INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 15125-4

First edition
1998-11-01

Information technology — International Standardized Profiles ADYnn — OSI Directory —

Part 4:
ADY22 — DSA support of Distributed Operations

Technologies de l'information — Profils normalisés internationaux ADYnn — Annuaire OSI —

Partie 4: ADY22 — Support DSA d'opérations distribuées

Reference number
ISO/IEC ISP 15125-4:1998(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 15125-4 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 15125 consists of the following parts, under the general title *Information technology — International Standardized Profiles ADYnn — OSI Directory*:

— *Part 1–ADY11: DUA support of Directory Access Protocol*

— *Part 2–ADY12: DUA support of Distributed Operations*

— *Part 3–ADY21: DSA support of Directory Access*

— *Part 4–ADY22: DSA support of Distributed Operations*

— *Part 5–ADY41: DUA Authentication as DAP initiator*

— *Part 6–ADY42: DSA Authentication as DAP responder*

— *Part 7–ADY43: DSA to DSA Authentication*

— *Part 8–ADY44: DSA Simple Access Control*

— *Part 9–ADY45: DSA Basic Access Control*

— *Part 10–ADY51: Shadowing using ROSE*

— *Part 11–ADY52: Shadowing using RTSE*

— *Part 12–ADY53: Shadowing subset*

— *Part 13–ADY61: Administrative areas*

— *Part 14–ADY62: Establishment and utilisation of shadowing agreements*

— *Part 15–ADY63: Schema administration and publication*

— *Part 16–ADY71: Shadowing Operational Binding*

— *Part 17–ADY72: Hierarchical Operational Binding*

— *Part 18–ADY73: Non-specific Hierarchical Operational Binding*

Annexes A and B form an integral part of this part of ISO/IEC ISP 15125. Annex C is for information only.

Introduction

The concept and structure of International Standardized Profiles for Information Systems are laid down in 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 part of ISO/IEC ISP 15125 specifies application profile ADY22 as defined in the Technical Report ISO/IEC TR 10000-2.

This part of ISO/IEC ISP 15125 is one of a set of International Standardized Profiles relating to the Directory (see TR 10000-2) for the '93 standards.

This part of ISO/IEC ISP 15125 profiles the behaviour of a DSA regarding the operation of the Directory System Protocol (DSP) when communicating with another DSA, and it defines the co-ordination of a DSA communication across several associations to perform a particular distributed operation.

ISO/IEC ISP 15125 is defined within the context of Functional Standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The concept of Functional Standardization is one part of the overall field of Information technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests and test methods. ISPs are produced not simply to "legitimise" a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realisation of this goal.

The text of this part of ISO/IEC ISP 15125 was developed in close co-operation among the Directory Expert Groups of the three International OSI Workshops:

- OSE Implementors Workshop (OIW)
- The European Workshop for Open Systems (EWOS) and
- The OSI Asia-Oceania Workshop (AOW).

This part of ISO/IEC ISP 15125 is harmonised among these three Workshops and it was finally ratified by the Workshops' plenary assemblies.

Information technology — International Standardized Profiles ADYnn — OSI Directory — Part 4: ADY22 — DSA support of Distributed Operations

1 Scope

1.1 General

This part of ISO/IEC ISP 15125 profiles the behaviour of a DSA regarding the operation of the Directory System Protocol (DSP) when communicating with another DSA, as an invoker, as a performer, or both. It also profiles the co-ordination of a DSA communication across several associations to perform a particular distributed operation. It also covers the behaviour of DSAs when acting in accordance with the rules of Distributed Operations (although, in this case, the interaction can be by means of returning referrals or continuation references to DUAs using the DAP protocol).

The objective of this part of ISO/IEC ISP 15125 is to define capabilities and constraints on support for DSP by DSAs so that DSAs will be able to interwork within the Directory.

It therefore profiles the following:

- DSAs as DSP invokers in terms of both protocol and functionality
- DSAs as DSP performers in terms of both protocol and functionality
- DSAs as users over (DAP or DSP) of Referrals and Continuation references
- DSAs as users of HOBS (Hierarchical Operational Bindings) and of Shadow Operational Bindings in so far as they affect distributed operations using DSP

Conformance to DOP (Directory Operational Protocol) is *outside* the scope of this part of ISO/IEC ISP 15125.

The objective of this part of ISO/IEC ISP 15125 is to ensure that DSAs will be able to interwork within the Directory in two respects:

- Correct protocol behaviour
- Correct behaviour in respect of the role that each DSA has to play in respect of Distributed Operations

Factors outside the scope of this part of ISO/IEC ISP 15125 include, but are not limited to:

- DIT structure
- The techniques of authentication more rigorous than simple authentication with passwords

DSAs that do not support the distributed Directory are outside the scope of this part of ISO/IEC ISP 15125.

1.2 Position Within the Taxonomy

This part of ISO/IEC ISP 15125 is identified in ISO/IEC TR 10000-2 as "ADY22–DSA support of Distributed Operations".

It may be combined with other parts of ISO/IEC ISP 15125, or with ISO/IEC ISP 15126-1 specifying the normal use of the directory, and with T-Profiles specifying the OSI connection-mode transport service.[1]

1.3 Scenario

The model used is described in Overview of Concepts, Models, and Services in [ISO/IEC 9594-1 : 1995 | ITU-T Rec. X.500 (1993)]. The specifications of this part of ISO/IEC ISP 15125 apply to both the invoker and the performer roles of DSP, and also to the use of referrals and continuation references over DAP. All protocol aspects of DAP, however, are profiled by ISO/IEC ISP 15125-3.

[1] T-Profiles are relevant to protocol-information and its handling (see 8.14)

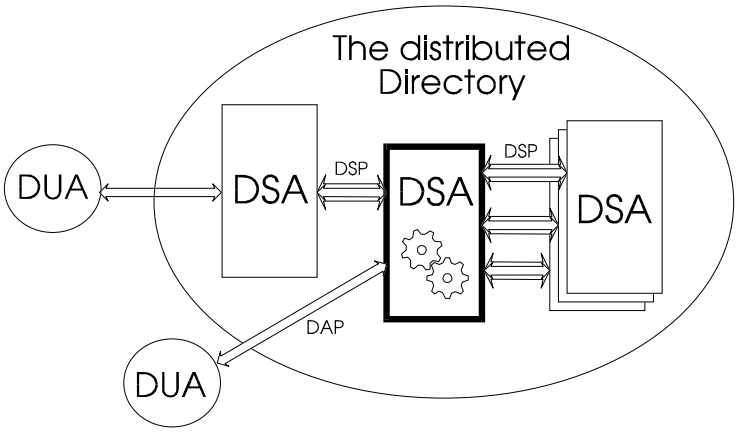

Figure 1 — DSA support of distributed operations

A DSA handles incoming DAP and DSP protocols, and creates chained and multi-chained operations in accordance with defined procedures.

2 Normative references

The following documents contain provisions which, through references in this text, constitute provisions of this part of ISO/IEC ISP 15125. 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 15125 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.

Amendments and corrigenda to the base standards are referenced: see Annex B for a complete list of these documents which are used in this part of ISO/IEC ISP 15125.

