INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10615-6

First edition
1998-09-15

Information technology — International Standardized Profiles ADInn — OSI Directory —

Part 6:
ADI32 — DSA Support for Distributed Operations

Technologies de l'information — Profils normalisés internationaux ADInn — L'Annuaire OSI —

Partie 6: ADI32 — Support DSA d'opérations réparties

Reference number
ISO/IEC ISP 10615-6:1998(E)

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. In addition to developing International Standards, ISO/IEC JTC 1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or a set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75 % of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 10615-6 was prepared with the collaboration of

— Asia-Oceania Workshop (AOW);

— European Workshop for Open Systems (EWOS);

— Open Systems Environment Implementors' Workshop (OIW).

ISO/IEC ISP 10615 consists of the following parts, under the general title *Information technology — International Standardized Profiles ADInn — OSI Directory*:

— *Part 1: ADI11 — DUA Support of Directory Access*

— *Part 2: ADI12 — DSA Support of Directory Access*

— *Part 3: ADI21 — DSA Performer Role*

— *Part 4: ADI22 — DSA Invoker Role*

— *Part 5: ADI31 — DUA Support for Distributed Operations*

— *Part 6: ADI32 — DSA Support for Distributed Operations*

— *Part 7: ADI41 — Specific Digital Signature Schemes*

— *Part 8: ADI4X — Use of Strong Authentication*

Annexes A and B form an integral part of this part of ISO/IEC ISP 10615. Annexes C and D are for information only.

Introduction

The concept and structure of International Standardized Profiles for Information Systems are laid down in the Technical Report ISO/IEC TR 10000. The purpose of an International Standardized Profile is to recommend when and how certain information technology standards shall be used. This International Standardized Profile ISO/IEC ISP 10615-6 specifies application profile ADI32 "DSA Support of Distributed Operations" as defined in the Technical Report ISO/IEC TR 10000-2.

This profile has been derived by EWOS/ETSI as editing workshop from the corresponding European profile A/DI32, published by EWOS as ED 024, and published by CEN as ENV 41215.

It has been reviewed in the process of development by AOW/INTAP, by OIW and by EWOS/ETSI, and changes have been made to accommodate comments from these other workshops.

Information technology — International Standardized Profiles ADInn — OSI Directory —

Part 6:
ADI32 — DSA Support for Distributed Operations

1 Scope

1.1 General

The Directory Standards define not only the protocol but also the behaviour of DSAs when they collaborate to carry out the purpose of the Directory. In order to achieve consistency and full interoperability, it is necessary to select from the options and interpretations laid down in the Directory Standards, and in particular within [ISO/IEC 9594-4 | CCITT X.518].

This part of ISO/IEC ISP 10615 specifies the behaviour of DSAs in exercising the DAP, the DSP, or both, that is required to carry out Distributed Operations in accordance with these requirements.

The scope of this part of ISO/IEC ISP 10615 is to define:

- Static capabilities that are required by DSAs in order to achieve acceptable levels of service in co-operation with other DSAs
- Procedures, based on procedures given within the base standards, in the detail required to achieve consistency and interoperability
- Protocol use, as required to implement the procedures

It is applicable to DSAs implementing the '88 Directory Standards [ISO/IEC 9594:1990 | CCITT X.500:1988].

It applies to all DSAs that contain a component of the distributed Directory, although many of its requirements are inapplicable to DSAs that do not support the invocation of DSP operations.

Implementations claiming conformance to this part of ISO/IEC ISP 10615 may be based on either ISO/IEC 9594 or CCITT X.500 or both. There are no practical differences as far as this part of ISO/IEC ISP 10615 is concerned.

This part of ISO/IEC ISP 10615 is not free-standing. Compliance with this part of ISO/IEC ISP 10615 requires compliance with ISO/IEC ISP 10615 parts 2 to 4 inclusive, and with normative references identified in those documents. Conversely, this part of the part of ISO/IEC ISP 10615 is applicable to DSAs which conform to other parts of ISO/IEC ISP 10615, and in particular to parts 2 (ADI12), 3 (ADI21) and 4 (ADI22).

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10615 is identified in ISO/IEC TR 10000-2 as ADI32 "Directory - Distributed Operations - DSA Support of Distributed Operations".

1.3 Scenario

In the Distributed Directory, one mode of interaction is the chaining (including multicasting) of enquiries in accordance with the procedures laid down in [ISO/IEC 9594-4 | CCITT X.518]. Another is the following of referrals and of embedded continuation references.

In carrying out these procedures, a DSA is accessed by a DUA or another DSA, and carries out the requested action with or without reference to other DSAs. This part of ISO/IEC ISP 10615 is concerned with

the information contained in a DSA to enable it to determine that other DSAs are involved, and with the procedures whereby other DSAs can be involved, by the use of chaining or referrals (Figure 1).

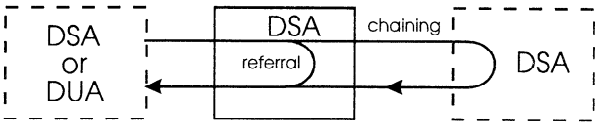

Figure 1-DSA Behaviour for Distributed Operations

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 10615. At the time of publication, the editions indicated were valid. All documents are subject to revision and parties to agreements based on this part of ISO/IEC ISP 10615 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and ITU-T maintains published editions of its current Recommendations.

2.1 Paired CCITT Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.208:1988, *Data Communications – Open Systems Interconnection (OSI) – Specification of Abstract Syntax Notation One (ASN.1).*

  ISO/IEC 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*

- CCITT Recommendation X.209:1988, *Data Communications – Open Systems Interconnection (OSI) – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

  ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

- CCITT Recommendation X.219:1988, *Data Communications – Open Systems Interconnection (OSI) – Remote Operations: Model, notation and service definition.*

  ISO/IEC 9072-1:1989, *Information processing systems – Text communication – Remote Operations – Part 1: Model, notation and service definition.*

- CCITT Recommendation X.229:1988, *Data Communications – Open Systems Interconnection (OSI) – Remote Operations: Protocol Specification.*

  ISO/IEC 9072-2:1989, *Information processing systems – Text communication – Remote Operations – Part 2: Protocol specification.*

- CCITT Recommendation X.500:1988, *Data Communication Networks – The Directory – Overview of Concepts, Models and Services.*

  ISO/IEC 9594-1:1990, *Information technology – Open Systems Interconnection – The Directory – Part 1: Overview of concepts, models and services.*

- CCITT Recommendation X.501:1988, *Data Communication Networks – The Directory – Models.*

  ISO/IEC 9594-2:1990, *Information technology – Open Systems Interconnection – The Directory – Part 2: Models.*

- CCITT Recommendation X.509:1988, *Data Communication Networks – The Directory – Authentication Framework.*

ISO/IEC 9594-8:1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework.*

- CCITT Recommendation X.511:1988, *Data Communication Networks – The Directory – Abstract Service Definition.*

  ISO/IEC 9594-3:1990, *Information technology – Open Systems Interconnection – The Directory – Part 3: Abstract service definition.*

- CCITT Recommendation X.518:1988, *Data Communication Networks – The Directory – Procedures for Distributed Operation.*

  ISO/IEC 9594-4:1990, *Information technology – Open Systems Interconnection – The Directory – Part 4: Procedures for distributed operation.*

- CCITT Recommendation X.519:1988, *Data Communication Networks – The Directory – Protocol Specifications.*

  ISO/IEC 9594-5:1990, *Information technology – Open Systems Interconnection – The Directory – Part 5: Protocol specifications.*

- CCITT Recommendation X.520:1988, *Data Communication Networks – The Directory – Selected Attribute Types.*

  ISO/IEC 9594-6:1990, *Information technology – Open Systems Interconnection – The Directory – Part 6: Selected attribute types.*

2.2 Normative Amendments and Technical Corrigenda

In accordance with ISO/IEC TR10000-1 subclause 6.3.2 c), attention is drawn to normative Amendments and Technical Corrigenda affecting the Directory Standards documents ISO/IEC 9594:1990 and the CCITT X.500:1988 recommendations.

Annex B defines the references to the agreed amendments and corrigenda. Compliance with these amendments and corrigenda is necessary to achieve the interoperability requirements for this document. It also identifies those which appear to be relevant to this part of ISO/IEC ISP 10615.

2.3 Additional normative references

- ISO/IEC TR 10000-1:1995, Information technology-Framework and Taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework.
- ISO/IEC TR 10000-2:1992, Information technology-Framework and Taxonomy of International Standardized Profiles - Part 2: Principles and taxonomy for OSI profiles.
- ISO/IEC ISP 10616-1:1995 Information technology - International Standardized Profile FDI11 - Directory data definitions - Common Directory Use (Normal)
- ISO/IEC ISP 11188-1:1995 Information technology - International Standardized Profile - Common upper layer requirements - Part 1: Basic connection oriented requirements
- CCITT Recommendation X.581:1992, Directory Access Protocol - Protocol Implementation Conformance Statement (PICS) Proforma.
- CCITT Recommendation X.582:1992, Directory System Protocol - Protocol Implementation Conformance Statement (PICS) Proforma.

3 Definitions

3.1 General

Many of the definitions used may be found in the referenced base standards. Since not all of the definitions are to be found in the Definitions clauses within the standards documents, references are listed in Table 1

below. The "Part" reference refers to the part number within ISO/IEC 9594 or its CCITT equivalent (see also Clause 2).

