INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10615-3

First edition
1996-07-01

Information technology — International Standardized Profiles ADInn — OSI Directory —

Part 3:
ADI21 — DSA Performer Role

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

Partie 3: ADI21 — Rôle de réalisateur du DSA

Reference number
ISO/IEC ISP 10615-3:1996(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 Standard 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 JTC1. In addition to developing International Standards, ISO/IEC JTC1 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 10615-3 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 3:ADI21 - DSA Performer Role*
- *Part 4:ADI22 - DSA Invoker Role*

Annexes A and B form an integral part of this part of ISO/IEC ISP 10615.

Introduction

This part of ISO/IEC ISP 10615 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 context 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 "legitimize" 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 realization of this goal.

The text of this part of ISO/IEC ISP 10615 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 10615 is harmonized among these three Workshops and it was finally ratified by the Workshops' plenary assemblies.

This page intentionally left blank

Information technology — International Standardized Profiles ADInn — OSI Directory —

Part 3:
ADI21 — DSA Performer Role

1 Scope

1.1 General

This part of ISO/IEC ISP 10615 covers the use of the DSP protocol by a DSA which receives an invoke from another DSA and responds with a result or error. The related part of the ISP, ADI32, covers the behavior of the DSA in fulfilling distributed operations, when considered to be independent of the protocol used.

The objective of this part of ISO/IEC ISP 10615 is to define capabilities and constraints on support for DSP by performer functions of DSAs so that DSAs will be able to interwork within the Directory. Factors outside the scope of this part of ISO/IEC ISP 10615 include, but are not limited to, DIT structure, behaviour in distributed operations and some aspects of authentication (e.g., simple authentication with protected passwords, strong authentication, and the use of non-local authentication).

The scope of ISO/IEC ISP 10615 is limited to the '88 edition of the Directory standards.

1.2 Position Within the Taxonomy

This part of ISO/IEC ISP 10615 is identified in ISO/IEC TR 10000-2 as "ADI21 - DSA Performer Role".

It may be combined with other parts of ISO/IEC ISP 10615, with ISO/IEC ISP 10616 specifying use of the directory, and with T-Profiles specifying the OSI connection-mode transport service.

1.3 Scenario

The model used is described in Overview of Concepts, Models, and Services in ISO/IEC 9594-1 : CCITT X.500. Specifications of ISO/IEC ISP 10615-3 apply to the performer role of DSP for a DSA within the scenario of Figure 1.

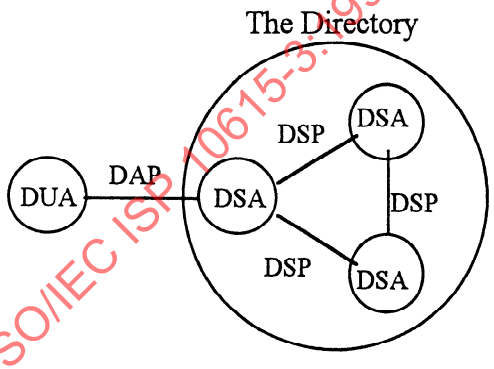

Figure 1 - Access to the Directory and Distributed Directory Model

2 Normative References

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

ISO/IEC 2022 : 1994, *Information technology - Character code structure and extension techniques.*

ISO 3166 : 1993, *Codes for the representation of names of countries.*

ISO/IEC 8824 : 1990, *Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).*
(See also CCITT Recommendation X.208: 1988.)

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

(See also CCITT Recommendation X.209: 1988.)

ISO/IEC 9594-1 : 1990, *Information technology - Open Systems Interconnection - The Diectory - Part 1 : Overview of concepts, models, and services.* (See also CCITT Recommendation X.500(1989).)

ISO/IEC 9594-2 : 1990, *Information technology - Open Systems Interconnection - The Directory - Part 2 : Models.* (See also CCITT Recommendation X.501(1989).)