2.1 Paired ITU-T Recommendations | International Standards equivalent in technical content

[ISO/IEC 9594-1 : 1995 | ITU-T Rec. X.500 (1993)], *Information technology — Open Systems Interconnection — The Directory: Overview of concepts, models, and services*.

[ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)], *Information technology — Open Systems Interconnection — The Directory: Models*.

[ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)], *Information technology — Open Systems Interconnection — The Directory: Abstract service definition*.

[ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)], *Information technology — Open Systems Interconnection — The Directory: Procedures for distributed operations.*

[ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)], *Information technology — Open Systems Interconnection — The Directory: Protocol specifications*.

[ISO/IEC 9594-6 : 1995 | ITU-T Rec. X.520 (1993)], *Information technology — Open Systems Interconnection — The Directory: Selected attribute types*.

[ISO/IEC 9594-7 : 1995 | ITU-T Rec. X.521 (1993)], *Information technology — Open Systems Interconnection — The Directory: Selected object classes*.

[ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)], *Information technology — Open Systems Interconnection — The Directory: Authentication framework.*

[ISO/IEC 8824-1 : 1995 | ITU-T Rec. X.680 (1994)], *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

[ISO/IEC 8824-2 : 1995 | ITU-T Rec. X.681 (1994)], *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification.*

[ISO/IEC 8824-3 : 1995 | ITU-T Rec. X.682 (1994)], *Information technology — Abstract Syntax Notation One (ASN.1): Constraint specification.*

[ISO/IEC 8824-4 : 1995 | ITU-T Rec. X.683 (1994)], *Information technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

[ISO/IEC 8825-1 : 1995 | ITU-T Rec. X.690 (1994)], *Information technology — Open Systems Interconnection — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER).*

[ISO/IEC 13712-1 : 1995 | ITU-T Rec. X.880 (1994)], *Information technology — Remote Operations: Concepts, models, and notation.*

[ISO/IEC 13712-2 : 1995 | ITU-T Rec. X.881 (1994)], *Information technology — Remote Operations: OSI realizations — Remote Operations Service Element (ROSE) service definition.*

[ISO/IEC 13712-3 : 1995 | ITU-T Rec. X.882 (1994)], *Information technology — Remote Operations: OSI realizations — Remote Operations Service Element (ROSE) protocol specification.*

2.2 Normative Amendments and Technical Corrigenda

In accordance with ISO/IEC TR 10000-1 subclause 6.3.2 c), attention is drawn to normative Amendments and Technical Corrigenda affecting the Directory Standards documents ISO/IEC 9594:1995 and the ITU-T X.500:1993 recommendations.

It should be noted that references made to these standards are almost always invalid if taken as references to the '88 standards.

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.

The following subset of these have been identified as particularly relevant to this part of ISO/IEC ISP 15125:

- Technical Corrigendum 1 to Recommendation X.501 (1993) | ISO/IEC 9594-2:1995 (addressing DRs 9594/088, 089, 090, 091, 102, 125)
- Draft Technical Corrigendum 2 to Recommendation X.501 (1993) | ISO/IEC 9594-2:1995 (addressing DRs 9594/134,136)
- Technical Corrigendum 1 to Recommendation X.511 (1993) | ISO/IEC 9594-3:1995 (addressing DR 9594/085)
- Draft Technical Corrigendum 2 to Recommendation X.511 (1993)| ISO/IEC 9594-3:1995 (addressing Defect Reports 9594/119,133)
- Technical Corrigendum 1 to Recommendation X.518 (1993) | ISO/IEC 9594-4:1995 (addressing DRs 9594/094, 106, 108, 109, 111, 112, 113, 114, 115)
- Draft Technical Corrigendum 2 to Recommendation X.518 (1993) | ISO/IEC 9594-4:1995 (addressing DRs 9594/116, 117, 118, 119, 120, 121, 130)
- Technical Corrigendum 1 to Recommendation X.519 (1993) | ISO/IEC 9594-5:1995 (addressing DRs 9594/075, 124)
- Draft (?) Technical Corrigendum 1 to Recommendation X.520 (1993) | ISO/IEC 9594-6:1995 (addressing DRs 9594/076, 122, 127)
- Technical Corrigendum 1 to Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 (addressing DR 9594/128)
- Draft (?) Technical Corrigendum 2 to Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 (addressing DRs 9594/077, 078, 083, 084)
- Draft (?) Technical Corrigendum 3 to Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 (addressing DRs 9594/080,092,100)
- Draft (?) Technical Corrigendum 1 to Recommendation X.525 (1993) | ISO/IEC 9594-9:1995 (addressing DRs 9594/097, 099, 123)
- Draft (?) Technical Corrigendum 2 to Recommendation X.525 (1993) | ISO/IEC 9594-9:1995 (addressing DR 9594/132)

2.3 Additional normative references

- [ISO/IEC 9594-8 : 1990 | CCITT Rec. X.509 (1988)], *Information technology — Open Systems Interconnection — The Directory: Authentication framework.*[2]
- ISO/IEC 13248-2[3] *— Information technology — Open Systems Interconnection — Protocol Implementation Conformance Statement (PICS) Proforma — Part 2: Directory System Protocol*
- 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 10000-2:1995, *Information technology framework and taxonomy of International Standardized Profiles — Part 2: Principles and taxonomy for OSI profiles.*

3 Definitions

3.1 General

Many of the definitions used may be found in the Standards. Since not all of the definitions are to be found in the Definitions subclauses 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 ITU-T equivalent (see also clause 2).

Table 1 — Definitions and references

Term	Part	Reference
access control scheme	2	15.1
administrative model	2	11
administrative role	2	13.3
base object	4	3
Basic Access Control	2	16
category	2	18.1
chaining	4	3
commonly usable	2	18.1
context prefix information	4	3
cooperative state	2	22.1
cross reference	2	18.1
directory operational framework	2	22.1
distributed name resolution	4	3
DSA information tree	2	19.1.1
DSA-shared attribute	2	19.1.1
DSA-specific attribute	2	19.1.1
DSA-specific entry (DSE)	2	19.1.1
DSE Type	2	19.1.1

[2]This specification defines Version 1 Certificates.

[3] To be published.