Table 1: Definitions and references

Term	Part	Reference
Administrative authority	2	5.1.3
Continuation reference	4	12.9
Cross reference	4	3.5.3
Evaluation Phase	4	17.2
First Level DSA	4	10.2
Internal reference	4	3.5.6
List (I) Procedure	4	18.7.2.1.1
List (II) Procedure	4	18.7.2.1.2
Name Resolution Phase	4	12.5.2.1
Naming context	4	3.5.12 [1]
Non-specific subordinate reference	4	3.5.13
Partial Outcome Qualifier	3	10.1.3.3
Presentation address	6	5.9.1
Referral	4	3.5.16
Results Merging Phase	4	17.2.3
Root Context	4	3.5.18
Search (I) Procedure	4	18.7.2.2.1
Search (II) Procedure	4	18.7.2.2.2
Subordinate reference	4	3.5.19
Superior reference	4	3.5.21

The terms in the following subclauses are defined for the purposes of this part of ISO/IEC ISP 10615.

a) *Caching*: The process of creating cache copies of entries or part of an entries whose consistency with the corresponding source entries is maintained by local means;

d) *Replication:* The process by which copies of entry and operational information are held by DSAs other than the master DSA;

e) *Shadowing*: Replication between two DSAs whereby the information is copied and maintained using a suitable Directory Information Shadowing Protocol;

f) *Find Naming Context procedure*: The procedure specified by [ISO/IEC 9594-4 | CCITT X.518] clause 18.6.5 and illustrated in Figure 8 of that document.

g) *Local Name Resolution procedure*: The procedure specified by [ISO/IEC 9594-4 | CCITT X.518] clause 18.6.6 and illustrated in Figure 9 of that document.

h) *Object Evaluation procedure*: The procedure specified by [ISO/IEC 9594-4 | CCITT X.518] clause 18.7.

i) *Results Merging procedure*: The procedure specified by [ISO/IEC 9594-4 | CCITT X.518] clause 18.8.

j) *Operation Performing Cycle*: An element of processing within a single DSA which includes a single Find Naming Context procedure with Local Name Resolution procedure as appropriate, together with

[1] Reference should be made to the corrigendum (ISO/IEC 9594-4: 1988/COR 2 1992(E)) , which redefines this item.

any associated Operation Evaluation procedures and Results Merging procedures; each alias encountered typically generates a separate Operation Performing Cycle.

3.2 Support Level

To specify the support level of protocol features for this part of ISO/IEC ISP 10615, the following terminology is defined.

3.2.1 Mandatory: m: Mandatory requirement for support

A feature is supported by a DSA implementation if the DSA is able to process the feature in accordance with the base standard or as specified in this part of ISO/IEC ISP 10615.

3.2.2 Optional: o: Optional requirement for support

The support of the feature is left to the implementor of the DSA.

3.2.3 Conditional: c: Conditional requirement for support

The requirement to support the item depends on a specified condition. The condition and the resulting support requirements are stated separately.

4 Abbreviations

The following abbreviations are used as defined in [ISO/IEC 9594 | CCITT X.500] or in ISO/IEC TR 10000-1 :

APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
AVA	Attribute Value Assertion
DAP	Directory Access Protocol
DIB	Directory Information Base
DIT	Directory Information Tree
DMD	Directory Management Domain
DSA	Directory System Agent
DSP	Directory System Protocol
DUA	Directory User Agent
ISP	International Standardized Profile
NSSR	Non-Specific Subordinate Reference
POQ	Partial outcome qualifier
PRL	Profile Requirements List
RDN	Relative Distinguished Name

5 Conformance

Conformance to this part of ISO/IEC ISP 10615 concerns the implementation of procedures which DSAs shall support. The compliance of a DSA with these procedures shall be capable of being tested by setting up suitable test suites, which, however, shall observe only the externally observable behaviour of the DSA. The conformance statements of this part of ISO/IEC ISP 10615 lay down the range of information for suitable DSA test suites.

In practice, the behaviour of an actual DSA may depend on multiple conditions, like access control, or schema or other restrictions applied for administrative reasons. Therefore test suites, even if applicable in principle, cannot be performed successfully in all situations. A DSA is conformant according to this part of ISO/IEC ISP 10615 if the DSA, after suitable set-up, is able to successfully carry out test suites within the range of information defined in this part of ISO/IEC ISP 10615.

NOTE. Suitable set-up is implied within this part of ISO/IEC ISP 10615.

DSAs claiming conformance to this part of ISO/IEC ISP 10615 shall satisfy the basic conformance requirement for distributed operations defined in [ISO/IEC 9594-5 | CCITT X.519] in clause 9.2.3; corresponding to each operation invoked by a requestor, performing DSAs shall behave in accordance with well-defined procedures so that an appropriate response will be returned deterministically.

Conformance requirements relating to this part of ISO/IEC ISP 10615 which lie outside standards requirements are listed in clause A.7 of Annex A.

6 Static conformance requirements

To conform to this part of ISO/IEC ISP 10615, implementations shall conform to all requirements of clause 9.2.2 of [ISO/IEC 9594-5 | CCITT X.519], and also to requirements identified in clause 18.1 of [ISO/IEC 9594-4 | CCITT X.518]; they shall conform to the requirements stated in the IPRL (Annex A) and to the remainder of this clause.

6.1 Elements of Distributed Operations

6.1.1 Reference Types

This part of ISO/IEC ISP 10615 requires conforming implementations to be able to hold and use reference types as summarised in Table 2 below.

Table 2: Reference Types

Reference types	Holding and using capability	Notes
Superior	Mandatory	Non-first-level DSAs shall hold precisely one single Superior Reference. All DSAs shall be capable of acting as a non-first-level DSA, and so are required to support a Superior Reference.
Subordinate	Mandatory	
Cross-reference	Optional	Support of Cross References may be required for particular configurations of DSA.
Non-specific Subordinate	Optional	

A DSA conformant to this part of ISO/IEC ISP 10615 shall be capable of holding and using a (single) Superior Reference.

DSAs conformant with this part of ISO/IEC ISP 10615 may optionally be able to hold and use Cross References.

NOTES.

1 [ISO/IEC 9594-4 | CCITT X.518] and this part of ISO/IEC ISP 10615 do not define any standardised procedures for creating, updating and deleting references or naming contexts.

2 A Cross Reference may be or become incorrect, or it may be temporarily or permanently unusable. No procedure is defined to handle these situations, which should nevertheless be taken into account in the design of DSAs.

3 There is currently no established mechanism whereby a DUA (or DSA) that receives an invalid reference from a DSA can advise that DSA of the fact, so that rectification can take place.

6.1.2 Knowledge References And the Root Context

6.1.2.1 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 comprises full knowledge of the naming contexts immediately subordinate to the root of the DIT.

The Directory standards require that the whole of the root context is replicated to and held by each First Level DSA. The procedures for accomplishing this replication are not standardised.

NOTE. See also [ISO/IEC 9594-4 | X.518] clause 10.2 for a more comprehensive statement of requirements.

6.1.2.2 First-Level DSAs

The concept of First-Level DSAs has been defined with a view to permitting centralisation of the Directory knowledge information needed for international interworking and navigation within a single country.

A DSA conformant to this part of ISO/IEC ISP 10615 and capable of acting as a First Level DSA shall be able to hold and use the Root Context and in addition shall hold as master (i.e. have administrative authority for) at least one Naming Context immediately subordinate to the root of the DIT. A DSA conforming to this part of ISO/IEC ISP 10615 is not, however, required to have the capability of being a First Level DSA.

There is no mandatory requirement for DSAs capable of acting as first-level DSAs to support Non-specific Subordinate References within the root context even if they claim to support Non-specific Subordinate References generally.

NOTE. If the root context contains a Non-specific Subordinate References, DSAs have potentially to multicast the operation to each other first-level DSA to determine whether the entry's first RDN exists.

6.1.2.3 Subordinate References

DSAs conformant to this part of ISO/IEC ISP 10615 shall be able to hold Naming Contexts which use Subordinate References.

DSAs shall be able to hold multiple subordinate references subordinate to a single entry in the DIT (Figure 2).

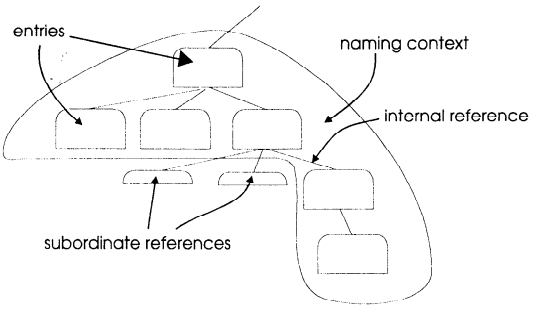

Figure 2—Support of subordinate references

DSAs shall also be able to hold local entries (accessible by internal reference) subordinate to an entry that is the immediate superior of a subordinate reference.

6.1.2.4 Non-Specific Subordinate References

DSAs conformant to this part of ISO/IEC ISP 10615 may optionally be able to hold Naming Contexts which use Non-Specific Subordinate References (NSSRs).

DSAs that support NSSRs shall be able to hold multiple Non-specific Subordinate References subordinate to a single entry in the DIT (Figure 3).

DSAs that support NSSRs shall be able to hold subordinate references and internal references subordinate to the entry associated with each NSSR.

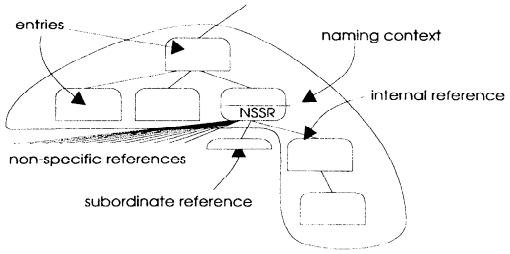

Figure 3—Support of NSSRs

6.1.2.5 Return-Cross-References

The support of the "return-cross-references" facility by the generation of protocol from internally stored information, either as requester or as supplier, as defined in [ISO/IEC 9594-4 | CCITT X.518] clause 10.4.1 is optional. (Support of the protocol elements itself, e.g. to relay cross-references, is mandatory - see **returnCrossRefs** in Table A.4.3.2.1 of ADI21 and Table A.4.3.2.1 of ADI22)

6.2 Administrative Authorities

6.2.1 Mandatory Administrative Authority Roles

DSAs shall be able to carry out the following specific roles of Administrative Authorities for Distributed Operations (here the term "Current DSA" is used to indicate the DSA under consideration).