ISO/IEC 9594-3 : 1990, *Information technology - Open Systems Interconnection - The Directory - Part 3 : Abstract service definition.* (See also CCITT Recommendation X.511(1989).)

ISO/IEC 9594-4 : 1990, *Information technology - Open Systems Interconnection - The Directory - Part 4 : Procedures for Distributed Operation. (See also CCITT Recommendation X.518(1989).)*

ISO/IEC 9594-5 : 1990, *Information technology - Open Systems Interconnection - The Directory - Part 5: Protocol specifications.* (See also CCITT Recommendation X.519(1989).)

ISO/IEC 9594-6 : 1990, *Information technology - Open Systems Interconnection - The Directory - Part 6 : Selected attribute types.* (See also CCITT Recommendation X.520(1989).)

ISO/IEC 9594-7 : 1990, *Information technology - Open Systems Interconnection - The Directory - Part 7 : Selected object classes.* (See also CCITT Recommendation X.521(1989).)

ISO/IEC 9594-8 : 1990, *Information technology - Open Systems Interconnection - The Directory - Part 8 : Authentication framework.* (See also CCITT Recommendation X.509(1989).)

ISO/IEC 9646-1 : 1994, *Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1 : General concepts.* (See also ITU-T Recommendation X.290(1995).)

ISO/IEC 9646-2 : 1994, *Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2 : Abstract Test Suite specification.*(See also ITU-T Recommendation X.291(1995).)

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.*

CCITT Recommendation T.61 : 1988, *Character Repertoire and Coded Character Sets for the International Teletex Service.*

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

For the purposes of this part of ISO/IEC ISP 10615, the following definitions apply.

Terms used in this part of ISO/IEC ISP 10615 are defined in the referenced base standards.

In addition, the following terms are defined.

3.1 General

3.1.1 APDU size (for sending/receiving): the size of the sent/received transfer encoding, including the ROSE header.

3.1.2 supported (for reception by a performer): A feature (capability, operation, or protocol element) is supported by a receiving performer if the implementation is able to process the features in accordance with the base standards and this ISP to accomplish the function associated by the base standards with that feature. If a protocol element is claimed to be supported, the full range of values shall be supported, unless stated otherwise.

3.1.3 supported (for sending by a performer): A feature (capability, result, error or protocol element) is supported for sending by a performer if the performer is able to generate the feature in response to each requests that requires that feature to support the function of the request.

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 in 3.2.1 through 3.2.5.

3.2.1 mandatory (requirement to support), m: Support for this item is required.

3.2.2 optional (requirement to support), o: Support for this item is optional.

3.2.3 conditional (requirement to support), c: The requirement to support this item is depends on the specified condition. The condition and the resulting support requirements are stated separately, usually via reference based on a number following the 'c'.

3.2.4 outside the scope (requirement to support), i: Support for item is outside of the scope of this part of ISO/IEC ISP 10615.

3.2.5 not applicable (requirement to support), -: This item is not defined in the context in which is mentioned. There is no support requirement.

4 Abbreviations

For the purposes of this part of ISO/IEC 10615, the following abbreviations apply.

Abbreviations used in this part of ISO/IEC ISP 10615 are defined in the referenced base standards.

ACSE	Association Control Service Element
APDU	Application Protocol Data Unit
AVA	Attribute Value Assertion
DAP	Directory Access Protocol
DIB	Directory Information Base
DIT	Direcotry Information Tree
DSA	Directory System Agent
DSP	Direcotroy System Protocol
DUA	Directory User Agent
IPRL	ISPICS Requirements List
ISP	International Standardized Profile
ISPICS	ISP Implementation Conformance Statement
PICS	Protocol Implementation Conformance Statement
RDN	Relative Distinguished Name
ROSE	Remote Operations Service Element
SPDU	Session Protocol Data Unit
SSDU	Session Service Data Unit

5 Conformance

This part of ISO/IEC ISP 10615 states requirements upon implementations to achieve interworking. A claim of conformance to this part of ISO/IEC ISP 10615 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in annex A of this part of ISO/IEC ISP 10615 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

To conform to this part of ISO/IEC ISP 10615, implementations shall conform to all requirements of 9.2 in ISO/IEC 9594-2 for a DSA implementing the directorySystemAC application context, including the requirements directory and indirectly referenced by that clause. A DSA claiming conformance to this part of ISO/IEC ISP 10615 shall satisfy the requirements specified in 5.1 through 5.3 following.

