INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 15125-7

First edition
1998-11-15

Information technology — International Standardized Profiles ADYnn — OSI Directory —

Part 7:
ADY43 — DSA to DSA Authentication

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

Partie 7: ADY43 — Authentification de DSA à DSA

Reference number
ISO/IEC ISP 15125-7:1998(E)

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Contents

1 Scope 1

1.1 General 1
1.2 Position within the taxonomy 1
1.3 Scenario 2

2 Normative references 2

2.1 Paired CCITT Recommendations | International Standards equivalent in technical content 2
2.2 Normative Amendments and Technical Corrigenda 3
2.3 Additional normative references 4

3 Definitions 4

3.1 General 4
3.2 Support Level 5

4 Abbreviations 5

5 Conformance 6

5.1 Static Conformance Requirements 7

6 Procedures 12

6.1 Introduction 12
6.2 Two-way Authentication 12
6.3 Random Numbers 14
6.4 Distinguished Encoding Rules 14
6.5 Simple Unprotected Authentication 15
6.6 Simple Protected Authentication 16
6.7 Strong Authentication in the DSA, DOP, or DISP Bind 17
6.8 Signed DSP or DISP operations 18
6.9 Merging signed results 20
6.10 Certificates 20
6.11 Access Control Identity in the Distributed Directory 21
6.12 Error Handling 23

Annex A (normative) **Profiles Requirements List** 26

Annex B (normative) **Amendments and Technical Corrigenda** 43

Annex C (informative) **Commonly Used Algorithms** 44

© ISO/IEC 1998

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and micro-film, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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 15125-7 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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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 ADY43 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 manner in which DSAs are to behave when authenticating each other using simple unprotected or protected authentication or strong authentication, or when using signed DSP or DISP operations.

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.

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Information technology — International Standardized Profiles ADYnn — OSI Directory — Part 7: ADY43 — DSA to DSA Authentication

1 Scope

1.1 General

The Directory Standards define various means of authentication between DUAs and DSAs and also between two DSAs.

As specified by the Directory Standards, the means of authentication at the time of establishment of an association (i.e. at Bind-time), for DAP, DSP, DOP, and DISP, are:

- None–no credentials are supplied
- Simple unprotected authentication, with or without password: each authenticating party supplies a name and optionally a password
- Simple protected authentication: each authenticating party supplies a name and a password whose information is transmitted in hashed form to preserve password confidentiality and to prevent replay
- Strong authentication in which each authenticating party supplies a token signed with a digital signature which can be verified by the other

The Directory standards also permit other forms of authentication at the time of association establishment, whereby credentials are passed by "external" elements. Such means are outside the scope of this part of ISO/IEC ISP 15125.

In addition, the Directory Standards define a method whereby certain DAP, DSP, or DISP enquiries and results can be authenticated and sealed by means of a digital signature.[1]

This part of ISO/IEC ISP 15125 profiles:

- Simple unprotected authentication, with or without password, between two DSAs
- Simple protected authentication between two DSAs
- Strong authentication between two DSAs
- Signed DSP and DISP invokes and return-results exchanged between two DSAs

It also profiles the behaviour of a DSA in combining signed uncorrelated list and search information as returned by DSP return results.

It also profiles the use of the **originator** element to convey information about the originator of the DAP association within which an operation is created.

Since there are many options and possibilities in the use of these techniques, this part of ISO/IEC ISP 15125 does not attempt to specify how each facility shall be used. This results in certain features (e.g. the double-hashing technique described in the last paragraph of [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] subclause 6.2) being considered as out-of-scope.

DSAs are also permitted to bind to each other using no credentials at all. However, this possibility is 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 “ADY43 — DSA to DSA Authentication”.

---

[1]When operations are not signed, authentication from user to DSA occurs only when the DUA binds to a DSA using DAP. Thereafter, the authenticated identity of the originator of an operation is passed from one DSA to another as appropriate. There is no obligation on a receiving DSA to regard the originator value supplied as valid, and in particular, an originator value supplied over a DSP association can be treated as if no authentication had taken place. The Directory Standards also permit DSAs to perform an assessment of "Authentication-Level" to reflect the perceived reliability of the authentication method (9594-2 Subclause 16.4.2.3).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1.3 Scenario

This part of ISO/IEC ISP 15125 profiles simple and strong authentication between DSAs (BIND dialogue in Figure 1) in the establishment of DSP, DOP and DISP Associations, and signed operations between DSAs (OPERATION dialogue in Figure 1) within these Associations. It also profiles the handling of uncorrelated list and search results (see right-hand-side of diagram) within DSP (there is no analogue for this within DOP and DISP).