How the administrative authority performs these roles is outside the scope of this part of ISO/IEC ISP 10615.

6.2.1.1 Naming Contexts

DSAs shall be able to create, update and delete Naming Contexts, thereby effecting the transition of authority for portions of the DIT (this calls for the presence of a subordinate reference in another DSA—the superior DSA—that references the current DSA—see Figure 4 below).

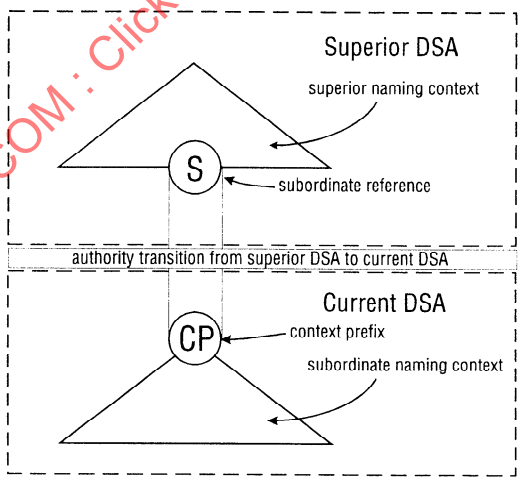

Figure 4—Authority Transition-Subordinate DSA

6.2.1.2 Superior references

Support of superior references is mandatory, although a DSA that is acting as a first-level DSA possesses no superior reference. DSA claiming support of a superior reference shall be able to create, update (i.e. change the name or presentation address, or both, for the referenced DSA). It shall also be capable of deleting the reference if required to become a first-level DSA.

6.2.1.3 Subordinate references

DSAs shall be able to create, update and delete Subordinate References, thereby effecting the transition of authority for portions of the DIT from the current DSA to another DSA (see Figure 5 below)

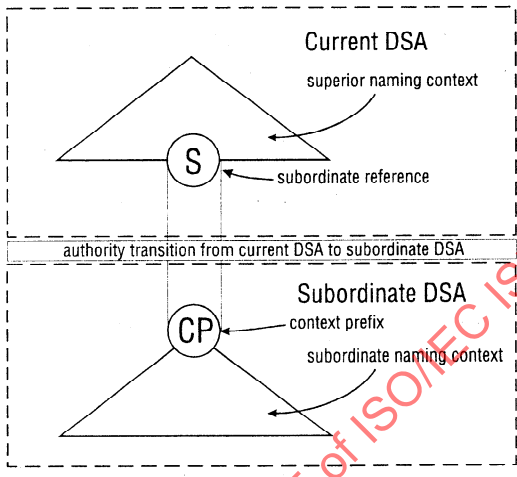

Figure 5—Authority Transition-Superior DSA

6.2.1.4 Correcting Knowledge Information

DSAs shall be able to rectify errors in knowledge information (e.g. Presentation Address and AETitle) by appropriate local means (for example, errors detected as a result of inconsistencies in Knowledge or of Naming Context information), and in particular shall be able to correct access-point information for any knowledge reference supported while maintaining consistency, or permitting the maintenance of consistency, between references to particular DSAs.

6.2.2 Optional Administrative Authority Roles

6.2.2.1 Cross references

Support of cross references is optional; however, a DSA claiming support of cross references shall be capable of the creation, updating (i.e. changing the name, presentation address, or both, for the referenced DSA) and deletion of cross-references.

6.2.2.2 Non-specific subordinate references

Support of Non-specific Subordinate References is optional; however, a DSA claiming support of Non-specific Subordinate References shall be capable of the creation, updating (i.e. changing the name, presentation address, or both, for each referenced DSA) and deletion of Non-specific Subordinate References.

6.2.2.3 Naming contexts comprising a single alias

DSAs are not obliged to contain naming contexts which consist of a single alias as the sole entry in the naming context.

NOTE. The use of such naming contexts may be required for certain Directory naming schemes (e.g. having dual naming schemes in which every RDN in the distinguished name of an entry has a corresponding alias).

6.3 Support of Application Contexts

All DSAs conformant to this part of ISO/IEC ISP 10615 shall support the **DirectoryAccessAC** or **DirectorySystemAC** or both.

A DSA which is to permit the dissemination of its knowledge references to one or more DSAs within another DMD (Directory Management Domain) is obliged to support the DirectorySystemAC, at least as a responder to chained operations. (see [ISO/IEC 9594-5 | CCITT X.519] Clause 9.2.1a.)

NOTE. If a DSA does not support the DirectorySystemAC, it may not be able to carry out simple authentication of a user whose entry is not held by that DSA (see clauses 6.3.2 and D.9 in Annex D of this part of ISO/IEC ISP 10615).

A DSA that can only act as an acceptor is not obliged to be able to generate a DSA-BIND (or DSA-UNBIND).

All DSAs supporting the DirectorySystemAC shall, however, be able to invoke an A-ABORT on an incoming DSP association.

6.3.1 Referral Mode

A DSA conforming to this part of ISO/IEC ISP 10615 shall be able to use the referral mode of interaction, even if it only supports the DirectorySystemAC.

6.4 Aliases

DSAs conformant with this specification shall be able to carry out Name Resolution and search continuation with respect to Aliases held outside the DSA (as well as those held inside the DSA).

6.5 Authentication for DSA-Bind

6.5.1 Forms Of Authentication

DSAs conforming to this part of ISO/IEC ISP 10615 that support the DirectorySystemAC shall be able to carry out the authentication of DSAs using simple unprotected authentication with password, with optional capability of using the following methods:

- Simple protected authentication
- Strong authentication
- External authentication procedure

NOTE. The bulleted options are outside the scope of this part of ISO/IEC ISP 10615.

A DSA shall be able to accept any valid DSA-Bind requests of any form, whether or not this form permits authentication, and even whether or not the authentication can be verified.

NOTE. DSAs should perhaps be encouraged not to emit authentication elements when they cannot be used, but there is a significant issue about how they are to determine when authentication (of a particular form) is appropriate and when it is not. DSAs probably ought to maintain a table from which they may find or deduce which DSAs should be recipients of authentication elements.

7 Procedures

7.1 Name Resolution

7.1.1 General Requirements

[ISO/IEC 9594-4 | CCITT X.518] defines a two-stage Name Resolution process, in which the Name Resolution is done first in terms of Naming Contexts ("Find Naming Context"), and subsequently in terms of entries (and possibly Subordinate or Non-specific Subordinate References) associated with a particular Naming Context ("Local Name Resolution").

This part of ISO/IEC ISP 10615 makes no specification as to the form of the Name Resolution procedure, provided that it is externally compatible with the standards. See Clause 7.3.3 which gives rules for the use of error reporting during Name Resolution.

7.1.2 Use Of Subordinate References

If the use of a Subordinate Reference results in an "invalid-reference" Service-Error, a DSA receiving such an error shall be able to return instead a "DIT-error" Service-Error (e.g. if security policy permits).

7.2 Request Decomposition

If a DSA is carrying out a list or search procedure involving multiple DSAs (i.e. it is carrying out a chaining operation in the course of a List or Search operation using the List (I) and List (II) procedures of X.518 clause 18.7.2.1 or the Search (I) or Search (II) procedures of X.518, clause 18.7.2.2), the DSA may receive an error indication from another DSA when it would normally expect to receive list or search entry data.

If such an error indication is received, it should not cause failure of the list or search operation, since to do so would prevent valid results being returned.

When it is possible that a DSA contains entry information that would normally be returned by following the continuation reference, but this fact is obscured by an error indication received from the DSA, PartialOutcomeQualifier shall be present and shall contain an unexplored element (defined as a **SET OF ContinuationReference**). There shall be a **ContinuationReference** element corresponding to the point of the tree at which continuation would have occurred, but this specific **ContinuationReference** element (which contains a **SET OF AccessPoint**) may optionally contain no access-point in respect of the particular DSA that reported the error. (Note that this could result in an empty SET OF access-points in the continuation reference.) This option avoids passing back a situation in which the DUA would only hit the same error if it attempted to follow the continuation reference.

7.3 Integrity of Operation Arguments

For any operation argument in the abstract service (ReadArgument, etc.) that can (in principle) be signed, the content of any such argument shall always be passed on unchanged (subject only to variations in ASN.1 encoding which do not affect primitive values).

In particular, elements having default values that are absent in the incoming ASN.1 shall remain absent, and defaulted elements that are present in the incoming ASN.1 shall remain present.

7.4 Use of Associations

7.4.1 Optional Establishment Of Ad-Hoc Associations

If as a consequence of Name Resolution, a DSA identifies a second DSA to which chaining is to take place (i.e. excluding the case of referrals), it has the following options:

Chain an operation to the DSA if an Association has already been established with it

Establish an Association with it which may be used to chain the operation

If neither of these are possible, the DSA shall indicate (if necessary) that an association cannot be established with the second DSA; this shall be treated as if the DSA to which the Association takes place had itself responded with a service problem "unavailable". Alternatively,the DSA may have a policy to return a referral, which optionally may contain an empty set of access points as recommended in 7.2 for the case of request decomposition.

7.5 Errors

7.5.1 General

Error handling is primarily described under the Abstract Operations part of the protocol ([ISO/IEC 9594-3 | CCITT X.511]). DSAs to which operations are chained using DSP shall respond to error situations so as to permit the correct error protocol to be generated by the DSA responding using DAP.

Errors arising from a particular basic condition may require different protocol responses, depending on the situation. Although Annex B "Error Handling for the Directory" gives recommendations for a wide variety of situations, some definite rules are needed in certain circumstances to ensure that DSAs can more effectively handle errors.