5.1 Conformance Statement

For each implementation claiming conformance to this part of ISO/IEC ISP 10615, an appropriate set of PICSs shall be produced stating support or non-support of each option identified in this part of O/IEC ISP 10615. The PICS shall conform to 9.2.1 in ISO/IEC 9594-5, and to the IPRL, annex A of this ISO/IEC ISP 10615.

5.2 Static Conformance Requirements

To conform to this part of ISO/IEC ISP 10615, implementations shall conform to all requirements of 9.2.2 in ISO/IEC 9594-5 for a DSA supporting the directorySystemAC application context, and shall conform to the requirements stated in the IPRL (Annex A) and the remainder of 5.2 of the part of ISO/IEC ISP 10615.

NOTE - In the IPRL defined in Annex A of this part of ISO/IEC ISP 10615, where protocol elements are nested, the conformance requirements is of relevance only when the immediately containing protocol element is transmitted (or received). The conformance requirement of the protocol elements at the highest level is of relevance only when the related operation is supported.

5.2.1 APDU Size

Implementations shall be capable of accepting and processing operation request APDUs of any size up to 32 767 (32k-1) octets. DSAs shall be capable of sending response APDUs of any size up 262 143 (256k-1) octets in length.

NOTE - See also 5.3.1 APDU Size Constraints.

5.2.2 Security Level

To conform to this part of ISO/IEC ISP 10615, implementations shall be able to carry out the peer entity authentication of DSAs by following ways:

- none
- simple authentication with unprotected password

The following method of peer entity authentication is optional.

- simple authentication without password

NOTE
1: The ways of following authentication are out of scope of this part of ISO/IEC ISP 10615.

- simple authentication with protected password
- strong authentication
- external authentication procedure

2: The originator authentication of DUA and results authentication are out of scope of this part of ISO/IEC ISP 10615.

5.3 Dynamic Conformance Requirements

To conform to this part of ISO/IEC ISP 10615, implementations shall conform to all requirements of 9.2.3 and 7.5 in ISO/IEC 9594-5 for a DSA supporting the directorySystemAC application context. Implementations shall conform to all procedures specified in the directory base standards as amended by corrigenda and defect reports listed in annex B of this part of ISO/IEC ISP 10615. 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 response as specified by the directory base standards.

5.3.1 APDU Size Constraints

When 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.

NOTE
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 10615 does not place an upper bound on the size of APDUs that a DSA is permitted to send or receive. However, it is recommended that it possible to configure a DSA to not send (generate or propagate) a response APDU in excess of 262 143 octets, except to DSAs that are known to be capable of receiving APDUs of the size being sent.

3: This part of ISO/IEC ISP 10615 does not impose constraints on the actions of the supporting layers upon receiving APDUs in excess of 32 767 octets in length.

4: See also 5.2.1, APDU Size

5.3.2 Rules of extensibility for operation processing

Implementation shall satisfy the rules of extensibility for operation processing specified in 7.5.2.4 and 7.5.2.5 of ISO/IEC 9594-5: Cor.1:1992(E).

5.3.3 Filter Constraints

Each DSA shall support at least 32 FilterItems in a SearchArgument, and shall support the nesting of at least any possible combination of elements of the Filter (i.e., Choice of item, and or, and not).

Note: An implementation that contains the deepest of the eight level to be item will be considered to meet this requirement.