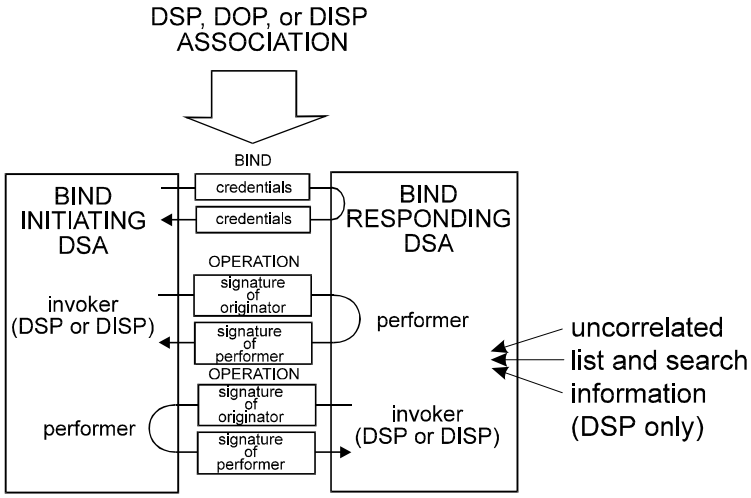

Figure 1 — Scenario

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 CCITT 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 9594-9 : 1995 | ITU-T Rec. X.525 (1993)], *Information technology — Open Systems Interconnection — The Directory: Replication.*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

[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 1 to Recommendation X.525 (1993) | ISO/IEC 9594-9:1995 (addressing DRs 9594/097, 099, 123)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- 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 13248-3:—[3], *Information technology — Open Systems Interconnection — Protocol Implementation Conformance Statement (PICS) Proforma — Part 3: Operational Binding Management Protocol.*
- ISO/IEC 13248-4:—[3], *Information technology — Open Systems Interconnection — Protocol Implementation Conformance Statement (PICS) Proforma — Part 4: Directory Information Shadowing 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 clauses or subclauses within the standards documents, references are listed in Table 1below. The "Part" reference refers to the part number within [ISO/IEC 9594 : 1995 | ITU-T Rec. X.500 (1993)] (see also clause 2).

Table 1 — Definitions and references

Term	Part	Reference
Authentication-level	2	Subclause 16.4.2.3
Backward certificate	8	Clause 8
Certificate	8	Clause 8
Certificate Revocation List	8	Subclause 11.2
Certification path	8	Clause 8
Digital signature	8	Clause 9
Directory Information Shadowing Protocol	9	Clauses 10 to 12
Directory Operational Binding Management Protocol	2	Clauses 21 to 24
Distinguished Encoding Rules	8	Clause 9 last para
Forward certificate	8	Clause 8
Key pair	8	Clause 7
One-way authentication	8	Subclause 10.2
Originator	4	Subclause 10.3
Signed operation	4	Subclause 12.1

[2]This specification defines Version 1 Certificates.

[3] To be published.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Term	Part	Reference
Simple protected authentication	8	Subclause 6.2
Simple unprotected authentication	3	Subclause 8.1.2
Strong authentication	8	Section 3
Strong hash function	8	Annex E
Two-way authentication	8	Subclause 10.3
Uncorrelated list information	3	Subclause 10.1.3
Uncorrelated search information	3	Subclause 10.2.3

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

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.

A similar definition applies to Signed DISP operations

Certificate Issuer — The name that is used as the value of **Certificate.issuer** in a certificate (normally the name of a Certification Authority)

Policy CA — The topmost CA in the CA hierarchy within an organisation

Trusted CA — A CA whose public key has been acquired in a trusted manner (for example, by a DSA)

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

A feature is supported by a DSA implementation if the DSA is able to process the feature in accordance with the base standard or as specified in this part of ISO/IEC ISP 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 Out of scope: i: Out of scope requirement for support

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

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

BER — Basic Encoding Rules (ASN.1)

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

CA	Certification Authority
CCITT	International Telegraph and Telephone Consultative Committee
CRL	Certificate revocation list
DAP	Directory Access Protocol
DER	Distinguished Encoding Rules
DIB	Directory Information Base
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DMD	Directory Management Domain
DOP	Directory Operational Binding Management Protocol
DSA	Directory System Agent
DSP	Directory System Protocol
DUA	Directory User Agent
IEC	International Electrotechnical Commission
IPRL	ISPICS Requirements List
ISO	International Organisation for Standardisation
ISP	International Standardized Profile
ISPICS	ISP Implementation Conformance Statement
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication standardisation sector
IUT	Implementation under test
NSSR	Non-specific Subordinate Reference
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PKCS	Public Key Cryptosystem
POQ	Partial outcome qualifier
PRL	Profile Requirements List
RDN	Relative Distinguished Name
ROSE	Remote Operations Service Element

5 Conformance

The Directory Standards state only limited conformance requirements within the scope of this part of ISO/IEC ISP 15125:

- Statement requirements in [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)] subclause 9.2.1 (e) (as amended by Technical Corrigenda)
- The Protocol specifications specify the use of particular elements concerned with the process of simple protected authentication, strong authentication, or digital signatures, but in a number of cases the contents of actual values are left incompletely specified.

The conformance requirements of this part of ISO/IEC ISP 15125 extend and clarify these conformance requirements, when appropriate.

DSAs claiming conformance with this part of ISO/IEC ISP 15125 shall support at least one of the following, for each of the protocols DSP, DOP, or DISP for which support is claimed:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- Simple Unprotected Authentication as specified in subclause 5.1.1, either in the responder role alone, or in both initiator and responder roles
- Simple Protected Authentication as specified in subclause 5.1.2, either in the responder role alone, or in both initiator and responder roles, together with Simple Unprotected Authentication capability
- Strong Authentication in the DSA, DOP or DISP Bind as specified in subclause 5.1.3, either in the responder role alone, or in both initiator and responder roles, together with Simple Unprotected Authentication capability
- Signed DSP or DISP operations as specified in subclause 5.1.4, either in the invoker role alone, or in both invoker and performer roles, together with Strong Authentication capability

DSAs claiming conformance with this part of ISO/IEC ISP 15125 for Signed DSP or DISP operations shall also support unsigned DSP or DISP operations as appropriate.

