSA does not have knowledge information of any other DSA. As a result, such a DSA cannot provide the capability of a referral.

8.3.2 Conformance Class 1 - Distributed DSA

> **Editor's Note -** The following paragraph is to be added immediately after the existing final paragraph of this clause in the Stable Agreements.

A distributed DSA must meet the minimum knowledge requirement (Directory documents, clause 10 and 9.1.1 in these agreements). As a result, such a DSA shall provide the capability of a referral.

8.4 Authentication Conformance

Refer to 8.4 of Stable Agreements.

8.5 Directory Service Conformance

Refer to 8.5 of Stable Agreements.

8.6 The Directory Access Profile

Refer to 8.6 of Stable Agreements.

8.7 The Directory System Profile

Refer to 8.7 of Stable Agreements.

8.8 Digital Signature Protocol Conformance Profile

Refer to 8.8 of Stable Agreements.

8.9 Strong Authentication Protocol Conformance Profile

Refer to 8.9 of Stable Agreements.

8.10 Subtree Specification Classes

Refer to 8.10 of Stable Agreements.

8.11 Replication Conformance

Refer to 8.11 in Stable Agreements.

8.12 Recommended Practices for Shadowing

Refer to 8.12 in Stable Agreements.

9 Distributed Operations

Refer to clause 9 in Stable Agreements.

9.1 Static Requirements

Refer to 9.1 in Stable Agreements.

9.1.1 Reference Types

Refer to 9.1.1 in Stable Agreements.

9.1.2 Superior References and Root Contexts

Refer To 9.1.2 in Stable Agreements.

9.1.2.1 First-Level DSAs

Refer to 9.1.2.1 in Stable Agreements.

9.1.2.2 Return-Cross-References

Refer to 9.1.2.2 in Stable Agreements.

9.1.3 Support of Application Contexts

Refer to 9.1.3 in Stable Agreements.

9.1.4 DSA-level Security

Refer to 9.1.4 in Stable Agreements.

9.1.5 Aliases

Refer to 9.1.5 of Stable Agreements.

9.1.6 Authentication for DSA Bind

Refer to 9.1.6 of Stable Agreements.

9.1.7 Authentication of User Whose Entry Is Held by Another DSA

Refer to 9.1.7 of Stable Agreements.

9.2 Dynamic Requirements

9.2.1 Detection of Search Loop

Refer to 9.2.1 of Stable Agreements.

9.2.2 Generation of Trace Information

Refer to 9.2.2 of Stable Agreements.

9.2.3 Integrity of Operation Arguments

Refer to 9.2.3 of Stable Agreements.

9.2.4 Referrals and Chaining

Refer to 9.2.4 of Stable Agreements.

9.2.5 Name-Error: "invalid-attribute-syntax"

Editor's Note - Editor's instructions from the September Workshop indicated that the following sentence was to be added as a note to Table 13 (from Stable Agreements): "This error shall only be generated when the DSA determines that there is an incompatibility in an AVA in that part of the name which it is expected to resolve." That statement is not consistent with the current state of Table 13 in Stable Agreements - there are at least two uses of N(IAS) in Table 13 that are not even tied to the name resolution phase of an operation (e.g., see the Table 13 entry for Symptom: E_ATT_BOUNDS and Situation: Modify-RDN). This issue should be revisited at the next Workshop meeting; either the proposed statement must be modified or changes in Table 13 need to be approved.

Editor's Note - Editor's instructions from the September Workshop indicated that the following sentences are to be added as a note to Table 13 (from Stable Agreements): "If a multicasting DSA receives this error and the matched part of the name is equal to or longer than that indicated by the next RDN to be resolved, name resolution shall be taken as having progressed. The error shall be relayed." The note has been added as note #15 in the list of notes for Table 13. References to the new note have also been added to Table 13;

the new references need to be checked at the next Workshop.