7.5.2 Permissible Errors

Table 3 below lists the '88 Directory Standards errors that are possible for particular operations. Implementations shall never use these errors outside the circumstances permitted by the table.

Table 3: Permitted errors by operation

Operation	Attribute Error	Name Error	Security Error	Service Error	Update Error	AbandonFailed
Bind	-	-	IA IC	UA	-	-
Read	NSA	ADP AP NSO IAS	IAR NI IS PR	Any	-	-
Compare	IM IAS NSA	ADP AP NSO IAS	IAR NI IS PR	Any	-	-
List		ADP AP NSO IAS	IAR NI IS PR	Any	-	
Search	IAS	ADP AP NSO IAS	IAR NI IS PR	Any	-	-
Add Entry	CV AVE IAS UAT	ADP AP NSO IAS NV	IAR NI IS PR	Any	AMD EAE OCV NV	-
Remove Entry		ADP AP NSO IAS	IAR NI IS PR	Any	AMD NAN	-
Modify-Entry	AVE CV IAS IM NSA UAT	ADP AP NSO IAS	IAR NI IS PR	Any	OMP OCV	-
Modify-RDN		ADP AP NSO IAS	IAR NI IS PR	Any	AMD NAN NV EAE	-
Abandon	-	-	-	-	-	NSO TL CA

The problem codings used in Table 3 are listed in Table 4.

Table 4: Problem codings

Abandon Failed problems

CA	Cannot abandon
NSO	No such operation
TL	Too late

Attribute Error problems

AVE	Attribute or value already exists
CV	Constraint violation
IAS	Invalid attribute syntax
IM	Inappropriate matching
NSA	No such attribute or value
UAT	Undefined attribute type

Name-Error problems

ADP	Alias dereferencing problem
AP	Alias problem
IAS	Invalid Attribute Syntax
NSO	No such object

Security Error problems

IA	Inappropriate authentication
IAR	Insufficient access rights
IC	Invalid credentials
IS	Invalid signature
NI	No information NOTE. This problem may be used in place of any other Security Error problem.
PR	Protection required

Service Error problems

ALE	Administrative limit exceeded
B	Busy
CR	Chaining required
DE	DIT Error
IR	Invalid reference
LD	Loop detected
OOS	Out of scope
TLE	Time limit exceeded
UA	Unavailable
UAP	Unable to proceed
UCE	Unavailable critical extension
UWP	Unwilling to perform

Update Error problems

AMD	Affects multiple DSAs
EAE	Entry already exists
NAN	Not allowed on non: leaf
NAR	Not allowed on RDN
NV	Naming violation
OCV	Object class violation
OMP	Object class modification prohibited

7.5.3 Errors In Name Resolution

In this clause, rules are given for the continuation of Name Resolution in the face of error situations which occur during both chaining and multicasting (i.e. following Non-specific Subordinate References).

> NOTE. The following is a logical consequence of NSSRs, but is a most important statement, because it extends the validity of the error reporting to general use, rather than in the specialised circumstances of NSSRs.

Since it is unreasonable that DSAs should behave differently depending on the use of NSSRs or otherwise, the rules for error generation shall apply wherever the specific error situation is encountered.

For the purposes of description, Name Resolution proceeds in terms of Operation Performing Cycles. This term describes the part of the procedure described in [ISO/IEC 9594-4 | CCITT X.518] Figures 7-9. An Operation Performing Cycle (see Figure 6 below) takes a name, and results in zero, one or more further cycles occurring; note that alias dereferencing occupies a complete cycle on its own.

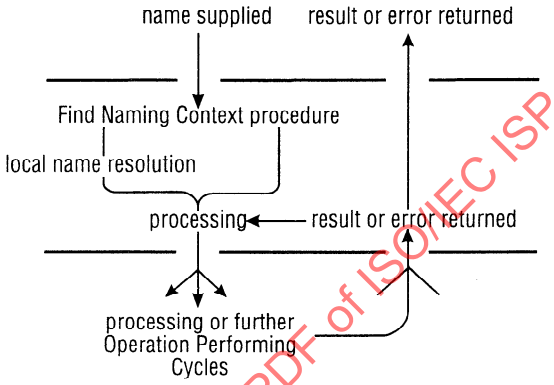

Figure 6: Operation Performing Cycle

An Operation Performing Cycle may take place in the same or in a different DSA to its predecessor, and may result in useful operation processing, or in the return of an error to the Operation Performing Cycle that instigated it. The cycle only results in multiple outputs in the case of the use of NSSRs. (List or Search continuation invoking "List (II)" or Search (II) procedures per [ISO/IEC 9594-4 | CCITT X.518] clauses 18.7.2.1 or 18.7.2.2 does not relate to this situation.) Of course, it is possible for an NSSR to reference a single DSA.

An Operation Performing Cycle that does not use a Non-specific Subordinate Reference will (if successful) usually return to its caller the error or result supplied by the resulting processing or by further Operation Performing Cycles.

In order to accommodate NSSRs and make it possible for them to work consistently, some special rules are required; these will now be described in the following clauses. As noted earlier, these rules apply generally.

7.5.3.1 Errors encountered when following NSSRs

In considering name-resolution in the presence of Non-specific Subordinate References, suppose that a DSA A is attempting to multicast sequentially to DSAs P, Q and R in respect of some operation. If P returns a result or a service error with problem "unable-to-proceed", the situation is (apparently) clear. If a result is returned, A has no need to contact Q and R. With "unable-to-proceed", Q does need to be contacted. But how about other situations?

The primary criterion is: did P manage to progress name-resolution down at least one RDN? If so, P was indeed the correct DSA to continue with name-resolution, and Q and R are not involved and should not be

contacted. Unfortunately, more indeterminate circumstances can arise. Specifically, these are the possible outcomes from A's viewpoint:

A. The operation succeeds

B. It results in a referral

C. It results in an error which indicates that nevertheless name resolution has been successfully completed

D. It results in an error which indicates that the target entry definitely does not exist

E. It results in an error which indicates that the DSA has been able to resolve the next-RDN-to-be-resolved, but it has not been possible to determine whether the object entry does or does not exist

F. It results in an error which indicates that the DSA has been unable to resolve even the next-RDN-to-be-resolved

G. It results in an error for which it is indeterminate whether the DSA is or is not capable of resolving the next-RDN-to-be-resolved on the basis of information stored within it

The semantics of error returns (as clarified in clauses 7.3.3.2.1 to 7.3.3.2.15) can be exploited to identify the situations in which each outcome occurs.

Situations A and B are self-explanatory.

Situation C is the case with the following errors:

"attribute-error" any
"update-error": any

Situation D is the case with the following errors:

name errors: "no-such-object", "alias-problem", "alias-dereferencing-problem", "invalid-attribute-syntax" with number of RDNs in matched name greater or equal to next-RDN-to-be-resolved

Situation E is the case with the following errors:

service-errors: "chaining-required", "out-of-scope"

Situation F is the case with the following errors:

name-error: "invalid-attribute-syntax" with number of RDNs in matched name shorter than next-RDN-to-be-resolved

service-error: "unable-to-proceed"

Situation G is the case for all remaining errors:

reject

operation-timeout

security-problem: any

service-error: "busy", "unavailable", "unwilling-to-perform", "loop-detected", "invalid-reference", "DIT-error", "time-limit-exceeded", "administrative-limit-exceeded", "unavailable-critical-extension"

These lists are based on application of the rules of 7.3.3.2 below.

7.5.3.2 Specific Error Semantics

The term "generated" in the following subclauses shall be taken to mean "generated as a consequence of a locally-detected error situation", as opposed to "relayed having received it from a further DSA to which chaining has taken place".

The term "relay" for a particular DSA shall be taken as meaning to pass back a return from a responding DSA to the DSA's caller, subject only to an overriding situation where a Service-Error "busy" or "unwilling-to-perform" may be required to be passed back.

The term "multicasting" in the following subclauses shall be taken to mean "in the process of a specific DSA carrying out a sequential Non-specific Subordinate Reference procedure".

The expression "containing the next RDN to be resolved" shall be taken as meaning that a DSA holds entry information for the name corresponding to that part of the target object from root down to and including the Nth RDN, where N is the next RDN to be resolved.

The expression "progressing name resolution" in respect of a particular DSA shall mean that the DSA at least contains the next RDN to be resolved.

NOTE. There appear to be a number of circumstances during name resolution when an error can either be generated by a DSA or relayed. In the latter case, name resolution will definitely have progressed; in the former case, this may or may not be the case. In such cases, relaying this error isn't helpful, but the standards leave no option.

7.5.3.2.1 Referral

A DSA (having received a chained operation as a result of an NSSR) shall not supply a referral unless it contains the next RDN to be resolved; the referral could then be generated to follow a reference to a further DSA.

A DSA may relay a referral, or may act upon it.

7.5.3.2.2 Attribute-error

An attribute error shall only be generated when an operation is being applied by a DSA to a specific entry; returning an attribute error shall therefore imply that name resolution has been successful.

A DSA, having received such an error during name resolution, shall relay it.

7.5.3.2.3 Name-Error: "no-such-object"

This error shall only be generated by a DSA when the DSA either determines that the entry does not exist (and is thus held in no DSA), or it does exist, but is inaccessible for security reasons.

A DSA, having received such an error during name resolution, shall relay it.

7.5.3.2.4 Name-Error: "alias-problem" or "alias-dereferencing-problem

This error shall only be generated when the DSA has encountered an alias but an error has subsequently been encountered in following the alias.

A DSA, having received such an error during name resolution, shall relay it.

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

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.

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.

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 but need not relay it.

7.5.3.2.6 Security-Errors

In all cases, it is indeterminate whether or not name resolution was progressed.

A DSA, having received such an error during name resolution, shall relay it.