DSAs claiming conformance with this part of ISO/IEC ISP 15125 for Signed DSP or DISP operations shall also support Strong Authentication in the DSA, DOP, or DISP Bind.

DSAs claiming conformance with this part of ISO/IEC ISP 15125 for Simple Protected or Strong Authentication in the DSA, DOP, or DISP Bind shall comply with the error-handling procedures specified in subclause 6.12.1 when carrying out Simple Protected or Strong Authentication in the DSA, DOP, or DISP Bind.

DSAs claiming conformance with this part of ISO/IEC ISP 15125 for signed DSP or DISP operations shall comply with the error-handling procedures specified in subclause 6.12.2.

DSAs claiming conformance with this part of ISO/IEC ISP 15125 as an invoker for DSP operations are in all cases required to be conformant with ISP ADY22.

DSAs claiming conformance with this part of ISO/IEC ISP 15125 for Simple Protected or Strong Authentication for DSP, DOP, or DISP, or claiming conformance for signed DSP or DISP operations, may optionally be able to claim conformance to two-way authentication. If they do claim conformance to two-way authentication, they shall be able to demonstrate conformance to the corresponding procedures of subclause 6.2.

5.1 Static Conformance Requirements

5.1.1 Simple Unprotected Authentication

For each of DSP, DOP or DISP for which a DSA claims support of Simple Unprotected Authentication, in accordance with this part of ISO/IEC ISP 15125, the DSA shall be capable of:

1. As responder, configuration to require Simple Unprotected Authentication, with password, as the sole means of authentication that can be accepted[4]
2. As initiator, initiating a Bind to another DSA using simple unprotected authentication in accordance with the procedures specified in subclause 6.5.1
3. As responder, accepting, and validating simple unprotected credentials generated by the initiator of a Bind, in accordance with the procedures specified in subclause 6.5.2, and creating return credentials in accordance with the procedures specified in subclause 6.5.2 or responding with an appropriate Bind Error.
4. As initiator, accepting, and validating simple unprotected credentials generated by the responder to a Bind, in accordance with the procedures specified in subclause 6.5.3, and responding with an Unbind or Abort if the credentials are invalid.
5. As initiator or as responder, acquiring or holding the passwords of other DSAs to which Simple Unprotected Authentication for Bind is required, without requiring any Directory operation.

A conformant DSA may nevertheless be configurable to accept any or all of the forms of authentication permitted by this part of ISO/IEC ISP 15125.

5.1.2 Simple Protected Authentication

For each of DSP, DOP or DISP for which a DSA claims support of Simple Protected Authentication in accordance with this part of ISO/IEC ISP 15125, the DSA shall be capable of:

---

[4] The use of name without password may be taken as an acceptable form of authentication, despite the lack of corroboration, when authentication is carried in some way by trusted software outside the scope of normal Directory procedures.

--`,,``,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1. As responder, configuration to require Simple Protected Authentication as the sole means of authentication that can be accepted.
2. As initiator, initiating a Bind to another DSA using simple protected authentication in accordance with the procedures specified in subclause 6.6.1
3. As responder, accepting, and validating simple protected credentials generated by the initiator of a Bind, in accordance with the procedures specified in subclause 6.6.2, and creating return credentials in accordance with the procedures specified in subclause 6.6.2 or responding with an appropriate Bind Error.
4. As initiator, accepting, and validating simple protected credentials generated by the responder to a Bind, in accordance with the procedures specified in subclause 6.6.3, and responding with an Unbind or Abort if the credentials are invalid.
5. As initiator or as responder, acquiring or holding the passwords of other DSAs to which Simple Protected Authentication for Bind is required, without requiring any Directory operation.
6. As initiator or as responder, configuring an expiry time for the acceptability of a protected password between 1 and 900 seconds with a granularity of 1 second or better (i.e. 1 sec, 2 sec, 3 sec, ... 900 sec).[5]

   Note. Configuration capability outside these limits is optional.

The support of Simple Protected Authentication using **time2** and **random2** is outside the scope of this part of ISO/IEC ISP 15125.

These requirements also do not preclude DSAs supporting *additionally* the use of procedures other than those specified in the referenced clauses and subclauses. In particular, DSAs may support procedures which differ only in the order of carrying out the steps.

A conformant DSA may nevertheless be configurable to accept additionally any or all of the forms of authentication permitted by this part of ISO/IEC ISP 15125.

5.1.3 Strong Authentication in the DSP, DOP, or DISP Binds

For each of DSP, DOP or DISP for which a DSA claims support of Strong Authentication, in accordance with this part of ISO/IEC ISP 15125, the DSA shall be capable of:

1. As responder, configuration to require Strong Authentication as the sole means of authentication that can be accepted.
2. As initiator, initiating a Bind with another DSA using strong credentials in accordance with the procedures specified in subclause 6.7.1
3. As responder, accepting and validating strong credentials generated by the initiator of a Bind, in accordance with the procedures specified in subclause 6.7.2; creating return strong credentials in accordance with the procedures specified in subclause 6.7.2 and responding with an appropriate Bind Error in accordance with the procedures specified in subclause 6.12.1.
4. As initiator, accepting, and validating strong credentials generated by the responder to a Bind, in accordance with the procedures specified in subclause 6.7.3, and responding with an Unbind or Abort if the credentials are invalid.
5. As initiator or as responder, EITHER acquiring or holding the public keys or certificates of other DSAs to or from which Binds are to be possible, OR acquiring or holding the public keys or certificates of the issuers of certificates for such other DSAs, prior to Strong Authentication in the Bind, without requiring any Directory operation.