Term	Part	Reference
error	4	3
first level DSA	2	18.5
hard error	4	3
Hierarchical Operational Binding (HOB)	4	3
immediate superior reference	2	18.1
knowledge (information)	2	18.1
knowledge reference	2	18.1
master knowledge	2	18.1
modification operations	4	3
multi-chaining	4	3
multiple entry interrogation operations	4	3
name resolution	4	3
naming context	4	17.1
non-cooperative state	2	22.1
Non-specific Hierarchical Operational Binding (NHOB)	4	3
Non-specific Subordinate Reference (NSSR)	2	18.1
NSSR decomposition	4	3
operation progress	4	3
operational attribute	2	11.2
operational binding	2	22.1
operational binding establishment	2	22.1
operational binding instance	2	22.1
operational binding management	2	22.1
operational binding modification	2	22.1
operational binding termination	2	22.1
operational binding type	2	22.1
originator	4	3
performer	4	3
procedure	4	3
reference path	2	18.1
referral	4	3
relevant hierarchical operation binding (RHOB)	4	3
reply	4	3
request	4	3

Term	Part	Reference
request decomposition	4	3
shadow knowledge	2	18.1
Simplified Access Control	2	16
single entry interrogation operations	4	3
soft error	4	3
subentry	2	11.1
subordinate DSA	4	3
subordinate reference	2	18.1
subrequest	4	3
superior DSA	4	3
superior reference	2	18.1
target object name	4	3
uni-chaining	4	3

The terms in the following table are defined for the purposes of this part of ISO/IEC ISP 15125:

Table 2 — Definitions

Term	Definition
Acting DSA	The DSA which enters the evaluation phase as defined in subclause 15.2 of [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)]. Such a DSA will have completed name resolution and also undertakes the merging of results.
APDU size (for sending/receiving)	The size of the sent/received transfer encoding, including the ROSE header
invoking DSA	The DSA that generates a DSP Invoke
performing DSA	The DSA that acts upon a DSP Invoke (perhaps by further chaining) and generates a DSP Return Result or Return Error
root context	The complete collection of knowledge information about first level DSAs
Signed DSP Operation	A DSP operation which uses the SIGNED option of the OPTIONALLY-SIGNED information object class, applied to chained operations as defined in [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 12.1. The enclosed DAP operation may or may not be signed, as defined in [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclauses 9.1.1,9.2.1, 9.2.3, 10.1.1, 10.2.1, 11.1.1, 11.2.1, 11.3.1, 11.4.1.
Supported (for reception by an initiator)	A feature (capability, result, error or protocol element) is supported for reception by an initiator if the implementation is able to process the feature in accordance with the base standard and this part of ISO/IEC ISP 15125 to accomplish the function associated by the base standard with that feature. If a protocol element is claimed to be supported, the full range of values shall be supported, unless stated otherwise.

Term	Definition
Supported (for sending by an initiator)	A feature (capability, operation or protocol element) is supported for sending by an initiator if the implementation is able to generate the feature for chaining a request from a DUA or another DSA in order to complete it in accordance with the base standard and this part of ISO/IEC ISP 15125.

3.2 Support Level

To specify the support level of protocol features for this part of ISO/IEC ISP 15125, the following terminology is defined.

3.2.1 Mandatory: "m": Mandatory requirement for support

The support of the feature is mandatory for all implementations claiming compliance with this part of ISO/IEC ISP 15125.

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.

3.2.4 Outside the scope: "i"

Support for the item is outside the scope of this part of ISO/IEC ISP 15125.

3.2.5 not applicable: "-"

The item is not defined in the context where it is mentioned. There is no support requirement. The occurrence of "not applicable' is mainly due to the format of the tables in the ISPICS Requirements List.

4 Abbreviations

The following abbreviations are used as defined in [ISO/IEC 9594 : 1995 | ITU-T Rec. X.500 (1993)] or in ISO/IEC TR 10000-1 :

ACSE	Association Control Service Element
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
AVA	Attribute Value Assertion
CA	Certification Authority
CRL	Certificate revocation list
DAP	Directory Access Protocol
DIB	Directory Information Base
DIT	Directory Information Tree
DMD	Directory Management Domain
DSA	Directory System Agent
DSE	DSA specific entry
DSP	Directory System Protocol
DUA	Directory User Agent
HOB	Hierarchical operation binding
IPRL	ISPICS Requirements List

ISP	International Standardized Profile
ISPICS	ISP Implementation Conformance Statement
IUT	Implementation under test
NHOB	Non-specific hierarchical operation binding
NSSR	Non-specific Subordinate Reference
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
POQ	Partial outcome qualifier
PRL	Profile Requirements List
RDN	Relative Distinguished Name
RHOB	Relevant hierarchical operation binding
ROSE	Remote Operations Service Element
SPDU	Session Protocol Data Unit
SSDU	Session Service Data Unit

5 Conformance - DSP

This part of ISO/IEC ISP 15125 states requirements upon DSA implementations to achieve interworking using DSP. A claim of conformance to this part of ISO/IEC ISP 15125 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following subclauses and in Annex A of this part of ISO/IEC ISP 15125 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

The conformance requirements in this section relate to protocol requirements, and apply under all circumstances. Additional conformance requirements are defined in Section 3 for the procedures of Distributed Operations, many of which take place under particular circumstances, some of which (e.g. maintenance of references) are only indirectly observable by protocol.

5.1 Conformance Statement

For each implementation claiming conformance to this part of ISO/IEC ISP 15125 , an appropriate set of PICS shall be produced stating support or non-support of each option identified in this part of ISO/IEC ISP 15125. The PICS shall conform to 9.2.1 in [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)], and to the IPRL, Annex A of this part of ISO/IEC ISP 15125.

5.2 Static Conformance Requirements

To conform to this part of ISO/IEC ISP 15125, DSA implementations shall conform to all requirements of subclause 9.2 in [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)] applicable to a DSA implementing the **directorySystemAC** application context, including the requirements directly and indirectly referenced by that subclause. A DSA claiming conformance to this part of ISO/IEC ISP 15125 shall satisfy the requirements specified in 5.2.1 through 5.2.2.

All DSAs claiming conformance to this part of ISO/IEC ISP 15125 shall support either the performer role, or both performer and invoker roles.

> Note: In the IPRL defined in Annex A of this part of ISO/IEC ISP 15125, where protocol elements are nested, the requirement to support the nested element is relevant only when the immediately containing protocol element is supported. The conformance requirement of the protocol elements at the highest level is of relevance only when the related operation is supported.

A DSA conforming to this part of ISO/IEC ISP 15125 shall be able to use the referral mode of interaction, even if it only supports the DirectorySystemAC.

5.2.1 APDU Size

Implementations shall be capable of handling APDUs of at least 1Mb.

5.2.2 Security Level

Implementations shall be able to carry out the peer entity authentication of DSAs by the following ways:

- None
- Simple authentication with unprotected password
- Simple authentication without password

The following methods of peer entity authentication are optional (see Note 2 below):

- Simple protected authentication
- Strong authentication

Notes

1. Simple authentication, with protected and unprotected passwords, and strong authentication are profiled by ISO/IEC ISP 15125-7; implementations claiming conformance to these methods of authentication must conform to the appropriate parts of ISO/IEC ISP 15125-7.
2. The originator authentication of DUAs and results authentication are out of scope of this part of ISO/IEC ISP 15125.
3. External authentication using the **externalProcedure** element in accordance with [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 11.1 and [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 8.1.2 is outside the scope of this part of ISO/IEC ISP 15125.

5.3 Dynamic Conformance Requirements

To conform to this part of ISO/IEC ISP 15125, implementations shall conform to all requirements of 9.2.3 and 7.5 in [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)] for a DSA supporting the **directorySystemAC** application context. Implementations shall conform to all procedures specified in the directory base standards as amended by the corrigenda listed in annex B of this part of ISO/IEC ISP 15125. Implementations shall support all procedures and capabilities in the directory base standards as they relate to operations and protocol elements for which support is claimed in the PICS.

Note: A chaining DSA must propagate both supported and non-supported protocol elements in chained operations and chained responses as specified by the directory base standards.