7.5.3.2.7 Service-Error: "loop-detected", "DIT-error"

A DSA, having received such an error during name resolution, shall relay it.

7.5.3.2.8 Service-Error: "busy", "unavailable", "unwilling-to-perform"

If returned while multicasting to an NSSR, it is permitted as a local option to continue processing the other access points in the NSSR. The "busy", "unavailable" and "unwilling-to-perform" errors may subsequently be returned if not superseded by the response to accessing a subsequent access point.

7.5.3.2.9 Service-Error: "chaining-required"

See clause 12.8.2 d) of [ISO/IEC 9594-3 | CCITT X.511].

7.5.3.2.10 Service-Error: "unable-to-proceed"

A DSA shall generate this error during name resolution when (A) it is responding to an NSSR and (B) it does not hold the next RDN to be resolved and (C) the DSA holds some other subordinate entry of the immediate superior of the next RDN to be resolved. If conditions A and B but not C are satisfied, "invalid-reference" is the correct error-see 7.3.3.2.11 below.

If, when multicasting, a DSA receives this error, name resolution shall be therefore be taken as not having progressed; multicasting shall proceed. This error shall not be returned to the DSA's caller; instead, Name-error no-such-object shall be used. This error shall never be relayed.

NOTE. Here also, there are circumstances when there is no satisfactory error return.

7.5.3.2.11 Service-Error: "invalid-reference"

A DSA (having received a chained operation as a result of an NSSR) shall only generate a Service-Error: "invalid-reference" if it has determined that it does not hold an entry which is the immediate subordinate of the immediate superior of the next RDN to be resolved.

A DSA, having received such an error during name resolution, shall relay a "DIT-error" Service-Error back to its caller.

NOTE. "Invalid-reference" may be handled in the same way as the errors described in clause 7.3.3.2.7 except that the error, if returned, is converted to "DIT-error".

7.5.3.2.12 Service-Error: "time-limit-exceeded", "administrative-limit-exceeded", "unavailable-critical-extension", "out-of-scope"

These errors shall only be generated when name resolution has been progressed. If it has not been possible to carry out name resolution, Service-Error "busy" shall be used instead.

A DSA, having received such an error during name resolution, shall relay it.

7.5.3.2.13 Update-Errors

All such errors shall be taken as indicating that name-resolution has completed.

A DSA, having received such an error during name resolution, shall relay it.

7.5.3.2.14 Reject

A DSA should only generate a ROS reject in the case of a syntactic error; if it receives a ROS reject as a consequence of chaining or multicasting (without having itself identified an error), this may be the result of the chained DSA having done a more complete analysis.

A DSA may therefore relay a reject.

7.5.3.2.15 Operation Timeout

If a DSA times out a chained operation, it should generate a service-error "time-limit-exceeded" or "administrative-limit-exceeded" (see 7.3.3.2.12 above).

7.5.3.3 Other rules

DSAs shall attempt to carry out Name Resolution using NSSRs where possible, subject to local administrative limits. This implies that NSSR handling shall be continued if possible until one of the following outcomes occur:

1. A result is received, or an error is received indicating continuation: name resolution terminates, and the result or error is passed on

OR

2. A Referral is received-the NSSR is considered resolved, and the Referral is pursued instead

OR

3. All DSAs in the NSSR have been tried, each with an outcome that is (a) some other error, or (b) a reject or (c) a time-out: if all the replies are "unable-to-proceed", the Operation Performing Cycle generates a name error "no-such-entry"; in other cases, the "unable-to-proceed" errors are ignored, and a single error from the remainder is selected (rules for such selection are a local matter; see notes on rejects and below)

OR

4. Local administrative, time limits or other limits have been reached-these may be signalled by a suitable service error from the list "busy", "time-limit-exceeded" or "administrative-limit-exceeded"

The outcomes just described may be modified by the following special circumstances:

7.5.3.3.1 Rejects

Since the present DSA has accepted the operation, it may presume that its syntax is correct, and may thus treat the problem as local to the remote DSA (or conceivably as due to an error in ChainingArguments). The response may be handled as if it was an "unavailable" Service Problem, but the DSA may also pass the reject back to the calling Name Resolution Phase.

7.5.3.3.2 Service-Problem "busy"

A DSA may retry an operation that returns this error.

7.5.3.3.3 Time-out

This may be treated as a "busy" Service-problem.

7.6 Operation Pass-Through

7.6.1 Illegal Or 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.

A DSA shall support all attributes that are held within it; i.e. it shall comply with all the rules associated with it as required by [ISO/IEC 9594-2 | X.501], [ISO/IEC 9594-3 | X.511] and the definition of each attribute (e.g. in [ISO/IEC 9594-2 | X.501]).

NOTE. The requirements for the support of attributes are defined in part of ISO/IEC ISP 10615 10616 Common Directory Use (Normal) clause 8.1.

7.6.2 Attribute Values With Multi-Octet ASN.1 Tags

DSAs shall support the pass-through of attribute values which use ASN.1 identification tags of up to 3 octets in length.

NOTE. ISP 11188-1 Basic connection oriented requirements states in clause 8.1.1:

"The maximum value of an ASN.1 tag shall be 16383. Since this is the largest unsigned number that can be represented in 14 bits, the encoding of a tag occupies at most 3 octets."

It is nevertheless permitted for a DSA to pass through ASN.1 elements with tags larger than 16383.

7.6.3 ASN.1 Syntax Checking

A DSA is not obliged to carry out complete ASN.1 syntax checking on an incoming Invoke which is passing through.

For example, it may restrict its analysis to those parts of the operation argument that are required for the purposes of name resolution, unless name resolution is successful.

7.6.4 Matching Names In Trace Information

A DSA 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 matching shall use an algorithm which reliably matches two names having the same primitive content.

7.7 Digital Signatures

DSAs supporting DSP shall accept signed chained-operations and their results intended for other DSAs; but they need not be capable of the evaluation of the signature. If they are capable of evaluating signed operations for local purposes, they shall be capable of evaluating both levels of signature (i.e. at both the operation and chained-operation levels).

DSAs are not obliged to be capable of evaluating digital signatures to be conformant to this part of ISO/IEC ISP 10615.

7.8 Unsupported Attributes in Filter Items

An attribute that is unsupported by the DSA may also be used in search filter-item definitions: in this case, no error shall be reported, but the attribute type or value shall be deemed to be "undefined" for all entries in the DSA (see [ISO/IEC 9594-3 | CCITT X.511] clause 7.8.3.2).

NOTE. The Directory Standards do not define when "undefined" shall be used instead of "false" (the use of "true" is, however, closely defined).

7.9 Extensibility Rules

7.9.1 Reference Type

A DSA receiving an unknown reference type in **ChainingArguments.referenceType** shall regard it as equivalent to a cross reference.

7.9.2 Continuation References

DSAs shall be able to accept and pass through extension elements within continuation references. When required to act on such elements, unknown reference type elements shall be treated as if they were cross references.

7.10 Loop detection/avoidance

7.10.1 In distributed operations

DSAs shall apply at least one of loop detection and avoidance in respect of received chained operations, as described in [ISO/IEC 9594-4 | X.518] clause 18.5

NOTE. Loop detection permits earlier detection of loops in the case where other DSAs do not support neither loop avoidance. For example, consider a looping situation in which the present DSA is A:

A=>B=>C=>A=>B ...

If C has loop avoidance, the loop would stop before the transition C=>A. Otherwise, if A has loop detection, the loop stops after the transition C=>A. Otherwise, if C has loop avoidance, the loop stops before the second transition A=>B. So, as far as A is concerned, loop detection obviates the unnecessary second processing of the operation

7.10.2 In internal processing

DSAs shall detect a situation where looping occurs without the generation of distributed operations, as a consequence of improper use of aliases. They may do this either by detection of the condition that would give rise to such a loop, or by detecting the condition when initiated by an appropriate operation.

NOTE. Such a condition can, for example, occur when an alias indirectly references a point higher in the DIT: P has P' as an aliased object name; Q is an alias subordinate to P' and has Q' as an aliased object name; Q' is superior to P.

Annex A
(normative)
Profile Requirements List

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10615 and the tables in this Annex, this Annex is to take precedence.

A.0. Introduction

This Annex specifies the constraints and characteristics of this part of ISO/IEC ISP 10615 on what shall or may appear in an Implementors' PICS for an implementation conformant to this part of ISO/IEC ISP 10615.

This Annex is based on both the Directory Access Protocol PICS Proforma of Recommendations CCITT X.581 and the Directory System Protocol PICS Proforma of Recommendation X.582. Although the purpose of these PICS Proformas is somewhat different to that of this part of ISO/IEC ISP 10615, and the correspondence is patchy, both are relevant, since this part of ISO/IEC ISP 10615 takes ISO/IEC ISP 10615 parts 2, 3 and 4 as applicable, and these reference X.581 and X.582

Therefore, although both are retained in outline (with avoidance of unnecessary duplication), most of the provisions are marked as "void", meaning either "no new requirements" or "not currently relevant".

A new clause (A.7) is introduced to hold the specific requirements of this part of ISO/IEC ISP 10615.

The terminology of conformance requirements is used as defined in 3.2.