   Notes.

   a) A DSA establishing a DSP Bind cannot necessarily require the credentials of the other DSA to be accessible by means of a Directory operation, since until an association exists, the credentials will sometimes be unavailable using Directory operations.

   b) A possible way of handling this requirement is for a DSA to support within themselves a list of certificates for potential correspondent DSAs using convenient storage means.

   c) Another way of resolving this issue is to support a list of certificate issuers in respect of potential correspondent DSAs. This, however, would require a DSA that was to bind to another to supply a certificate. This is the reason for requirement 6.

[5] The interval actually chosen should normally be the shortest interval guaranteed to be achieved between construction of the protocol and its analysis, taking into account network delays.

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

d) A conformance test could take the following form:

Create a new key pair and certificate to represent the Tester, and supply the certificate to the IUT.

Require that the certificate be pre-installed or otherwise made available to the DSA

Subsequently require that the bind operation be carried out without permitting any form of Directory operation.

6. As initiator or as responder, configuration to pass a certificate within the **BindArgument** or **BindResult**, for each such protocol element supported.

   Note. This requirement ensures interoperability of a DSA that can only hold an issuer's certificate.

7. As initiator or as responder, the capability of automatically acquiring and validating both (i) CA Certificates and (ii) Revocation Lists relevant to any certificates held, together with the capability of terminating a DSP, DOP or DISP association in the event that such a certificate is found to be invalid.[6] The termination can be by an abort or unbind. It is not required that, for each bind, the certificates used need to be validated.

   Notes.

   a) The requirement to validate the credentials by reference to pre-stored certificates is specified in subclause 6.7.2.

   b) There is no requirement that the CA Certificate and Revocation List validation process should take place before the establishment of a DSP association, since in some cases this will not be possible (e.g. the DSA initiating a bind may hold the CA Certificate and revocations lists relevant to certificate validation).

   c) The establishment of credentials prior to binding needs to be done bilaterally using adequately secure procedures.

   c) To support these requirements, the requirement 8 and 9 below are added.

8. DSAs claiming support of strong authentication for DSP, DOP or DISP shall be capable of holding a certificate (or a public key) for a trusted CA to enable those CA certificates and revocation lists identified in 7 to be validated

9. DSAs claiming conformance to strong authentication for DSP, DOP or DISP shall be capable of automatic validation of chains of user and CA certificates when the CA relationships conform to the topology specified in subclause 5.1.6.3.

10. DSAs supporting strong authentication for DOP or DISP shall support DSP, with or without the capability of strong authentication.

    Note. This permits validation of the certificates using Directory means. However, the use of DSP may not always be required.

These requirements also do not preclude DSAs supporting *additionally* the use of procedures other than those specified in the referenced clauses and subclauses. In particular, DSAs may support procedures which differ only in the order of carrying out the steps.

5.1.4 Signed DSP or DISP operations

For each of DSP or DISP for which a DSA claims support of signed operations, in accordance with this part of ISO/IEC ISP 15125, the DSA shall be capable of:

1. As invoker:

   - Configuration to sign all invokes in a particular association.[7]
   - Initiating a signed invoke in accordance with the procedures specified in subclause 6.8.1.
   - Accepting and validating the signature of a signed return result, and discarding the result when the signature is invalid, and handling the error in accordance with the procedures of subclause 6.12.2, including termination of the association.

   Note. This last requirement can be conformance tested by the following steps:

[6] For example, a certificate's issuer's signature is found to be invalid by reference to a CA certificate acquired in this way, or a certificate is revoked by reference to a revocation list.

[7] All DSP operations can be signed (except abandons - see last sentence of Clause 12 of [ISO/IEC 9594-4 : 1993 | ITU-T Rec. X.518 (1993)]). Similarly, all DSP return-results can be signed, even NULL returns to update operations. No error can be signed.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The tester returns a valid signed result: this must be forwarded (e.g. by DAP)

In the same test and with an identical operation, the tester returns an invalid signed result: this must not be forwarded.; an error must be returned instead, in accordance with subclause 6.12.2.2.

2. As performer:

- Configuration to require all invokes to be signed.
- Configuration to respond to a signed invoke with a signed return-result, and to respond to a signed operation with an unsigned return-result, if requested by means of an incoming **protectionRequest** element.
- Accepting, and validating the signature of a signed DSP or DISP invoke, and responding with a signed return result in accordance with the procedures specified in subclause 6.5.2, or generating an appropriate DSP or DISP Error if the signature is invalid, in accordance with the procedures of subclause 6.7.2.

3. As invoker or as performer:

- Validating (i) CA Certificates and (ii) Revocation Lists, as necessary to validate signatures, in accordance with the static requirements of subclause 5.1.6 and the procedures defined in subclause 6.6.
- Terminating the DSP or DISP association (as appropriate) when an invalid signature is found.[8]

Notes.

a) Although evaluation of the signature of each signed operation against pre-evaluated certificates is required, there is no requirement that the CA Certificate and Revocation List validation process should be fully carried out in respect of each DSP or DISP operation. In fact, doing so would multiply the traffic by a factor of at least 3 (the original operation plus at least one read operation initiated by the Responder to obtain a CA Certificate a Revocation Lists, plus at least one similar operation initiated by the Invoker).

b) It would be reasonable to carry out such checks periodically (e.g. once every hour, or at times when new revocation lists are known to have been posted), and to rely on earlier pre-evaluations of certificate chains.