5.3.1 Bind Response

The following forms of credentials represent acceptable responses to incoming DSA-Binds. The columns represent the form of the incoming bind. The cells are marked as follows:

M Mandatory

X Forbidden

A Acceptable but not recommended

R Recommended but not mandated

CHOICE	(unused)	simple authentication			strong authentication
Form in ⇒ ⇓ Form out	none	no password	unprotected password	protected password	
none	A	X	X	X	X
simple no password	R	M	A	X	X
simple unprotected password	X	X	R	X	X
simple protected password	X	X	X	M	X
strong	X	X	X	X	M

Note. This follows the following principles:

1. The Directory standards require that where the CHOICE is present in the incoming bind, the same choice must be used in the bind response (see [ISO/UEC 9594-3 : 1995 (E) | ITU-T Rec. X.511] subclause 8.1.3 , last sentence of 2nd paragraph, which carefully clarifies in the parentheses that ASN.1 CHOICE is what is meant by form here). Where the CHOICE is absent (as with 'none'), no stipulations are made, allowing some existing implementations to return (for example) a name without a password to permit the identification of the responding DSA. Note that the standards make no requirements that the precise form of authentication within the single choice of simple authentication should match for initiator and responder. These aspects, make it desirable to clarify what behaviour is acceptable.
2. When identification is confirmed (e.g. by password), the response must be comparable in security. Conversely, where no confirmation is provided (e.g. "none" or simple authentication without password), responding with a password appears to be a potentially unsafe publication of secret information, and cannot normally be recommended.
3. The responding DSA is always permitted to identify itself.

5.3.2 APDU Size Constraints

When for an invoking DSA an oversize response APDU is received or oversize request APDU would be sent, it may be discarded, in which case an appropriate error (i.e., ServiceError "unwillingToPerform" or "administrativeLimitExceeded") should be returned. However, it is recommended in the case of oversize list or search responses that the DSA truncate them to an acceptable size, marking the truncation with a partial outcome qualifier that signifies "administrative-limit-exceeded".

When for a performing DSA an oversize request APDU is received or an oversize response APDU would be sent, it may be discarded, in which case an appropriate error (i.e., Service Error "unwillingToPerform" or "administrativeLimitExceed") should be returned.

Notes

1. A DSA may be operated with administrative limits on APDU size lower than those specified in the static conformance requirements. The possible effects on distributed operations should be considered in establishing such limits.
2. This part of ISO/IEC ISP 15125 does not impose constraints on the actions of the supporting layers upon receiving response APDUs in excess of the limits specified.
3. See also subclause 5.2.1, APDU Size.

5.3.3 Rules of Extensibility for Result and Error Handling

Implementations shall satisfy the rule of extensibility for result and error handling specified in subclause 7.5 of [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)].

5.3.4 Filter Constraints

Filter constraints as defined in ADY21 shall apply.

5.3.5 Digital Signatures

Chaining DSAs shall accept and return signed chained operations and responses on behalf of other DSAs, but they need not be capable of evaluating the signature.

ISO/IEC ISP 15125-6 profiles the protocol and procedures associated with digital signatures in the context of DAP operations, both as returned to DUAs directly or as transmitted by DAP. ISO/IEC ISP 15125-7 profiles the protocol and procedures associated with digital signatures in the context of DSP operations.

5.4 Errors

5.4.1 General

Error handling is primarily described under the Abstract Operations part of the protocol ([ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)]). 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.

5.4.2 Permissible Errors

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

Table 3 below lists the errors that are possible for particular operations as defined within the Directory Standards. 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 except IQR	-	-
Compare	IM IAS NSA	ADP AP NSO IAS	IAR NI IS PR	Any except IQR	-	-
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	IAR NI IS PR	Any except IQR	AMD EAE OCV NV	-
Remove Entry	-	ADP AP NSO IAS	IAR NI IS PR	Any except IQR	AMD NAN	-
Modify-Entry	AVE CV IAS IM NSA UAT	ADP AP NSO IAS	IAR NI IS PR	Any except IQR	OMP OCV	-
Modify- RDN	-	ADP AP NSO IAS	IAR NI IS PR	Any except IQR	AMD NAN NV EAE	-
Abandon	-	-	-	-	-	NSO TL CA

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

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
IQR	Invalid Query reference
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

5.5 Use of info

It is recommended that the **info** component (of ASN.1 type **DomainInfo**, currently defined as **ANY**) is defined for profiling purposes as follows:

```
DomainInfo ::= SET OF CHOICE {
    SEQUENCE {
        infoType    OBJECT IDENTIFIER,
        infoValue   ANY DEFINED BY infoType
        },
    EXTERNAL
    }
```

No rules are made here for the use of the **info** element. In particular, there is no obligation to forward **info** elements using DSP.

5.6 DSA Unbind

Either the initiating or the responding DSA is permitted to initiate an unbind.[4] However, a DSA that has initiated an unbind may be unable to handle subsequently received returns from the responding DSA that were emitted prior to the unbind response**;** in view of this uncertainty, the use of A-ABORT is clearer, and is recommended.

A DSA that receives an unbind request is permitted to abandon incomplete operations on the association.

[4] Clause 9.2.1 of ISO/IEC 8649 (1994) states: “The A-RELEASE [which maps to the ROS Unbind] service is used by a requestor *in either AE* to cause the completion of the use of an association; it is a confirmed service.”

6 Conformance to Distributed Operations Procedures

Conformance to this section of the ISP 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 15125 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 that may occur in practice. A DSA is conformant to this part of ISO/IEC ISP 15125 if the DSA, after suitable set-up, is able to successfully carry out test suites within the range of requirements defined in this part of ISO/IEC ISP 15125.

Notes

1. Suitable set-up is implied within this part of ISO/IEC ISP 15125.
2. The requirements of this subclause apply whether or not HOBs (Hierarchical Operational Bindings) are supported.

DSAs claiming conformance to this part of ISO/IEC ISP 15125 shall satisfy the basic conformance requirement for distributed operations defined above.

Conformance requirements relating to this part of ISO/IEC ISP 15125 which lie outside X.500 standards requirements are listed in subclause A.7 of Annex A.

Note. Currently, this is empty.

7 Static conformance requirements

To conform to this part of ISO/IEC ISP 15125, implementations shall conform to clause 5 above and to the following additional requirements.

7.1 Elements of Distributed Operations

7.1.1 Reference Types

this part of ISO/IEC ISP 15125 requires conforming implementations to be able to hold and use reference types as summarised in Table 5 below.

Table 5 — Reference Types

Reference types	Holding and using capability	Notes
Superior reference	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 reference	Mandatory	
Cross-reference	Optional	Support of Cross References may be required for particular configurations of DSA.
Non-specific Subordinate reference	Optional	
Supplier reference	Conditional	This form or reference is applicable to DSAs that support shadowing as shadow consumers; such DSAs must support a Supplier Reference.
Master reference	Conditional	This form or reference is only applicable to DSAs that support shadowing as shadow consumers; such DSAs may optionally support a Supplier Reference.