When a request exceeding the filter constraints is received, the DSA may refuse to perform the request if the DSA reaches the operation evaluation phase, in which case the ServiceError response shall be ServiceProblem, unwillingToPerform.

A DSA shall support search string ("initial", "any" or "final" element) of at least 1024 characters.

For approximate matching, a DSA is not required to use any matching rule other than the relevant equality matching rule.

5.3.4 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 the evaluation of the signature.

5.3.5 Error Handling

To conform to this part of ISO/IEC ISP 10615, implementations shall deal with errors in the following way.

If a request has more than one attribute in Error, a DSA is not required to report all attributes in error in a returned AttributeError.

Annex A
(normative)
ISPICS Requirements List(IPRL)

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.1 Introduction

The tables of this annex specify the level of support for each feature of the DSP protocol, as required by this part of ISO/IEC ISP 10615.

The abbreviations as used in the headings of the tables in this annex are

D - conformance requirement as defined in the base standard

P - conformance requirement for this part of ISO/IEC ISP 10615.

Section 1: Identification of the Implementation

A.2 Identification of the Implementation

A.2.1 Identification of PICS

(void)

A.2.2 Identification of the implementation and/or system

Item 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	non-First-level DSA or First-level DSA
8	Other Information	(void)

A.2.3 Identification of the system supplier and/or test laboratory client

(void)

Section 2: General Specification

A.3 Identification of the Protocol

1	Protocol Standard	ISO/IEC 9594:1989:Information technology - Open Systems Interconnection - The Directory
2	Protocol Version	Version 1
3	Implemented Addenda	None
4	Implemented Defect Reports	See Annex B

A.4 Global Statement of Conformance

Item No	Question	D	P
1	Are all mandatory general capabilities implemented?	m	m
2	Are minimum knowledge requirements (ISO/IEC 9594-4: 1990) implemented?	m	m
3	Are all mandatory First-level DSA requirements (ISO/IEC 9594-4: 1990) implemented?	c01	c01
4	Is Cross Reference implemented?	o	i
5	Is NSSR (non-specific subordinate reference) implemented?	o	i
6	Is security level "none" for peer entity authentication supported?	o.1	m
7	Is security level "simple without password" for peer entity authentication supported?	o.1	o
8	Is security level " simple with unprotected password" for peer authentication supported?	o.1	m
9	Is security level "simple with protected password" for peer authentication supported?	o.1	i
10	Is security level "strong" for peer entity authentication supported?	o.1	i
11	Is security level "none" for originator authentication supported?	o.2	o.12
12	Is security level "simple with distinguished name" for originator authentication supported?	o.2	o.12
13	Is security level "strong" for originator authentication supported?	o.2	i
14	Is security level "none" for results authentication supported?	o.3	m
15	Is security level "strong" for results authentication supported?	o.3	i
16	Is "DSA Referal Mode" supported?	m	m
17	Is "Chaining Mode" supported?	o	o(Note 1)
18	Is the alias mechanism implemented?	o	i

Note 1: Chaining mode is within the scope of ADI22.
o.1: At least one of Security levels for peer entity authentication shall be supported.
o.2: At least one of Security levels for originator authentication shall be supported.
o.3: At least one of Security levels for results authentication shall be supported.
o.12: At least one of Security levels for originator authentication shall be supported.
c01: if the special configuration in A.2.2.7 is First-level DSA then m else -.

Section 3: Capabilities and Options

A.5 Capabilities and Options

A.5.1 Supported Application Context

1	The only application context supported by this part of ISO/IEC ISP 10615 is Directory System Application Context defined in ISO/IEC 9594-5.