Note. A conformance test for this could cause a certificate to be revoked, and to require the DSA to act accordingly after not later than some agreed period.

5.1.5 Signed Results

DSAs claiming conformance to this part of ISO/IEC ISP 15125 in supporting signed DSP operations shall be capable of signing Directory Abstract Service return results, as permitted by the protocol and defined in [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] clauses or subclauses 7.10, 9, 10, and 11, and shall also be capable of signing the aggregation of locally generated list results, search results and uncorrelated list or search results from other DSAs in accordance with clause 10, leaving intact the signatures (if any) on the latter.

5.1.6 Certificates and Revocation Lists

5.1.6.1 Certificates

DSAs claiming conformance to this part of ISO/IEC ISP 15125 in supporting Strong Authentication or Signed DSP or DISP operations shall support Certificates in accordance with Version 3 as defined by [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)], as amended by the extension mechanism of Corrigendum 2 to [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] (except that there is no requirement to support any Version 3 extension), and in accordance with subclause 6.10.3 (Certificate Processing) below.

5.1.6.2 Revocation Lists

DSAs claiming conformance to this part of ISO/IEC ISP 15125 in supporting Strong Authentication or Signed DSP or DISP operations shall support Revocation Lists in accordance with the definitions of [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)], as amended by the extension mechanism of Corrigendum 3 to [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] and in accordance with subclause 6.10.4 below.

Notes

1. If an extension is defined as critical, DSAs conformant to this part of ISO/IEC ISP 15125 shall handle it as specified in subclause 6.6.4.

[8] A DSP or DISP association with a bad signature on a signed operation is suspect, so that being able to close down the association is an important requirement.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

2. The '88 form of CRL was amended, outside the scope of extensibility, to correct certain problems. It therefore seems appropriate to mandate the '93 form.

5.1.6.3 Certification Hierarchy Topology

A DSA's signature is provided as credentials (bottom right of the Figure 2) for evaluation by reference to the signing DSA's certificate. This signature may be provided in a bind request or result, or as part of a signed invoke or return result. The certificate can be held by the evaluating DSA, or otherwise made available to the evaluating DSA in the same protocol exchange, or in different ones.

DSAs shall be able to support a certification topology whereby validation of all correspondent DSAs shall be possible in accordance with the following arrangements (see Figure 2). The validation referred to here is the full validation by reference to all relevant certificates and revocation lists, and not the validation of credentials by means of pre-stored certificates, etc.

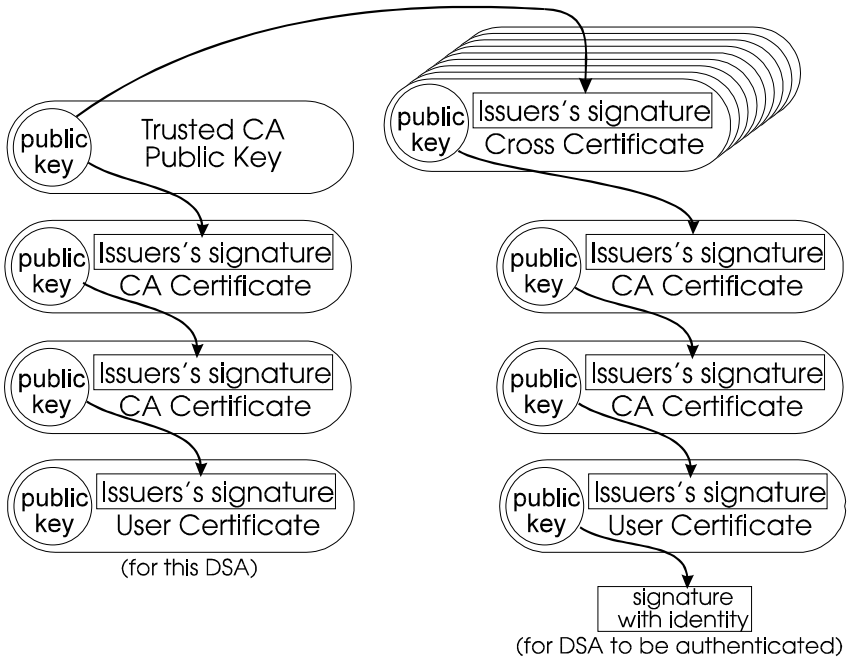

Figure 2 — Certificate Hierarchies and evaluation paths

There are two arrangements of CA that must be supported:

1. The DSA holds the public key for at least one trusted CA (top left of the figure - see definition in 3.1), which can be used to validate certificates for other DSAs which contain this CA in their own certification hierarchy (left side of the figure).

   Note. This CA may be, but need not be, the Policy CA for the organisation that owns the DSA.

2. The entry for this trusted CA may hold cross-certificates (top right of the figure) which can be used to validate certificates for other DSAs in a certification hierarchy which is directly referenced by such cross-certificates.