Editor's Note - Editor's instructions from the September Workshop indicated that the following sentences are to be added as a note to Table 13 (from Stable Agreements): "If a chaining or multicasting DSA receives this error and the matched part of the name is not equal to or longer than that indicated by the next RDN to be resolved, the error indicates an incompatibility in schema between the DSA and the one to which chaining takes place. Multicasting may continue, and the error in that case may be ignored. A DSA, having received such an error during name resolution, may be need not relay it." The note has been added as note #16 in the list of notes for Table 13. References to the new note have also been added to Table 13; the new references need to be checked at the next Workshop.

9.2.6 Service-Error: "invalid-reference"

Editor's Note - Editor's instructions from the September Workshop indicated that the following sentences are to be added as a note to Table 13 (from Stable Agreements): "If a DSA generates a chained operation on the basis of a cross reference and receives a serviceError with the problem of invalidReference in response, then it is recommended that the invalid cross reference be removed to eliminate repeated errors. Note that attempting to resolve the correct reference via the returnCrossRefs mechanism should be regarded as nonreliable due to the optional nature of returnCrossRefs. The resolution of an invalidReference due to a superior or subordinate reference is a local administrative issue."

9.2.7 Unsupported Attributes

A DSA may receive an AVA that is unsupported by the DSA. If the DSA is not required to act on it, or to store it within an entry, it shall handle it by passing it on by chaining, or providing a referral, and in particular shall not return an error response on its own initiative.

9.2.8 Matching Names in traceInformation

A DSA, when performing loop avoidance, may be required to match names in traceInformation; in the (unlikely) event of the attribute type of an AVA in such a name being unsupported by the DSA, the DSA may forward the operation to the target DSA, since the consequential state of the operation is unknown.

10 Underlying Services

Refer to clause 10 of Stable Agreements.

10.1 ROSE

Refer to 10.1 of Stable Agreements.

10.2 Session

Refer to 10.2 of Stable Agreements.

10.3 ACSE

Refer to 10.3 of Stable Agreements.

11 Access Control

For information regarding access control in the 1988 Directory Documents, refer to clause 11 of Stable Agreements.

The following table is applicable to access control as defined in the 1992 Edition of the Directory Documents. The table below is for information only; definitive conformance requirements associated with Basic Access Control (BAC) and Simple Access Control (SAC) are specified in the 1992 Edition of the Directory Documents.

Table 1 - 1992 Extensions for Access Control

Extension	Required by BAC	Required by SAC
Subentries	yes	yes
Operational Attributes		
PrescriptiveACI	yes	yes
SubentryACI	yes	yes
EntryACI	yes	no
uniqueMember	yes	yes
groupOfUniqueNames (object class)	yes	yes
Extended ChainingArguments (includes AuthenticationLevel)	yes	yes
Extended ContinuationReference (includes returnToDUA)	yes	yes
Access Control Specific Area (ACSA)	yes	yes
Access Control Inner Area (ACIA)	yes	no
Extended EntryInformationSelection (includes ExtraAttributes)	yes	yes
Extended Matching Rule for ACIItem	yes	yes

11.1 Use of localQualifier in AuthenticationLevel

Editor's Note - for future study

11.2 Distributed Administrative Areas

Editor's Note - for future study

11.3 ProtectedItem Granularity

Editor's Note - for future study

11.4 UserClass Granularity

Editor's Note - for future study

12 Test Considerations

Refer to clause 12 of Stable Agreements.

12.1 Major Elements of Architecture

Refer to 12.1 of Stable Agreements.

12.2 Search Operation

Refer to 12.2 of Stable Agreements.

13 Errors

Refer to clause 13 of Stable Agreements.

13.1 Permanent vs. Temporary Service Errors

Refer to 13.1 of Stable Agreements.

13.2 Guidelines for Error Handling

Refer to 13.2 of Stable Agreements.

13.2.1 Introduction

Refer to 13.2.1 of Stable Agreements.

13.2.2 Symptoms

Refer to 13.2.2 of Stable Agreements.