Reference types	Holding and using capability	Notes
Immediate superior reference	Conditional	Applicable to DSAs that support Hierarchical Operational Bindings as the subordinate DSA

A DSA conformant to this part of ISO/IEC ISP 15125 shall be capable of holding and using a (single) Superior Reference.

DSAs conformant with this part of ISO/IEC ISP 15125 may optionally be able to hold and use Cross References.

Notes.

1. [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] and this part of ISO/IEC ISP 15125 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.
4. The protocol element **ReferenceType** also defines the value **self**. However, this is not a form of reference in the sense of [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)] subclause 18.3.2, and so has been omitted from this table. The value relates to the **returnToDUA** feature described in [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.10 i).

7.1.2 Knowledge References and the Root Context

7.1.2.1 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. The term "Root Context" is not defined in the '93 standards, but the usage seems well enough established by ‘88 practice to be perpetuated. See [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)] subclause 18.5 for a more comprehensive statement of requirements for first level DSAs.

7.1.2.2 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 15125 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 15125 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 one or more Non-specific Subordinate References, DSAs have potentially to multicast the operation with target object is not known to each other first-level DSA to determine whether the entry's first RDN actual exists anywhere.

7.1.2.3 Subordinate References

DSAs conformant to this part of ISO/IEC ISP 15125 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).

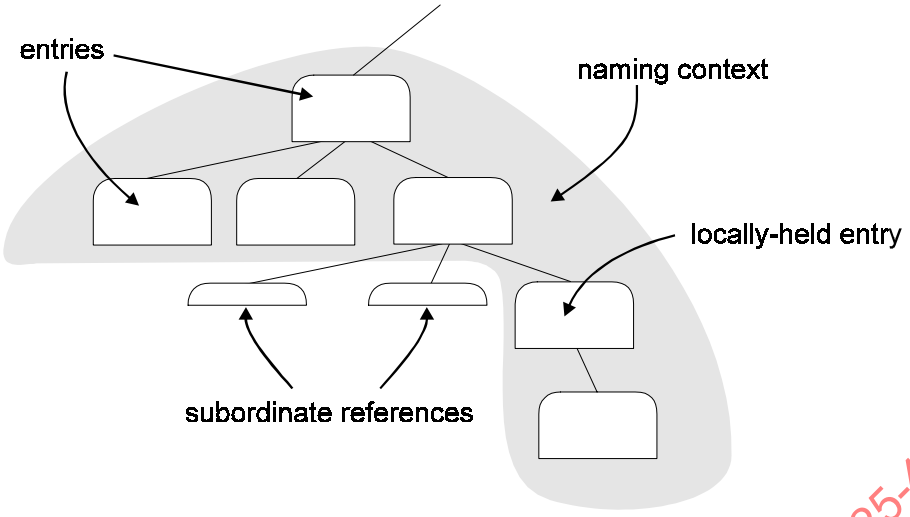

Figure 2 — Support of subordinate references

DSAs shall also be able to hold one or more locally mastered entries subordinate to an entry that is the immediate superior of a subordinate reference (Figure 2 lower right).

7.1.2.4 Non-specific Subordinate References

DSAs conformant to this part of ISO/IEC ISP 15125 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 zero, one, or more subordinate references, and zero, one, or more locally-mastered entries subordinate to the entry associated with each NSSR (Figure 3 lower right).

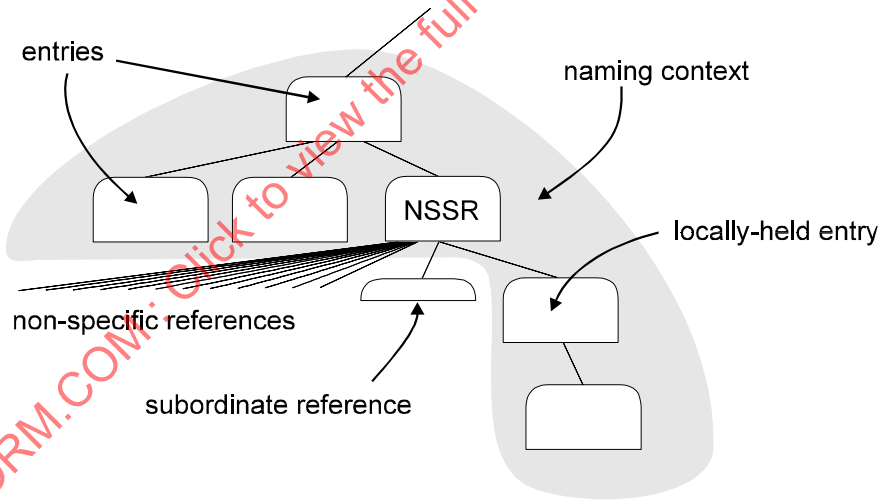

Figure 3 — Support of NSSRs

7.1.2.5 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 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.4 b) is optional.

A DSA is permitted to ignore the request for returning cross-references (“The administrative authority of a DSA may have a policy not to return such knowledge …), and is therefore not obliged to relay such a request.

7.2 Administrative Authorities

7.2.1 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).

There is no fixed requirement on the way the administrative authority performs these roles. However, DSAs may use the procedures of HOBs to achieve them where practical.

Notes.

1. See also clause 9 below.
2. The use of HOBS is not always possible, so DSAs must support other mechanisms as well.

7.2.1.1 Naming Contexts

DSAs shall be able to create 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).

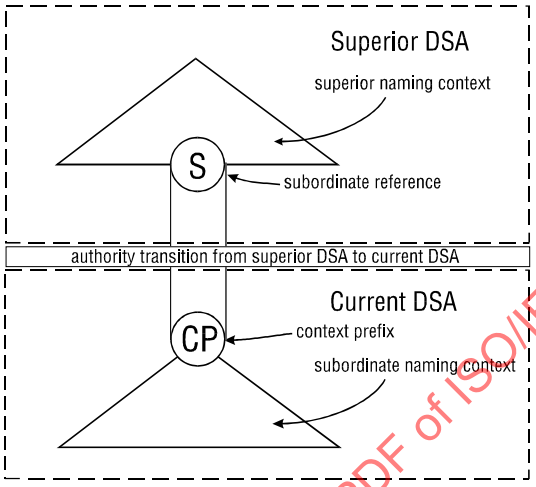

Figure 4 — Authority Transition-Subordinate DSA

7.2.1.2 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.

7.2.1.3 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)

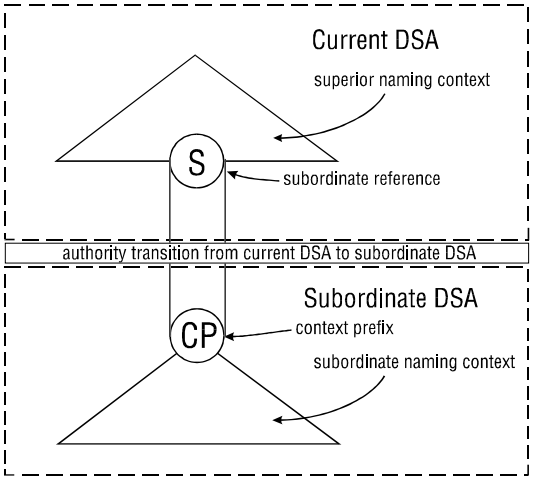

Figure 5 — Authority Transition-Superior DSA

7.2.1.4 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 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.