The procedures for full validation in accordance with this topology are as follows (see Figure 3 which uses precisely the same graphic elements as Figure 2, but omits the captions on the elements):

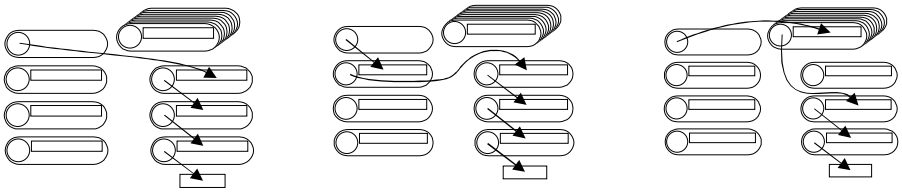

Figure 3 — Validation strategies

1. Validate the signature of the user by reference to the public key held in the user's certificate; validate the issuer's signature for this certificate by reference to the public key held in the issuer's certificate, and so on, where the issuer

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

of one of the certificates encountered in this way is the trusted CA whose public key is held; establish that no such certificate has been revoked. (In the left hand side of figure, the first known issuer is the trusted CA; in the centre figure, a known issuer is encountered earlier).

2. As above, except that the trusted CA is not in the same hierarchy as the user; however the issuer of one of the certificates encountered in this way has its public key supplied in the set of cross-certificates issued by the trusted CA whose public key is held (right hand side of the figure).

If the top of the certification hierarchy for the credentials signature is reached without encountering a CA whose public key is known in this manner, or if one of the required certificates is unavailable or has been revoked, the evaluation may fail.

Notes.

1. There are many possibilities for practical topologies, and this requirement in no way obligates the use of this particular topology. Other topologies may be supported.

2. In particular, some topologies demand that the CA hierarchy must be reflected in the DIT hierarchy. However, this is not compatible with some practical naming strategies, for example those in which two parts of a company are placed under different country entries. CAs for the two parts of the tree cannot then have a hierarchical relationship. DSAs compatible with this profile are therefore not permitted to assume that CAs have a hierarchical relationship.

6 Procedures

6.1 Introduction

DSAs claiming conformance to this part of ISO/IEC ISP 15125 shall be capable of carrying out the procedures specified below, as specified by other static conformance requirements specified above.

DSAs are permitted to use a DSP association in particular in either direction (i.e. the invoker of a operation on a DSP association can be different to the DSA that initiated the bind).

Notes

1. However, DSAs are entitled to refuse to use an inadequately authenticated association within which to invoke new operations, and may attempt to create a new, securer association for this purpose. The use of anonymous DSP associations by other than the initiator appears to be poor practice.

2. Strong authentication can only work satisfactorily when there is adequate synchronisation between the creator and the valuator of a signature. Achieving synchronisation may be possible using a trusted synchronisation service, but other techniques are possible. Note that if the means of synchronising time is vulnerable to attack or correct time synchronisation is lost then the authentication mechanism can become vulnerable to replay attack. However, no conformance requirement for synchronisation is made in this part of ISO/IEC ISP 15125.

6.2 Two-way Authentication

DSAs supporting Simple Protected or Strong Authentication for DSP, DOP, or DISP, or signed DSP or DISP operations, may optionally be able to claim conformance to two-way authentication as opposed to two one-way authentications.[9] The difference between these in the present context is that, for two-way authentication, the initiator's (or invoker's) random number is returned by the responder (or performer) *in addition to* a random number of the responder's (or performer's) own choosing. With two one-way authentications, the only random number returned is a random number of the responder's (or performer's) own choosing; there is no correlation with the initiator's (or invoker's) random number.

[9] Two-way authentication is valid both in binds and in signed operations.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

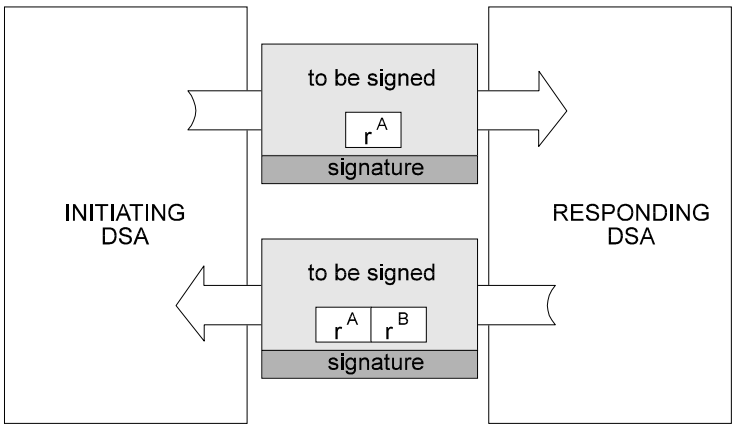

Figure 4 — Two-way authentication

The choice of two-way authentication (Figure 4) as opposed to two one-way authentications is a matter of authentication policy between pairs of DSAs, and could vary from protocol to protocol. This part of ISO/IEC ISP 15125 makes no recommendations as to when two-way authentication should be applied, or how DSAs should enter the necessary bilateral agreements.

When two-way authentication is being used, the initiator (or invoker) shall check that the initiator's (or invoker's) random number, as returned, is identical to the value as initially despatched.

The ASN.1 elements **SimpleCredentials.validity.random1**, **StrongCredentials.bind-token.random** and **SecurityParameters.random**, each of which is defined as having **BIT STRING** syntax can be used to carry the information necessary for two-way authentication. The initiator supplies a random number (call it r^A) and may wish to signal that two-way authentication is to be used. The responder returns both r^A and r^B. All this information needs to be placed in the **random1** or **random** elements referred to.