A.5.2 Operations

Item No	Operation	Reference	D	P
1	DSABind	A.5.3.1	m	m(Note 1)
2	DSAUnbind	A.5.3.2	m	m(Note 1)
3	ChainedRead	A.5.3.3	m	m
4	ChainedCompare	A.5.3.4	m	m
5	ChainedAbandon	A.5.3.5	m	m
6	ChainedList	A.5.3.6	m	m
7	ChainedSearch	A.5.3.7	m	m
8	ChainedAddEntry	A.5.3.8	m	m
9	ChainedRemoveEntry	A.5.3.9	m	m
10	ChainedModifyEntry	A.5.3.10	m	m
11	ChainedModifyRDN	A.5.3.11	m	m

Note 1: Only support as an association responder is required.

A.5.3 Protocol Elements

A.5.3.1 DSABind Protocol Elements

A.5.3.1.1 DSABind Arguments

Item No	Protocol Element/Parameter	Reference	Sending		Receiving		Supported values and Notes
			D	P	D	P	
1	DirectoryBindArgument		o	o	m	m	
2	credentials		c10	m	c10	m	
3	simple		c11	m	c11	m	
4	name		m	m	m	m	
5	validity		o	i	o	i	
6	password		o	m	o	m	
7	strong		c12	i	c12	i	
8	externalProcedure		o	i	o	i	
9	versions		m	m	m	m	v1988(0)

c10: if at least one of answers to A.4.7, A.4.8, A.4.9 and A.4.10 is "Yes" then m else o.
c11: if at least one of answers to A.4.7, A.4.8 and A.4.9 is "Yes" then m else o.
c12: if answers to A.4.10 is "Yes" then m else o.

A.5.3.1.2 DSABind Result

Item No	Protocol Element/Parameter	Reference	Sending D	Sending P	Receiving D	Receiving P	Supported Values and Notes
1	DirectoryBindResult		m	m	o	o	
2	credentials		c10	m	c10	m	
3	simple		c11	m	c11	m	
4	name		m	m	m	m	
5	validity		o	i	o	i	
6	password		o	m	o	m	
7	strong		c12	i	c12	i	
8	externalProcedure		o	i	o	i	
9	versions		m	m	m	m	v1988(0)

A.5.3.1.3 DSABind Error

Item No	Protocol Element/Parameter	Reference	Sending D	Sending P	Receiving D	Receiving P	Supported (Note1) Values and Notes
1	DirectoryBindError		m	m	o	o	
2	versions		m	m	m	m	v1988(0):Note 2
3	serviceError		m	m	m	m	unavailable
4	securityError		m	m	m	m	inappropriate-Autentication invalidCredentials

Note 1 : Only the specified values shall be generated, execpt as noted.
Note 2 : When indicating directory bind error, DSA may indicate versions that it supports other those within the scope of ISO/IEC ISP 10615-3.

A.5.3.2 DSAUnbind Protocol Element

DSAUnbind has no arguments(refer 13.2 in ISO/IEC 9594-4).

A.5.3.3 ChainedRead Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	ChainingArguments	A.5.3.21	m	m	
2	ReadArgument		m	m	
3	object		m	m	
4	selection	A.5.3.16	m	m	
5	CommonArguments	A.5.3.13	m	m	
6	ChainingResults	A.5.3.22	m	m	
7	ReadResult		m	m	
8	entry	A.5.3.17	m	m	
9	CommonResults	A.5.3.14	m	m	

A.5.3.4 ChainedCompare Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supporeted Values and Notes
1	ChainingArguments	A.5.3.21	m	m	
2	CompareArgument		m	m	
3	object		m	m	
4	purported		m	m	
5	CommonArguments	A.5.3.13	m	m	
6	ChainingResults	A.5.3.22	m	m	
7	CompareResult		m	m	
8	DistinguishedName		m	m	
9	matched		m	m	
10	fromEntry		m	m	
9	CommonResults	A.5.3.14	m	m	

A.5.3.5 ChainedAbandon Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	ChainingArguments	A.5.3.21	m	m	
2	AbandonArgument		m	m	
3	invokedId		m	m	
4	ChainingResults	A.5.3.22	m	m	
5	AbandonResult		m	m	