7.2.2 Optional Administrative Authority Roles

7.2.2.1 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.

7.2.2.2 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.

7.2.2.3 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).

7.3 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).

8 Procedures

8.1 Operation Pass-Through

8.1.1 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 : 1995 | ITU-T Rec. X.501 (1993)], [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)]and the definition of each attribute (e.g. in [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)]).

Note. The requirements for the support of attributes are defined in ISP 15126-1 Common Directory Use (Normal).

8.1.2 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 and including 3 octets in length.

Note. ISP 11188-1 Basic connection oriented requirements states in subclause 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.

8.1.3 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.

8.1.4 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.

8.2 Extensibility Rules

8.2.1 Non-critical extensions

All extensions within **ChainingArguments** and **ChainingResults** shall be regarded as non-critical, unless marked as critical.

Specifically, the following new components of **ChainingArguments** shall be regarded as non-critical, and shall be ignored if not supported:[5]

authenticationLevel

exclusions

excludeShadows

nameResolveOnMaster

and similarly for **ChainingResults**:

alreadySearched

8.2.2 Reference Type

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

[5] The derivation and handling of **uniqueIdentifier** is defined in ADY43.

8.2.3 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.

8.3 Loop detection/avoidance

DSAs are required to use loop detection in distributed operations, and may optionally use loop avoidance as defined by [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 15.4.1 and 15.4.2.

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.

8.4 Processing alias dereferencing during search

When aliases are to be dereferenced during search, DSAs are permitted to process them in the following manner:

1. Collect all aliases generated within the search scope being processed and discard duplicates.
2. Discard all aliases that are subordinate to:
   - The current base object
   - Any other base objects previously processed as part of the search
   - Any exclusions
   - Any other alias within the set of aliases

No recommendations are given for the case where an alias in the set is superior to the current base object or to any other base objects previously processed as part of the search. In the absence of special provisions, this would result in the search process encountering duplicates that would in any case be filtered out (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 21 3)).

8.5 Target object in chaining arguments, for add-entry

The name of **targetObject** should correspond to the object referred to by the argument, and not the superior of the object (as may be inferred from [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 15.2).

> Note.There can be a difference as a result of alias dereferencing during add entry operations.

8.6 Omission or variation of originator element in chaining arguments

In accordance with [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)] subclause 15.2.1 (see Note 2 following second paragraph) DSAs are permitted to omit the originator element in chaining arguments in support of a security policy which has determined that the value as supplied (by DSA or by a DAP bind) is unreliable.[6]

8.7 Local Scope

DSAs shall handle the **localScope** service control as if the operation is to be restricted wholly to a defined set of DSAs. The definition of the scope shall be defined in the first instance by the DSA to which the operation is initially directed, and subsequently by any other DSAs to which chaining takes place. Such chaining will only take place if the local scope is defined as a set of DSAs, and not just a single DSA.[7]

For each DSA encountered with the **localScope** service control set, no DSA outside this scope shall be chained to or referenced in continuation references. Aliases that point outside the local scope shall be handled as if they pointed to non-existent entries.

A DSA shall be configurable to implement **localScope** as meaning: respond as if the whole DIT were present in the present DSA; entries which are known about only as glue DSEs shall be considered absent, but indicative of the presence

---

[6] Further guidelines are provided in ADY43 Clause 6.10

[7] The group of DSAs implementing local scope needs management action to ensure that each DSA has a coordinated view of the group.

of this and possibly other entries being present in the DIT. Thus, a search from a base entry that is superior to a locally-held naming context shall successfully search that naming context, even if the base entry is not present in the DSA.

DSAs may also be configurable to interpret the **localScope** flag in terms of a pre-configured list of DSAs instead of a single DSA. The profiling of this interpretation is outside the scope of this part of ISO/IEC ISP 15125, but it is recommended that the effect be in accordance with the rules above, replacing the bound scope as the DMD or other collection of DSAs. The total effect should be that each DSA in the scope has a common understanding of the DSAs within this scope.

Specific rules for operations are:

1. In the case of read or compare operations, or a single-entry search operation, a DSA configured to act in this way shall return a return result if and only if the entry is held (as a master or shadow entry, as relevant) within the scope; chaining is permitted only within the scope. If not so held, the entry shall be considered not to exist, even if the DSA holds a glue DSE for the name. An alias referencing an entry not held within the local scope shall be treated as if the aliased entry did not exist (i.e. a name-error with alias-dereferencing-problem is returned).
2. In the case of list operations or search operations other than single-entry search operations, a DSA configured to act in this way shall generate a return result if and only if the base entry is held as a DSE (possibly just a glue DSE) within the DSA or within the set of DSAs in the defined local scope; the entries returned shall be selected from those actually held as entries or as aliases (in the case of searches, the alias may be dereferenced if possible and appropriate) within the operation's scope (one-level or subtree). Any aliases pointing outside the local scope shall be ignored. Aliases encountered before completion of name resolution shall be treated as for read or compare objects. Chaining and continuation references are permitted only to other DSAs within the local scope.
3. In the case of update operations, the DSA shall attempt to handle the operation as if **localScope** were not set, but shall fail to carry out the operation, and shall respond with Service Error **unwillingToPerform** if the DSA requires the participation of any DSA outside the local scope to fulfil the operation.

8.8 Time and size limits

On expiry of **timeLimit** in a DSP operation, processing of an operation must be terminated (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 16.1.4.1). However, if termination were to take place in all participating DSAs simultaneously, information returned at or just before this time will be discarded. This would diminish the quality of service of the Directory.

DSAs shall therefore be permitted to pass results back, even though the time limit has expired, within a configurable period after expiry.

A DSA shall return a result, if available, even if the time limit is exceeded, with a configurable period of grace.

In the case of **sizeLimit**, or where a local APDU size limit would be exceeded, a DSA is permitted to truncate the results. **PartialOutcomeQualifier** shall be used to indicate the missing information.

Note. DSAs should not return more results than the **sizeLimit** value permitted.

8.9 Authentication Level

A DSA that is passing through an operation is permitted to omit the **AuthenticationLevel** element. An omitted authentication level shall be taken as having the equivalent semantics for the '88 Directory standards, which may be taken as follows:

- If the **originator** component is absent in **ChainingArguments** and the DAP operation is unsigned, the authentication shall be taken as equivalent to none, with local qualifier omitted, which would be encoded as an **AuthenticationLevel** value of **{none}**
- If the **originator** component is present in **ChainingArguments** but the DAP operation is unsigned, the authentication shall be taken as equivalent to Simple unprotected with password, with local qualifier omitted, which would be encoded as an **AuthenticationLevel** value of **{simple}**
- If the DAP operation is signed, the authentication shall be taken as equivalent to Strong, with local qualifier omitted, which would be encoded as an **AuthenticationLevel** value of **{strong}**

DSAs that support access control in accordance with ISO/IEC ISP 15125-8 or 15125-9 shall be configurable to accept the incoming value of **AuthenticationLevel** as valid, whether the value is supplied explicitly or implicitly as described above. All DSAs shall be configurable to relay the incoming value of **authenticationLevel** when chaining on to other DSAs.