DSAs claiming support for two-way authentication shall, when two-way authentication is being applied:[10]

1. As initiator (or invoker), encode the initiator/invoker-supplied random number r^A (a **BIT STRING**) in the form of a **BIT STRING** containing the value r^A, encoded most significant bit first, potentially with leading 0's (i.e. it is legitimate to round off the bits to 8-bit boundaries).
2. As responder (or performer), encode the random number r^B (a **BIT STRING**) in the form of a **BIT STRING** containing the simple concatenation of r^A and r^B. For example, if r^A is $1A3C50_{16}$ and r^B is $03E660_{16}$, then the resulting bitstring is the $1A3C5003E660_{16}$, again with most significant bit first; r^A being retained as is, and r^B potentially having leading 0's.
3. As initiator (or invoker), declare the returned credentials as invalid if the returning **random1** or **random** bitstring is not the same as the outgoing bitstring with additional bits concatenated.

The responder must determine from bilateral agreement with the initiator that two way authentication is required, as this cannot be determined from the incoming protocol.

The responding DSA shall use the presence of the **RandomAWithOptionalRandomB** encoding within the **random1**/**random** element bitstrings as signalling a request for two-way authentication. That is: DSAs claiming support for two-way authentication shall respond as above if the **random1**/**random** element contains ASN.1 encoding as specified.

When two-way authentication is not used, a DSA is not required to conform to the encoding rules of two-way authentication as defined above. If a responder receives a random number value which is not encoded as described above, it can take action appropriate to an attempt to initiate authentication that was not two-way.

> Note. Credentials are made insensitive in this way to an attack in which an impostor DSA Z observes another DSA Y responding to an association initiated by a DSA X; it subsequently intercepts a new association request and replays the credentials, thereby purporting to be DSA Y. Another form of attack which is protected against is one in which an impostor DSA Z observes another DSA Y responding to an association initiated by a DSA X; it subsequently intercepts a new association request from another DSA X' to Y, and replays the observed credentials, thereby purporting to be DSA Y.

[10] The Directory Standards do not define precisely how two way authentication is done. The method defined above is one of several choices. Future versions may specify alternative encodings.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

(When using simple protected authentication, an attack of this kind can also be protected against by giving a DSA different passwords for each other DSA to which it habitually binds.)

6.3 Random Numbers

The random numbers used to derive **SimpleCredentials.validity.random1** in the case of Simple Protected Credentials, **StrongCredentials.bind-token.SIGNED.random** in the case of Strong Credentials in the bind or **SecurityParameters.random** for signed operations, shall not repeat regularly within 2^{32}-1 iterations.

6.4 Distinguished Encoding Rules

The encoding rules for DER (Distinguished Encoding Rules) are defined in [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] clause 9. However, these rules make the presumption that the mechanism carrying out the encoding are aware of the precise syntax of what is encoded. This is not the case for the Directory, since DSAs must handle encodings prepared by other entities, and these encoding may contain (A) unknown extensions, (B) values encoded in accordance with locally unknown syntaxes, and (C) **info** and other elements encoded with an unknown **ANY** syntax.

When the DER rules cannot be completely applied, for these reasons, the rules shall be applied in a form modified as follows (using the original reference letters):

a) As in X.509;

b) for string types which are identifiable as such by the ASN.1 encoding or by knowledge of the syntax, the constructed form of encoding shall not be used; in other cases, the form of the syntax shall remain as supplied to the DSA by the originating entity, modified by other of these rules as necessary;

c) if a value of a type is its default value, where identifiable as such by knowledge of the syntax, it shall be absent; in other cases, the value shall remain (i.e. as supplied to the DSA by the originating entity, modified by other of these rules as necessary);

d) the components of a Set type (but not a Set-of type), where identifiable as such by knowledge of the syntax[11], shall be encoded in ascending order of their tag value; where absence of knowledge of the syntax makes it impossible to distinguish between a Set type and a Set-of type, the Set-of type encoding rule, as defined below shall be used; in other cases, the value shall remain (i.e. as supplied to the DSA by the originating entity, modified by other of these rules as necessary);

e) the components of a Set-of type (but not a Set type), where identifiable as such by knowledge of the syntax, shall be encoded in ascending order of their octet value; this rule shall also apply where absence of knowledge of the syntax makes it impossible to distinguish between a Set type and a Set-of type; in other cases, the value shall remain (i.e. as supplied to the DSA by the originating entity, modified by other of these rules as necessary);

f) if for a value of Boolean type, which is identifiable as such by the ASN.1 encoding or by knowledge of the syntax, the value is true, the encoding shall have its contents octet set to "FF"$_{16}$; in other cases, the form of the syntax shall remain as supplied to the DSA by the originating entity, modified by other of these rules as necessary;

g) if for a value of Bit String type, which is identifiable as such by the ASN.1 encoding or by knowledge of the syntax, each of the unused bits in the final octet of the encoding, if there are any, shall be set to zero; in other cases, the form of the syntax shall remain as supplied to the DSA by the originating entity, modified by other of these rules as necessary;

h) for a value of Real type, which is identifiable as such by the ASN.1 encoding or by knowledge of the syntax, bases 8, 10, and 16 shall not be used, and the binary scaling factor shall be zero; in other cases, the form of the syntax shall remain as supplied to the DSA by the originating entity, modified by other of these rules as necessary.