A.5.3.6 ChainedList Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	ChainingArguments	A.5.3.21	m	m	
2	ListArgument		m	m	
3	object		m	m	
4	CommonArguments	A.5.3.13	m	m	
5	ChainingResults	A.5.3.22	m	m	
6	ListResult		m	m	
7	listInfo		m	m	
8	DistinguishedName		m	m	
9	subordinates		m	m	
10	RelativeDistinguishedName		m	m	
11	aliasEntry		m	m	
12	fromEntry		m	m	
13	partialOutcomeQualifier		m	m	
14	limitProblem		m	m	
15	unexplored	A.5.3.20	m	m	
16	unavailableCriticalExtensions		m	m	
17	CommonResults	A.5.3.14	m	m	
18	uncorrelatedListInfo	A.5.3.6.6	m	m	

A.5.3.7 ChainedSearch Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	ChainingArguments	A.5.3.21	m	m	
2	SearchArgument		m	m	
3	baseObject		m	m	
4	subset		m	m	
5	filter	A.5.3.18	m	m	
6	searchAliases		m	m	
7	selection	A.5.3.16	m	m	
8	CommonArguments	A.5.3.13	m	m	
9	ChainingResults	A.5.3.22	m	m	
10	SearchResult		m	m	
11	searchInfo		m	m	
12	DistinguishedName		m	m	
13	entries	A.5.3.17	m	m	
14	partialOutcomeQualifier	A.5.3.6.13	m	m	
15	CommonResults	A.5.3.14	m	m	
16	uncorrelatedSearchInfo	A.5.3.7.10	m	m	

A.5.3.8 ChainedAddEntry Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	ChainingArguments	A.5.3.21	m	m	
2	AddEntryArgument		m	m	
3	object		m	m	
4	entry		m	m	
5	CommonArguments	A.5.3.13	m	m	
6	ChainingResults	A.5.3.22	m	m	
7	AddEntryResult		m	m	

A.5.3.9 ChainedRemoveEntry Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	ChainingArguments	A.5.3.21	m	m	
2	RemoveEntryArgument		m	m	
3	object		m	m	
4	CommonArguments	A.5.3.13	m	m	
5	ChainingResults	A.5.3.22	m	m	
6	RemoveEntryResult		m	m	

A.5.3.10 ChainedModifyEntry Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer		Supported Values and Notes
			D	P	
1	ChainingArguments	A.5.3.21	m	m	
2	ModifyEntryArgument		m	m	
3	object		m	m	
4	changes		m	m	
5	addAttribute		m	m	
6	removeAttribute		m	m	
7	addValues		m	m	
8	removeValues		m	m	
9	CommonArguments	A.5.3.13	m	m	
10	ChainingResults	A.5.3.22	m	m	
11	ModifyEntryResult		m	m	

A.5.3.11 ChainedModifyRDN Protocol Elements

Item No	Protocol Element/Parameter	Reference	Performer		Supported Values and Notes
			D	P	
1	ChainingArguments	A.5.3.21	m	m	
2	ModifyRDNArgument		m	m	
3	object		m	m	
4	newRDN		m	m	
5	deleteOldRDN		m	m	
9	CommonArguments	A.5.3.13	m	m	
10	ChainingResults	A.5.3.22	m	m	
11	ModifyRDNResult		m	m	

A.5.3.12 Errors and Parameters

Item No	Protocol Element/Parameter	Reference	Performer		Supported Values and Notes
			D	P	
1	Abandoned		m	m	
2	AbandonFailed		m	m	
3	problem		m	m	
4	operation		m	m	
5	AttributeError		m	m	
6	object		m	m	
7	problems		m	m	
8	problem		m	m	
9	type		m	m	
10	value		m	m	
11	NameError		m	m	
12	problem		m	m	
13	matched		m	m	
14	DSAReferral		m	m	
15	ContinuationReference	A.5.3.20	m	m	
16	contextPrefix		m	m	
17	SecurityError		m	m	
18	problem		m	m	
19	ServiceError		m	m	
20	problem		m	m	
21	UpdateError		m	m	
22	problem		m	m	