Note. Nevertheless, local security policies are permitted to modify the incoming value of **AuthenticationLevel** (e.g. in accordance with the perceived reliability of the source of the operation).

The use of **other** in **AuthenticationLevel** is outside the scope of this part of ISO/IEC ISP 15125.

8.10 Commonly usable replicated area

It is recommended that by "commonly usable replicated area" is meant one satisfying the following characteristics:

- The replicated area's Replication Base Entry corresponds to the Naming Context's context prefix
- The information content of the Replicated Area is complete in terms of both entries and attributes

8.11 Scope of referral

If a DSA claims support of **scopeOfReferral**, it shall satisfy the following requirements:

- The DSA shall be able to configure an arbitrary list of DSAs as within the same DMD (by unspecified means), and shall only create a referral with the **scopeOfReferral** service control set to **dmd** if the referral is to a DSA in this set
- The DSA shall be able to configure an arbitrary list of DSAs as within the same country (by unspecified means), and shall only create a referral with the **scopeOfReferral** service control set to **country** if EITHER the referral is to a DSA in this set OR if the locally defined country of location of the acting DSA matches the first RDN of the distinguished name of the DSA's name to which the referral applies

8.12 Return to DUA

DSAs are not obliged to generate the **returnToDUA** element, but shall relay it if one is received, back to the user.

DSAs shall never act themselves on a continuation reference containing a **returnToDUA** element, but shall always return it (e.g. in the form of a referral) to the originating DUA.

8.13 Name-resolve on Master

nameResolveOnMaster, as defined in [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 r) shall be supported by DSAs supporting NSSRs. The value shall be relayed when chaining occurs to another DSA.

8.14 Protocol information

No requirements are made on the use of **ProtocolInformation**. Recommendations are made in Annex C.

8.15 Exclusions

DSAs constructing the **exclusions** sub-element of **ChainingArguments** or of a **ContinuationReference** shall include the values contained in the **exclusions** sub-element of any corresponding incoming **ChainingArguments** or **ContinuationReference**.

8.16 Aliased RDNs

aliasedRDNs shall be present if an alias was encountered.

8.17 Dereferencing Continuation References

Because continuation references can be caused by service failures (e.g. non-availability of DSAs), DSAs are not obliged always to dereference continuation references.

Annex A
(normative)
Profiles Requirements List

Note. In the event of a discrepancy becoming apparent in the body of autonomous DSA procedures and the tables in this Annex, this Annex is to take precedence.

A.0 Introduction

This Annex specifies the constraints and characteristics of DSAs that claim conformance to this part of ISO/IEC ISP 15125.

DSAs shall support the performing role (see subclause 5.2), and may optionally support the invoking role.

Invoking DSAs are considered to be acting in one of two modes, *relaying* or *acting*:

- An invoking DSA in a relaying mode chains on an operation to another DSA without undertaking an Evaluation Phase as defined in [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 5.2 (this will occur if name resolution is incomplete)
- An invoking DSA in an acting mode is one that chains on an operation having undertaken the Evaluation Phase

Similarly, responding DSAs are considered to be acting in one of two modes, *relaying* or *acting*:

- A responding DSA in a relaying mode passes back unchanged the result or error, or some component of it, as received from a DSA to which the operation was originally chained
- A responding DSA in an acting mode is one that creates or changes the result or error, or some component of it, as received from a DSA to which the operation was originally chained

The abbreviations used 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 15125

There are three columns indicating the mandatory, optional or conditional status (etc) of elements within associations (i.e. after bind has taken place).

For invokes

Column heading:	Rel (relaying)	Act (acting)	Resp (responding)
Applies to	Initiator	Initiator	Responder
Meaning:	Initiates a chained operation as a result of relaying in the Name Resolution Phase	Initiates a chained operation in the Evaluation Phase	Responds to a chained operation as a result of relaying or acting

For return-results or errors:

Column heading:	Init (initiating)	Rel (relaying)	Act (acting)
Applies to	Initiator	Responder	Responder
Meaning:	Accepts a response to a chained operation	Returns an element unchanged	Returns a new or changed element

A definition of the Name Resolution and Evaluation phases is given in [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 15.2.

A.1 Identification of the implementation

A.1.1 Identification of PICS

(void)

A.1.2 Identification of the implementation and/or system

Item no.	Question	Response
1	Implementation Name	
2	Version Number	
3	Machine Name	
4	Machine Version Number	
5	Operating System Name	
6	Operating System Version No.	
7	Special Configuration	

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

(void)

A.2 Identification of the protocol

Item no	Question	Response
1	Title, Reference, No., publication date of the protocol standard	[ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)]
2	Protocol Version Number	Version 1
3	Implemented Addenda	
4	Implemented Defect Reports (Reference No.)	See Annex B

A.3 Global statement of conformance

A.3.1 DSA implementation and/or system

Item No.	Question	D	P	Predicate Name or note	Response
1.	Are all mandatory general capabilities for the DSA implemented?	m	m		
2.	Are all mandatory First-level DSA requirements ([ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)]) implemented?	c	o	p_first_level_dsa	
3.	Are minimum knowledge requirements [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)] implemented?	m	m		
4.	Is a Superior Reference supported?	-	c1	A.3.1/8	
5.	Are Subordinate References supported?	-	m		
6.	Are Cross References supported?	o	o	p_cross_references	
7.	Are Non-Specific Subordinate References supported?	o	o	p_nssr	

Item No.	Question	D	P	Predicate Name or note	Response
8.	Are Supplier References supported?	-	c2	A.3.1/11	
9.	Are Master References supported	-	o	p_master_reference	
10.	Are Immediate Superior References supported	-	c3	A.3.1/12	
11.	Is shadowing supported as a consumer?			p_shadow_consumer	
12.	Are Hierarchical operational bindings supported?	-	o	p_hob	
13.	Is asynchronous (ROSE class 2) mode of operation supported?	m	m		
14.	Does the DSA follow the rules of extensibility as defined in section 7.5 of [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)]?	m	m		
15.	Is the alias dereferencing mechanism implemented in name resolution?	m	m		
16.	Is the alias dereferencing mechanism implemented in the evaluation phase of search operations?	m	m		
17.	Does the DSA support the application-context(s) directorySystemAC?	m	m		
18.	Does the DSA support being a non-first-level DSA?	-	o	p_non_first_level_dsa	
19.	Does the DSA support the invoker role?		o	p_invoker	
20.	Does the DSA support “none” credentials in the DSA Bind?		m	Note 1	
21.	Does the DSA support simple unprotected credentials in the DSA Bind?	o	m	Note 1	
22.	Does the DSA support simple protected credentials in the DSA Bind?	o	o	p_simple_protected Note 2	
23.	Does the DSA support strong credentials in the DSA Bind?	o	o	p_strong Note 2	
24.	Does the DSA support signed chained operations?	o	o	p_signed_chained Note 2	
25.	Does the DSA support unique names? (See [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 n)	o	o	p_unique_name	
26.	Does the DSA support authentication level? (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 m)	o	o	p_auth_level	
27.	Does the DSA support exclusions (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 p)	o	o	p_exclusions	
28.	Does the DSA support excludeShadows (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 q)	o	o	p_excludeShadows	
29.	Does the DSA support nameResolveOnMaster (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 r)	o	o	p_nameResolveOnMaster	