The abbreviations sued in the heading of the tables in this Annex are:

D - conformance requirement as defined in the base standard

P - conformance requirement as defined in this part of ISO/IEC ISP 10615

Profile Requirements List

A.1. General

A.1.1. Identification of PICS

A.1.1.1. Directory Access Protocol (DAP)

(void)

A.1.1.2. Directory System Protocol (DSP)

(void)

A.1.2. Identification of the implementation and/or system

Ref. No.	Question	Response
1	Implementation Name	(void)
2	Version Number	(void)
3	Machine Name	(void)
4	Machine Version Number	(void)
5	Operating System Name	(void)
6	Operating System Version No.	(void)
7	Special Configuration (1)	(void)
8	Does the DSA support DAP?	yes/no
9	Does the DSA support DSP?	yes/no
10	Is the DSA capable of acting as a First-level DSA?	yes/no
11	Is the DSA capable of acting as a Non-First-level DSA?	yes/no
12	Is the DSA capable of acting as a Co-operating DSA (i.e. having knowledge references for other DSAs and the capability to act on them by referrals or by chaining)	yes
13	Does the DSA support cross-references?	yes/no
14	Does the DSA support NSSRs?	yes/no
15	Is the DSA capable of reference from other DMDs?	yes/no
16	Does the DSA support single-alias naming contexts?	yes/no

The following predicates are defined:

p_dap = A.1.2/8

p_dsp = A.1.2/9

p_fl = A.1.2/10

p_nfl = A.1.2/11

p_xr = A.1.2/13

p_nssr = A.1.2/14

p_dmd_ref = A.1.2/15

p_anc = A.1.2/16

A.1.3 Identification of the system supplier and/or test laboratory client

(void)

A.2. Identification Of The Protocol

A.2.1. DAP

NOTE. The following is a normative statement: this clause applies if p_dap.

Ref. No.	Question	Response
1	Title, Reference Number, publication date of the protocol standard	ISO/IEC 9594:1990 Information Technology - Open Systems Interconnection - The Directory Directory Access Protocol
2	Protocol Version Number	**v1988**
3	Implemented Addenda	None
4	Implemented Defect Reports (Ref. No)	See Annex B

A.2.2. DSP

NOTE. The following is a normative statement: this clause applies if and only if p_dsp.

Ref. No.	Question	Response
1	Title, Reference Number, publication date of the protocol standard	ISO/IEC 9594:1990: Information Technology - Open Systems Interconnection - The Directory Directory System Protocol
2	Protocol Version Number	**v1988**
3	Implemented Addenda	None
4	Implemented Defect Reports (Ref. No)	See Annex B

A.3 Global Statement Of Conformance

A.3.1. DSA implementation and/or system

Ref. no	Question	D	P
1	Are all mandatory general capabilities for the DSA implemented?	m	m
2	Are minimum knowledge requirements (X.518) implemented?	m	m
3	Are all mandatory First-level DSA requirements (X.518) implemented?	c Note 1	c Note 1
4	Is Cross Reference implemented?	o	c Note 2
5	Is NSSR (Non-specific Subordinate Reference) implemented?	o	c Note 3
6	Supported Security Level(s) (DAP)	(void)	
7	Is asynchronous (ROSE class 2) mode of operation supported?	(void)	
8	Is the alias mechanism implemented?	o	m (see 6.4)

NOTES

1. if p_fl then m else i
2. if p_xr then m else i
3. if p_nssr then m else i

A.3.2. DUA implementation and/or system

(void)

A.3.3 General Capabilities

(void)

A.4. Capabilities and Options

This part of the IPRL identifies the supported application context, the PDUs and operations. Finally, the operation arguments and PDU parameters are identified.

A.4.1. Supported application context - DAP

This clause applies only if p_dap.

The only application context supported by this clause of the is Directory Access application context. See also reference to Directory System Application Context below.

This part of ISO/IEC ISP 10615 creates no special requirements for protocol or schema.

A.4.2. Operations - DAP

This clause applies only if p_dap.

This part of ISO/IEC ISP 10615 creates no special requirements for DAP operations.

A.4.3. Protocol elements - DAP

This clause applies only if p_dap.

This part of ISO/IEC ISP 10615 creates no special requirements for DAP protocol elements.

A.4.4. Directory schema - DAP

This clause applies only if p_dap.

This part of ISO/IEC ISP 10615 creates no special requirements for the schema.

A.4.5. Operations - DSP

This clause applies only if p_dsp. This part of ISO/IEC ISP 10615 defines no special requirements for these operations.

A.4.5.1. DSABind Protocol Elements

A.4.5.1.1. DSABind Arguments

(void)

A.4.5.1.2. DSABind Result

(void)

A.4.5.1.3. DSABind Error

(void)

A.4.5.2. DSAUnbind Elements

(void)

A.5. Other information

(void)

A.6. Multi-Layer Dependencies

(void)

A.7. Requirements particular to this part of ISO/IEC ISP 10615

A.7.1. Static Capabilities

Ref. no	Capability	Reference	P	Notes
1	Support of Superior Reference	6.1.1	m	Mandatory
2	Support of Subordinate Reference	6.1.1	m	
3	Support of Cross-reference	6.1.1	c	if p_xr then m else i
4	Support of Non-specific Subordinate Reference	6.1.1	c	if p_nssr then m else i
5	Support of root context by holding and replicating first-level information	6.1.2.1	c	if p_fl then m else i

Ref. no	Capability	Reference	P	Notes
Ref. no	Capability	Reference	P	Notes
6	Support of naming context immediately beneath root	6.1.2.2	c	if p_fl then m else i
7	Support of naming contexts with multiple subordinate references	6.1.2.3	m	
8	Support of naming contexts with multiple Non-specific Subordinate References	6.1.2.4	c	if p_nssr then m else i
9	Support of return-of-cross-references as requestor	6.1.2.5	o	
10	Support of return-of-cross-references as supplier	6.1.2.5	o	
11	Creation, updating and deletion of Naming Contexts	6.2.1.1	m	
12	Creation, updating and deletion of Superior Reference	6.2.1.2	m	Mandatory
13	Creation, updating and deletion of Subordinate References	6.2.1.3	m	
14	Correction of Access Point information for a knowledge reference	6.2.1.4	m	
15	Creation, updating and deletion of cross references	6.2.2.1	c	if p_xr then m else i
16	Creation, updating and deletion of Non-specific Subordinate References	6.2.2.2	c	if p_nssr then m else i
19	Creation and administration of a naming context comprising a single alias	6.2.2.3	c	if p_anc then m else i
19	Support DirectorySystemAC as responder	6.3	c	if p_dmd_ref then m else i
20	Support referral mode	6.3.1	m	
21	Support of remote authentication (e.g. by chained read or chained compare)	6.3.2	c	if p_rem_auth then m else i
22	Support of aliases pointing to other DSAs	6.5	m	
23	Support of DSA-bind using simple unprotected authentication with password	6.6.1	m	

A.7.2. Procedures

Ref. no	Procedure	Reference	m	Notes
1	Support correct handling of name with first arc not within the root context		c	if p_fl then m else i
2	Support of continuation reference during list or search	7.2	m	
3	Use of Subordinate references: ditError	7.1.2	m	
4	Support of operation integrity	7.3	m	
5	Use of "unavailable" service error with lost associations	7.4.1	m	
6	Restriction of errors to permissible errors only	7.5.2	m	
7	Handling of errors in name resolution	7.5.3	m	Error procedures apply whether or not NSSRs are used.
8	Passing on illegal or unsupported attributes	7.6.1	m	
9	Passing on ASN.1 tags up to 3 octets in length	7.6.2	m	
10	Matching names in TraceInformation	7.6.4	m	
11	Acceptance of signed operations and results	7.7	m	
12	Use of "undefined" in filter handling	7.8	m	
13	Handling unknown reference types in chainingArguments	7.9.1	m	
14	Handling extension elements in continuation references	7.9.3	m	
15	Loop detection/avoidance in distributed operations	7.10.1	m	
16	Loop detection/avoidance in internal processing	7.10.2	m	

Annex B
(normative)
Amendments and corrigenda

International standards are subject to constant review and revision by ISO/IEC Technical Committee concerned and by CCITT. The following amendments and corrigenda are approved by ISO/IEC JTC1 and by CCITT, but at the date of publication of this part of ISO/IEC ISP 10615 they were not yet incorporated in the text of the corresponding base standards as referenced in Clause 2. The amendments and corrigenda as listed below are considered as normative references in this part of ISO/IEC ISP 10615.

ISO/IEC 9594-2:1988/Cor.1	resolving defects 006, 021
ISO/IEC 9594-2:1988/Cor.2	resolving defects 036, 037
ISO/IEC 9594-3:1988/Cor.1	resolving defects 001, 007, 012, 014, 020, 032
ISO/IEC 9594-3:1988/Cor.2	resolving defects 038, 042
ISO/IEC 9594-3:1988/Cor.3	resolving defect 052
ISO/IEC 9594-3:1988/Cor.4	resolving defects 041, 054, 060, 063, 068, 069
ISO/IEC 9594-4:1988/Cor.1	resolving defects 004, 010, 011, 012, 013, 022, 023, 025, 026, 027, 029
ISO/IEC 9594-4:1988/Cor.2	resolving defects 002, 034, 048, 050, 059
ISO/IEC 9594-4:1988/Cor.3	resolving defects 024, 062, 065, 066
ISO/IEC 9594-5:1988/Cor.1	resolving defect 052
ISO/IEC 9594-7:1988/Cor.1	resolving defect 005
ISO/IEC 9594-7:1988/Cor.2	resolving defect 055
ISO/IEC 9594-8:1988/Cor.1	resolving defects 009, 015, 016, 019, 031

Annex C
(informative)
Error Handling for the Directory

C.1. Introduction

This Annex presents error conditions that may be encountered in DSAs, and maps them onto Directory errors, depending on the circumstance in which they are encountered.

The Annex is intended to clarify the base standards and to assist implementors in determining which errors to use under a range of circumstances.

There are normative requirements made in the body of this part of ISO/IEC ISP 10615 (clause 7.3) which are to be implemented in the event of conflict between the recommendations of this Annex and the normative part of the part of ISO/IEC ISP 10615.

C.2. Mappings

Although the Directory standards define the semantics of return-error protocol data units, the mapping of particular error conditions to the defined protocol is not always clear.

This profile provides a recommended mapping of error situations which may be encountered, to ROSE Rejects, or to the errors provided in the DAP and DSP protocols by the Directory Documents.