A.5.3.13 Common Arguments Elements

Item No	Protocol Element/Parameter	Reference	Performer		Supported Values and Notes
			D	P	
1	ServiceControls	A.5.3.15	m	m	
2	SecurityParameters		c13	i	
3	requestor		o	i	
4	OperationProgress		m	m	
5	nameResolutionPhase		m	m	
6	nextRDNToBeResolved		m	m	
7	aliasedRDNs		m	m	
8	criticalExtensions		o	m	

c13: if answer to A.4.13 is "Yes" then m else o.

A.5.3.14 Common Results Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	SecurityParameters		c14	i	
2	performer		o	i	
3	aliasDereferenced		m	m	

c14: if answer to A.4.15 is "Yes" then m else o.

A.5.3.15 Service Controls

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	options		m	m	
2	priority		m	m	
3	timeLimit		m	m	
4	sizeLimit		m	m	
5	scopeOfReferral		m	m	

A.5.3.16 Entry Information Selection

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	attributeTypes		m	m	
2	allAttributes		m	m	
3	select		m	m	
4	infoTypes		m	m	

A.5.3.17 Entry Information

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	DistinguishedName		m	m	
2	fromEntry		m	m	
3	SET OF CHOICE		m	m	
4	AttributeType		m	m	
5	Attribute		m	m	

A.5.3.18 Filter Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	item	A.5.3.19	m	m	
2	and	A.5.3.18	m	m	
3	or	A.5.3.18	m	m	
4	not	A.5.3.18	m	m	

A.5.3.19 Filter Item Elements

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	equality		m	m	
2	substrings		m	m	
3	type		m	m	
4	strings		m	m	
5	initial		m	m	
6	any		m	m	
7	final		m	m	
8	greaterOrEqual		m	m	
9	lessOrEqual		m	m	
10	present		m	m	
11	approximateMatch		m	m	

A.5.3.20 Continuation Reference

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	targetObject		m	m	
2	aliasedRDNs		m	m	
3	operationProgress		m	m	
4	nameResolutionPhase		m	m	
5	nextRDNToBeResolved		m	m	
6	rdnsResolved		m	m	
7	referenceType		m	m	
8	accessPoints		m	m	
9	ae-title		m	m	
10	address		m	m	
11	entryOnly		m	m	

A.5.3.21 Chaining Arguments

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	originator		m	m	
2	targetObject		m	m	
3	operationProgress		m	m	
4	nameResolutionPhase		m	m	
5	nextRDNToBeResolved		m	m	
6	traceInformation	A.5.3.24	m	m	
7	aliasDereferenced		m	m	
8	aliasedRDNs		m	m	
9	returnCrossRefs		m	m	
10	entryOnly		m	m	
11	referenceType		m	m	
12	info		o	i	
13	timeLimit		m	m	
14	SecurityParameters		c13	i	

A.5.3.22 Chaining Results

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	info		m	m	
2	crossReferences	A.5.3.23	m	m	
3	SecurityParameters		c14	i	

A.5.3.23 CrossReference

Item No	Protocol Element/Parameter	Reference	Performer D	Performer P	Supported Values and Notes
1	contextPrefix		m	m	
2	accessPoint		m	m	
3	ae-title		m	m	
4	address		m	m	

A.5.3.24 Trace Information

Item No	Protocol Element/Parameter	Reference	Performer		Supported Values and Notes
			D	P	
1	TraceItem		m	m	
2	dsa		m	m	
3	targetObject		m	m	
4	operationProgress		m	m	
5	nameResolutionPhase		m	m	
6	nextRDNToBeResolved		m	m	