Item No.	Question	D	P	Predicate Name or note	Response
30.	Does the DSA support alreadySearched (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.4 d)	o	o	p_alreadySearched	
31.	Does the DSA support creation of a request for cross-references (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 f)	o	o	p_obtain_xr	
32.	Does the DSA support the supply of cross-references on request (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.4 b)	o	o	p_supply_xr	
33.	Does the DSA support the request to return the operation to the DUA (see [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.10 i)	o	o	p_return_to_dua	

Conditionals:

c1: if p_non_first_level_dsa then m else o

c2: if p_shadow_consumer then m else o

c3: if p_hob then m else o

Notes:

1. As required by subclause 5.2.2.
2. Security levels are profiled in ADY43. They are represented in this PRL by the predicates p_simple_protected (A.3.1.22), p_strong (A.3.1.23), p_signed_chained(A.3.1.24).

A.4 Capabilities and options

A.4.1 Supported application context

The only application context supported by this part of ISO/IEC ISP 15125 is the Directory System Application Context.

A.4.2 Operations and Extensibility

A.4.2.1 Operations

Item No.	Protocol Element	D Init	D Resp	P Rel	P Act	P Resp	Reference/notes
1	DirectoryBind	m	m	c4	c4	m	Note 1
2	DirectoryUnbind	m	m	c4	c4	m	Note 1
3	ChainedRead	m	m	c4	c4	m	Note 1
4	ChainedCompare	m	m	c4	c4	m	Note 1
5	ChainedAbandon	m	m	c4	c4	m	Note 1
6	ChainedList	m	m	c4	c4	m	Note 1
7	ChainedSearch	m	m	c4	c4	m	Note 1
8	ChainedAddEntry	m	m	c4	c4	m	Note 1
9	ChainedRemoveEntry	m	m	c4	c4	m	Note 1
10	ChainedModifyEntry	m	m	c4	c4	m	Note 1
11	ChainedModifyDN	m	m	c4	c4	m	Note 1

Conditionals:

c4: if p_invoker then m else o

Notes

1. The PICS doesn't distinguish between the relaying and acting role.

A.4.2.2 Extensibility

The Directory System Protocol requires general conformance to the principles of extensibility, as defined in [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)]. No additional requirements are specified.

A.4.3 Protocol Elements

A.4.3.1 DSA Bind Elements

A.4.3.1.1 DSA Bind Arguments

The column marked Init correspond to the bind initiator

Item No.	Protocol Element	D Init	D Resp	P Init	P Resp	References/Notes
1	DirectoryBindArg	m	m	m	m	A.4.2.1/1
2	credentials	c	c	m	m	
3	simple	c	c	m	m	
4	name	m	m	m	m	
5	validity	o	o	c5	c5	Note 1
6	time1	o	o	c5	c5	Note 1
7	time2	o	o	o	o	Note 1
8	random1	o	o	c5	c5	Note 1
9	random1	o	o	o	o	Note 1
10	password	o	o	m	m	
11	unprotected	o	o	m	m	
12	protected	o	o	c5	c5	Note 1
13	algorithmIdentifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c6	c6	
16	certification-path	o	o	o	m	Note 2
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithmIdentifier	m	m	m	m	
24	encrypted	m	m	m	m	
25	name	o	o	o	m	
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Predicates:

c5: If p_simple_protected then m else o

c6: If p_strong then m else o

Notes.

1. The support of simple protected authentication is profiled by ADY43.
2. Requirements on certification-path are profiled by ADY43

A.4.3.1.2 DSA Bind Result

Item No.	Protocol Element	D Init	D Resp	P Init	P Resp	References/Notes
1	DirectoryBindResult	m	m	m	m	A.4.2.1/1
2	credentials	c	c	m	m	
3	simple	c	c	m	m	
4	name	m	m	m	m	
5	validity	o	o	c5	c5	Note 1
6	time1	o	o	c5	c5	Note 1
7	time2	o	o	o	o	Note 1
8	random1	o	o	c5	c5	Note 1
9	random2	o	o	o	o	Note 1
10	password	o	o	m	m	
11	unprotected	o	o	m	m	
12	protected	o	o	c5	c5	Note 1
13	algorithmIdentifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c6	c6	
16	certification-path	o	o	m	o	Note 2
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithmIdentifier	m	m	m	m	
24	encrypted	m	m	m	m	
25	name	o	o	o	m	
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Predicates:

c5: If p_simple_protected then m else o

c6: If p_strong then m else o

Notes.

1. The support of simple protected authentication is profiled by ADY43.
2. Requirements on certification-path are profiled by ADY43

A.4.3.1.3 Directory Bind Error

Item No.	Protocol Element	D Init	D Resp	P Init	P Resp	References/Notes
1	DirectoryBindError	m	m	m	m	A.4.2.1/1
2	versions	m	m	m	m	

Item No.	Protocol Element	D Init	D Resp	P Init	P Resp	References/Notes
3	error	m	m	m	m	
4	serviceError	m	m	m	m	
5	securityError	m	m	m	m	

A.4.3.2 Directory Unbind Elements

DirectoryUnbind has no argument (see Section 8.2 of [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)]).

A.4.3.3 Chained Operation Elements

A.4.3.3.1 Argument

Item No.	Protocol Element	D Init	D Resp	P Rel	P Act	P Resp	References/Notes
1	chainedXxx	c	m	c4	c4	m	A.4.1.1/3-11 omitting A.4.1.1/5 Note 1
2	chainedXxxArgument	m	m	m	m	m	Note 1
3	unsigned (chainedXxxArgument)	m	m	m	m	m	Note 1
4	ChainingArguments	m	m	m	m	m	
5	XxxArgument	m	m	m	m	m	Note 1
6	signed (chainedXxxArgument)	o	o	c7	c7	c7	A.4.1.1/3-11 omitting A.4.1.1/5 Note 1
7	ToBeSigned	m	m	m	m	m	
8	ChainingArguments	m	m	m	m	m	A.4.3.7
9	XxxArgument	m	m	m	m	m	Note 1
10	algorithmIdentifier	m	m	m	m	m	Note 3
11	encrypted	m	m	m	m	m	
12	ChainingArguments	m	m	m	m	m	
13	XxxArgument	m	m	m	m	m	Note 1

Predicates:

c4: if p_invoker them m else o

c7: if p_signed_chained them m else o

Notes.

1. Xxx is any one of:

   read (A.4.2.1/3)
   compare (A.4.2.1/4)
   list (A.4.2.1/6)
   search (A.4.2.1/7)
   add-entry (A.4.2.1/8)
   remove-entry (A.4.2.1/9)
   modify-entry (A.4.2.1/10)
   modify-DN (A.4.2.1/11)

2. Requirements on the signatures of chained operations are profiled in ADY43. Requirements on arguments are profiled in ADY12.

3. Requirements on **algorithmIdentifier** are profiled in ADY43.