Error situations are defined by the combination of:

Symptom-that is, the manner in which the error was detected (this may occur in several situations)

Situation-that is, the circumstance or phase during which the error was detected.

For each such combination, error-handling recommendations are provided.

C.3. Symptoms

This subsection describes a set of symptoms (not necessarily exhaustive). Each is identified by a title for reference later in the section; this title is not intended to imply any particular usage in a particular implementation.

E_ACCESS

The initiator has insufficient access rights to carry out this operation.

E_ADMIN_LIMIT

The Directory has reached some limit set by an administrative authority, and no partial results are available to return to the user. Examples of administrative limits are:

Too many RDNs in a DN

Too many changes in a modify-entry

Too many attributes in a list of attributes or attribute types

Too many elements in a filter

E_ALIAS_DEREF

An alias has been encountered while a previous alias was being dereferenced, or a name contained an alias plus one or more additional RDNs when the **dontDereferenceAliases** service control was being used, or the name supplied in an operation that precluded alias dereferencing contained an alias plus one or more additional RDNs.

E_ALIAS_LOOP

During a whole-subtree search operation, an alias has been encountered which would lead to a loop (i.e. the alias points to an entry which is superior to entries which have already been evaluated in carrying out the search).

E_ALIAS_PROBLEM

An Alias has been encountered, but the entry to which it points does not exist.

E_ARG_BOUNDS

The argument does not comply with pragmatic constraints (defined locally or by ISPs).

E_ARG_SYNTAX

An operation argument either has incorrect ASN.1 syntax, or it has correct ASN.1 syntax but it does not conform with the syntax as defined in the Directory Documents.

NOTES

1. Within **BindArgument**, additional elements are permitted, to allow future extensions, and do not create an error situation.
2. Errors within attribute values are not included in this codification (see E_ATT_SYNTAX).

E_ARG_VIOL

An operation argument has correct syntax, but it violates additional rules and constraints laid down by the Directory Documents (such as the use of a **Priority** integer value whose meaning is undefined).

NOTES.

1. Within a Relative Distinguished Name, having two AVAs of the same attribute type is an error which is covered by E_DN, and not by E_ARG_VIOL.
2. Errors within attribute values are not included in this codification (see E_ATT_SYNTAX).

E_ATT_BOUNDS

An attribute value does not comply with bounds specified either by the Directory Documents, or by ISPs.

E_ATT_OR_VALUE_EXISTS

Within an entry, an attribute or attribute value already exists, causing an error situation.

E_ATT_VALUE

Either an attribute value either has incorrect ASN.1 syntax, or, although of correct ASN.1 syntax, does not comply with the ASN.1 syntax defined by the attribute type, or is not compliant with other rules (e.g. a non-ISO 3166 country name encoding).

Among these rules could be a rule that a distinguished name is not permitted within an attribute-value assertion within a value of distinguished-name-syntax.

E_AUTHENTICATION

The authentication offered does not match that required by the object being authenticated.

E_BUSY

The DSA is unable to handle this operation at this time (but it may be able to do so after a short while).

E_CHAIN

The DSA must use chaining to carry out this operation, but is prohibited from doing so by Service Controls.

E_CREDENTIALS

The credentials offered do not match those of the object with which authentication is taking place.

E_DBE

An inconsistency has been detected in the DSA's data base, which may be localised to a particular entry or set of entries.

E_DN

A DN contains an RDN with two AVAs of the same attribute type, or contains an RDN with zero AVAs.

E_DSA

A DSA to which chaining is taking place is unable to respond.

E_ENTRY_EXISTS

An entry of the given name already exists, causing an error.

E_EXTENSION

The DSA was unable to satisfy a request because one or more critical extensions were not available.

E_ILLEGAL_ROOT_OBJECT

Root's DN has been supplied as the object of a Read, Compare, AddEntry, RemoveEntry, ModifyEntry, ModifyRDN, or as the BaseObject of a single-level search.

E_ILLEGAL_ROOT_VALUE

Root's DN has been supplied illegally as an attribute value (e.g. as an **AliasedObjectName**)

E_LOOP

The Directory is unable to accomplish the request due to an internal loop.

E_MATCH

The attribute specified does not support the required matching capability.

E_MISSING_OBJECT_CLASS

When creating an entry, the entry does not possess an object class.

E_MULTI_DSA

The operation is an update operation which affects other DSAs.

E_NAMING_VIOLATION

The name of the new or modified entry is incompatible with its object class or structure-rule.

E_NO_SUCH_ATT

The specified attribute has not been found.

E_NO_SUCH_OBJECT

The specified entry has not been found.

E_NO_SUCH_VALUE

The specified attribute value has not been found.

E_NON_LEAF_OPERATION

The operation being attempted is illegal except on a leaf.

E_NONNAMING_ATTRIBUTE

In either an add-entry or a modify-RDN operation, an attribute is included in the last RDN that is not a valid naming attribute according to the DIT structure rules locally applicable

E_NOT_SINGLE_VALUED

An attribute, registered as single-valued, is found at the conclusion of a modify operation (add-entry, modify-entry or modify-RDN) to possess more than one value. Such an error would occur, for example, when a second value has been added to the single-valued country-name attribute.

This error would not occur when a second value has been added to such an attribute, followed by removal of a value, all within the same modify operation. This transient situation should be tolerated by implementations, since the attribute conforms to requirements at the end of the operation. (A similar situation occurs when the first and only value is removed and a second value is subsequently added within a single modify operation; although the attribute at one stage of the processing is left with no values, at the end of the operation it possesses at least one value, as required. this transient situation should also be tolerated by implementations.) See also under E_ZERO_VALUES.

E_OBJECT_CLASS_MOD

An (illegal) attempt has been made to alter or remove an object class attribute.

E_OBJECT_CLASS_VIOL

There is a schema violation (e.g. missing mandatory attribute, or non-allowed attribute present).

E_REFERENCE

An erroneous reference has been detected (e.g. DSA cannot handle name even as far as the number of RDNs that have already been resolved).

E_REM_NAMING_ATT

An attempt has been made in a modify entry to remove a naming attribute or the distinguished value

E_SCOPE

No referrals were available within the requested scope.

E_SYSTEM_PERM

A serious and permanent software or system error has been detected which prevents completion of the operation.

E_SYSTEM_TEMP

A serious but temporary software or system error has been detected which prevents completion of the operation.

E_TIMEOUT

The operation has not completed within the allotted time.

E_UNABLE_TO_COMPLETE

The DSA is unable to complete this operation, or others like it. (This applies particularly to search.)

E_UNABLE_TO_PROCEED

The DSA cannot satisfy the operation after receiving it on the basis of a valid Non-specific Subordinate Reference.

E_UNDEFINED_ATT

A locally unsupported attribute has been encountered.

E_UNSUPPORTED_OC

The object class of the entry is not supported as a valid object class for entries within this DSA.

E_VERSION

An unexpected version has been found in Bind.

E_ZERO_VALUES

An attribute is found at the conclusion of a modify operation (add-entry or modify-entry) to possess no value at all. Such an error would occur, for example, when a single value is removed by a modify-entry operation.

This error would not occur when a single value is removed for an attribute, followed by addition of a value for the same attribute, all within the same modify operation. This transient situation should be tolerated by implementations, since the attribute conforms to requirements at the end of the operation. (See also under E_NOT_SINGLE_VALUED.)

NOTE. The result of a read operation may contain attributes without values as a consequence of access controls on the values that might otherwise have been returned. This situation is not related to the E_ZERO_VALUES error condition.

C.4. Situations

The following situations are recognised within which particular symptoms may give rise to distinct error actions:

BIND-LOCAL

A bind is being attempted; either the entry named is (or should be) within a local naming context, or name resolution is being carried out on the part of the name that is known locally.

BIND-REMOTE

A bind is being attempted, and the entry named is not within a local naming context; remote validation of credentials is being carried out.

NAME-RESOLUTION

Name resolution is being carried out.

ADD-ENTRY-NAME-RESOLUTION

During an add entry operation, name resolution has been successfully accomplished on the superior object, and is now being carried out to determine whether the new entry already exists. (If it does, there is an error.)

ADD-ENTRY

The entry is being generated by an add-entry operation.

MODIFY-ENTRY

The entry is being modified by a modify-entry operation.

MODIFY-RDN

The RDN is being modified by a modify (R)DN operation.

REMOVE-ENTRY

The entry is being removed by a remove-entry operation.

READ

The entry is being read by a read operation.

COMPARE

A Compare operation is being carried out on the entry.

LIST

A List operation is being carried out on the entry.

SEARCH-FILTER

A Search operation is being carried out; the filter is being evaluated or acted upon.

SEARCH-ENTRY

A Search operation is being carried out; the required entry information is being evaluated or acted upon.

ABANDON

An Abandon operation is being carried out.

TRACE-EVALUATION

The trace element is being evaluated for loops.

The situations imply models of procedure for certain circumstances:

Bind (Figure C-1)
Normal operation evaluation (Figure C-2)
Add-entry operation evaluation (Figure C-3)
Modify-RDN operation evaluation (Figure C-4)

These models are presented in the form of procedure diagrams.