13.2.3 Situations

Refer to 13.2.3 of Stable Agreements.

13.2.4 Error Actions

Refer to 13.2.4 of Stable Agreements.

13.2.5 Reporting

Refer to 13.2.5 of Stable Agreements.

14 Specific Authentication Schemes

Refer to 14 of Stable Agreements.

14.1 Specific Strong Authentication Schemes

Refer to 14.1 of Stable Agreements.

14.2 Protected Simple Authentication

Refer to 14.2 of Stable Agreements.

14.3 Simple Authentication

Refer to 14.3 of Stable Agreements.

Annex A (normative)

Maintenance of Attribute Syntaxes

Refer to Annex A of Stable Agreements.

A.1 Introduction

Refer to A.1 of Stable Agreements.

A.2 General Rules

Refer to A.2 of Stable Agreements.

A.3 Checking Algorithms

Refer to A.3 of Stable Agreements.

A.3.1 distinguishedNameSyntax

Refer to A.3.1 of Stable Agreements.

A.3.2 integerSyntax

Refer to A.3.2 of Stable Agreements.

A.3.3 telephoneNumberSyntax

Refer to A.3.3 of Stable Agreements.

A.3.4 countryName

Refer to A.3.4 of Stable Agreements.

A.3.5 preferredDeliveryMethod

Refer to A.3.5 of Stable Agreements.

A.3.6 presentationAddress

Refer to A.3.6 of Stable Agreements.

A.4 Matching Algorithms

Refer to A.4 of Stable Agreements.

A.4.1 UTCTimeSyntax

Refer to A.4.1 of Stable Agreements.

A.4.2 distinguishedNameSyntax

Refer to A.4.2 of Stable Agreements.

A.4.3 caseIgnoreListSyntax

Refer to A.4.3 of Stable Agreements.

Annex B (informative)

Glossary

Refer to Annex B of Stable Agreements.

Annex C (informative)

Requirements for Distributed Operations

Refer to Annex C of Stable Agreements.

C.1 General Requirements

Refer to C.1 of Stable Agreements.

C.2 Protocol Support

Refer to C.2 of Stable Agreements.

C.2.1 Usage of ChainingArguments

Refer to C.2.1 of Stable Agreements.

C.2.2 Usage of ChainingResults

Refer to C.2.2 of Stable Agreements.

C.3 The Root Context

The root context as held by a first level DSA consists of the root and a number of subordinate references to naming contexts held (as master copies) by the DSA and by other first level DSAs. It is replicated to each first level DSA and comprises full knowledge of the naming contexts immediately subordinate to the root of the DIT. The means of this replication is not standardized.

Annex D (informative)

Guidelines for Applications Using the Directory

Refer to Annex D of Stable Agreements.

D.1 Tutorial

Refer to D.1 of Stable Agreements.

D.1.1 Overview

Refer to D.1.1 of Stable Agreements.

D.1.2 Use of the Directory Schema

Refer to D.1.2 of Stable Agreements.

D.1.2.1 Use of Existing Object Classes

Refer to D.1.2.1 of Stable Agreements.

D.1.2.2 Kinds of Object Classes

Refer to D.1.2.2 of Stable Agreements.

D.1.2.3 Use of Unregistered Object Classes

Refer to D.1.2.3 of Stable Agreements.

D.1.2.4 Side Effects of Creating Unregistered Object Classes

Refer to D.1.2.4 of Stable Agreements.

D.2 Creation of New Object Classes

Refer to D.2 of Stable Agreements.

D.2.1 Creation of New Subclasses

Refer to D.2.1 of Stable Agreements.

D.2.2 Creation of New Attributes

Refer to D.2.2 of Stable Agreements.

D.3 DIT Structure Rules

Refer to D.3 of Stable Agreements.

Annex E (informative)

Template for an Application Specific Profile for Use of the Directory

Refer to Annex E of Stable Agreements.

Annex F (informative)

Bibliography

Refer to Annex F of Stable Agreements.