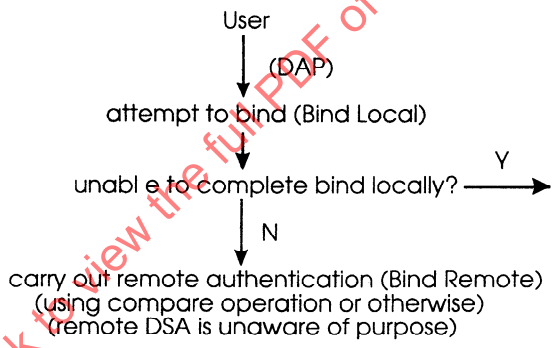

Figure C-1: Bind

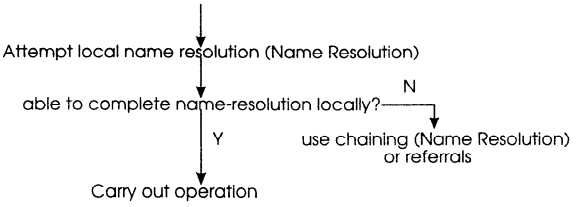

Figure C-2: Normal operation evaluation
(not add-entry or modify-RDN)

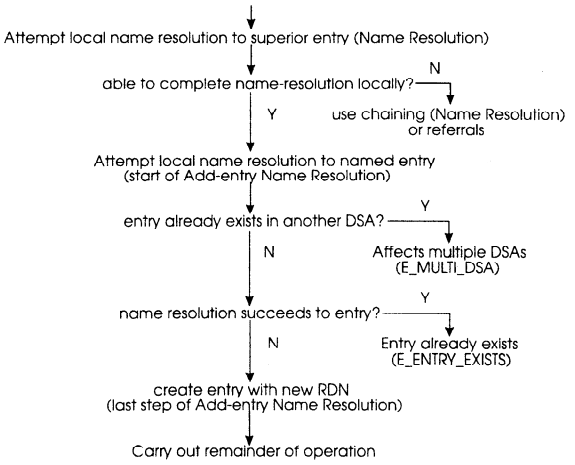

Figure C-3: Add-entry operation evaluation

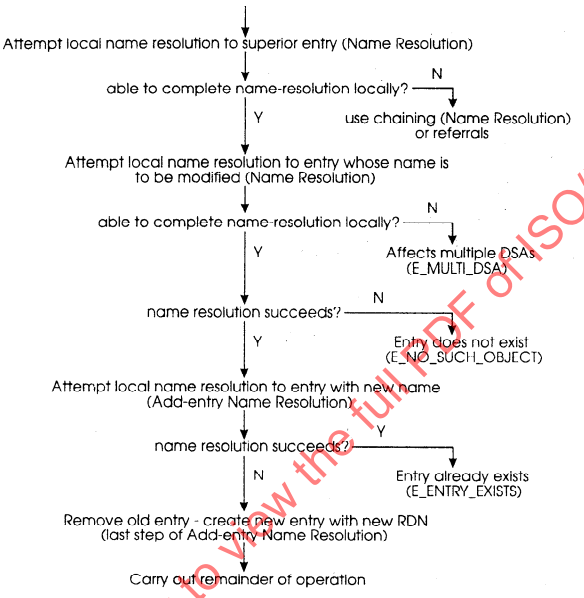

Figure C-4: Modify-RDN operation evaluation

C.5. Error Actions

In the following tables, the recommended actions are identified for all the error symptoms in each situation in which it may be encountered.

The notation is as follows:

Rej-A Reject operation is generated, with problem mistyped-argument.

Ab.ppp.-Abandon Failed Error is generated. ppp may take values codified as follows:

CA-Cannot abandon
NSO-No such operation
TL-Too late

A.ppp-Attribute Error is generated. ppp may take values:

AVE-Attribute or value already exists
CV-Constraint violation
IAS-Invalid attribute syntax

IM-Inappropriate matching
NSA-No such attribute or value
UAT-Undefined attribute type

N.ppp-NameError is generated. ppp may take values:

ADP-Alias dereferencing problem
AP-Alias problem
IAS-Invalid Attribute Syntax
NSO-No such object

SC.ppp-Security Error is generated. ppp may take values:

IA-Inappropriate authentication
IAR-Insufficient access rights
IC-Invalid credentials
IS-Invalid signature
NI-No information
PR-Protection required

NOTE. SC.NI may be used in place of any other Security Error.

S.ppp-Service Error is generated. ppp may take values:

ALE-Administrative limit exceeded
B-Busy
CR-Chaining required
DE-DIT Error
IR-Invalid reference
LD-Loop detected
OOS-Out of scope
TLE-Time limit exceeded
UA-Unavailable
UAP-Unable to proceed
UCE-Unavailable critical extension
UWP-Unwilling to perform

U.ppp-Update Error is generated. ppp may take values:

AMD-Affects multiple DSAs
EAE-Entry already exists
NAN-Not allowed on non-leaf
NAR-Not allowed on RDN
NV-Naming violation
OCV-Object class violation
OMP-Object class modification prohibited

NOTE. U.NAR is used when an attempt is made to remove a naming attribute.

In addition, bracketed numerals give references to the notes that follow

Table C-1 Error Mappings (part 1).

	Bind Local	Bind Remote	Name Resolution	AddEntry Name Resol'n	Add-Entry	Modify Entry	Trace Evaluation	ModifyRDN
E_ACCESS	-	-	SC.IAR (17)	SC.IAR (17)	SC.IAR (17)	SC.IAR (17)	-	SC.IAR
E_ADMIN_LIMIT	-	S.UA	S.ALE	-	S.ALE	S.ALE	-	-
E_ALIAS_DEREF (8)	SC.IC	SC.IC	N.ADP	-	-	-	-	-
E_ALIAS_LOOP	-	-	-	-	-	-	-	-
E_ALIAS_PROBLEM (8)	SC.IC	SC.IC	N.AP	-	-	-	-	-
E_ARG_BOUNDS	(9)	(7)	S.UWP (11)	S.UWP (11)	S.UWP (11)	S.UWP (11)	-	S.UWP (11)
E_ARG_SYNTAX	(1)	(1)	Rej	Rej	Rej	Rej	Rej	Rej

	Bind Local	Bind Remote	Name Resolution	AddEntry Name Resol'n	Add-Entry	Modify Entry	Trace Evaluation	ModifyRDN
E_ARG_VIOL	(1)	(1)	Rej	Rej	Rej	Rej	Rej	Rej
E_ATT_BOUNDS	SC.IC	(7)	N.NSO (16)	(7)	A.CV	A.CV	(7)	U.NV
E_ATT_OR_VALUE_ EXISTS	-	-	-	-	A.AVE	A.AVE	-	-
E_ATT_VALUE	SC.IC	(28)	N.NSO (16)	N.IAS (29)	A.IAS	A.IAS	(7)	U.NV
E_AUTHENTICATION	SC.IA	SC.IA	-	-	-	-	-	-
E_BUSY	S.UA	S.UA	S.B	S.B	S.B	S.B	-	S.B
E_CHAIN	-	-	S.CR	-	-	-	-	-
E_CREDENTIALS	SC.IC	SC.IC	-	-	-	-	-	-
E_DBE	S.UA	-	S.UA	S.UA	S.UA	S.UA	-	S.UA
E_DN	SC.IC	SC.IC	N.NSO	U.NV	-	-	-	U.NV
E_DSA	-	S.UA	S.UA (19)	S.UA (20)	-	-	-	-
E_ENTRY_EXISTS	-	-	-	U.EAE	-	-	-	U.EAE
E_EXTENSION	-	-	S.UCE (21)	S.UCE (21)	S.UCE	S.UCE	-	S.UCE
E_ILLEGAL_ROOT_ OBJECT	SC.IC (23)	SC.IC	N.NSO (23)	(24)	N.NSO	N.NSO	-	(24)
E_ILLEGAL_ROOT_ VALUE	SC.IC	SC.IC (7)	N.IAS (26)	N.IAS (26)	A.IAS	A.IAS	(7)	N.IAS (26)
E_LOOP	-	S.UA	S.LD	-	-		-	-
E_MATCH	SC.IC	SC.IC	N.NSO	U.NV	-	A.IM	(7)	U.NV
E_MISSING_OBJECT_ CLASS	-	-	-	-	U.OCV	U.OMP	-	-
E_MULTI_DSA	-	-	U.AMD (31)	U.AMD		-	-	U.AMD
E_NAMING_ VIOLATION	-	-	-	U.NV	-	-	-	U.NV
E_NO_SUCH_ATT	-	-	-	-	-	A.NSA	-	-
E_NO_SUCH_OBJECT	SC.IC	SC.IC	N.NSO	-	-	-	-	-
E_NO_SUCH_VALUE	-	-	-	-	-	A.NSA	-	-
E_NON_LEAF_ OPERATION	-	-	-	-	-	-	-	U.NAN
E_NONNAMING_ ATTRIBUTE	-	-	-	U.NV	-	-	-	(34)
E_NOT_SINGLE_ VALUED	-	-	-	-	A.CV	A.CV	-	U.NV
E_OBJECT_CLASS_ MOD	-	-	-	-	-	U.OMP	-	-
E_OBJECT_CLASS_ VIOL	-	-	-	-	U.OCV	U.OCV	-	U.OCV
E_REFERENCE	-	S.UA	S.IR (33)	-	-	-	-	-
E_REM_NAMING_ATT	-	-	-	-	-	U.NAR	-	-
E_SCOPE	-	-	(22)	-	-	-	-	-
E_SYSTEM_PERM	S.UA	-	S.UWP	S.UWP	S.UWP	S.UWP	S.UWP	S.UWP
E_SYSTEM_TEMP	S.UA	-	S.UA	S.UA	S.UA	S.UA	S.UA	S.UA
E_TIMEOUT	S.UA	(10)	S.TLE	S.TLE	S.TLE	S.TLE	-	S.TLE
E_UNABLE_TO_ COMPLETE	-	S.UA	-	-	-	-	-	-
E_UNABLE_TO_ PROCEED	-	(2)	(2)	-	-	-	-	-
E_UNDEFINED_ATT	SC.IC	-	(3)	U.NV	A.UAT	A.UAT	(7)	U.NV
E_UNSUPPORTED_OC	-	-	-	-	U.OCV	-	-	-
E_VERSION	S.UA	-	-	-	-	-	-	-
E_ZERO_VALUES	-	-	-	-	A.CV	A.CV	-	(12)