Values of UTCTime type should always use the form in which seconds are present. In any case, the form of the syntax shall remain as supplied to the DSA by the originating entity, modified by other of these rules as necessary.

[11] Where the syntax is unknown, it is impossible to distinguish between a Set and a Set-of type. In addition, implicit encodings may be Set or Set-of types, but cannot be recognised as such by the DSA if the encoding is unknown

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The application of the more general rule e) in place of rule d) produces exactly the same result in all currently known circumstances, and it is acceptable that implementations base their DER encoding on rule e) to cover both situations. [12]

DSAs shall contribute to the accuracy of application of the original rules by using the following rules in their own use of BER encoding:

1. If a value of a type is its default value, it shall be absent.
2. Wherever implicit encoding is used, the encoding shall follow the DER rules at least for the element having the implicit encoding (but not necessarily any elements contained within it).

6.5 Simple Unprotected Authentication

6.5.1 Initiator of the Bind

For a DSA claiming conformance to Simple Unprotected Authentication, the initiator shall be capable of the following procedures: the initiator shall generate **SimpleCredentials** within a **BindArgument** as follows:

- Only **name** and (optionally) **password** shall be present
- The **unprotected** choice for **password** (if present) shall be taken.

6.5.2 Responder to the Bind

If the password is present, the responder to the Bind shall validate the unprotected simple credentials as follows:

- By making use of its own stored knowledge of the initiating DSA's password, the credentials shall be taken as invalid if the two password values, as received and as locally known, are different.

Notes.

1. If the password is absent, a DSA may take as invalid a bind request from a DSA not known to it (e.g. by pre-configuration).
2. This provision does not disallow the use of a trusted password server.

The responding DSA shall be capable of returning simple credentials defined in subclause 6.2.1 in the same form (i.e., if password was present, with **name** and **password** present and taking the **unprotected** choice for **password**; if password was absent, with just **name** present).

If the Initiator's credentials are invalid, or if the Bind Request is rejected, the error procedures specified in subclause 6.7 shall be followed.

6.5.3 Initiator's response to Bind Result

When the password is present, the initiator of the Bind shall validate the incoming protected simple credentials as follows:

- By making use of its own stored knowledge of the responding DSA's password, the credentials shall be taken as invalid if the two password values, as received and as locally known, are different.

If the responder's credentials are invalid, or if the Bind Request is to be rejected, the error procedures specified in subclause 6.7.1 shall be followed.

6.5.4 Response to DSA, DOP, or DISP bind without credentials

A DSA is permitted to respond to a DSA, DOP, or DISP bind without any credentials by supplying **SimpleCredentials** with **name** present.

Initiating DSAs shall be capable of accepting such credentials.

---

[12] An example of two ASN.1 types which can have similar contents but different DER by the X.509 rules are:

SET{ SEQUENCE {}, PrintableString }

SET OF CHOICE {SEQUENCE {}, PrintableString }

The hex encoding 31/04/30/00/13/00 can represent a value of either syntax, but it would not be a correct DER encoding for the second syntax (for which the hex encoding 31/04/13/00/30/00 would be correct DER).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

6.6 Simple Protected Authentication

6.6.1 Initiator of the Bind

For a DSA claiming conformance to Simple Protected Authentication, the initiator shall be capable of the following procedures:

1. The initiator shall comply with procedures laid down in:
   - [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 11.1
   - [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 8.1.2 2nd paragraph.
   - [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] subclauses 6.1 and 6.2, following the procedures that do not include $t2^A$ and $q2^A$.

with additional requirements as specified in the paragraphs 2 to 5 below.

Note. The use of **time2** and **random2** is out of the scope of this part of ISO/IEC ISP 15125.

2. **time1** shall be present and shall be set equal to an expiry time for the bind credentials; down to seconds, using any compliant **UTCTime** encoding that includes the seconds field, in accordance with 8824-1 clause 35 .3 a), b) option 2), c) option 1 or 2; it shall thus be set equal to the time of the bind plus a short positive interval.

3. **random1** shall be present. If two-way authentication is to be supported, then the DSA shall be able to encode this element in accordance with the requirements of subclause 6.2.

4. The **protected** choice for password shall be taken.

5. Within the **SIGNATURE**, the algorithm identifier shall represent a specific hashing algorithm, taken from the definitions given in Normative Annex C (see also note3 below).

   Note. This algorithm must include any padding that may be needed to bring the length to one compatible with the hashing algorithm.

6. Also within the **SIGNATURE**, the **encrypted** element shall, taken as a binary number, equal the result of application of the algorithm of 5 to the octet string formed by the following ASN.1 DER encoding:

```
SEQUENCE {
    name        DistinguishedName, -- equal to SimpleCredentials.name
    time1       UTCTime, -- equal to SimpleCredentials.validity.time1
    random1     BIT STRING, -- equal to SimpleCredentials.validity.random1
    password    OCTET STRING -- equal to SimpleCredentials.password.unprotected
    }
```

   where the last element is the value (of the DSA's own password) that would have been supplied if the credentials had been unprotected.

   Notes.

   1. If **time2** and **random2** are used, these should be present as follows:

```
SEQUENCE {
    name        DistinguishedName, -- equal to SimpleCredentials.name
    time1       UTCTime, -- equal to SimpleCredentials.validity.time1
    time2       UTCTime, -- equal to SimpleCredentials.validity.time2
    random1     BIT STRING, -- equal to SimpleCredentials.validity.random1
    random2     BIT STRING, -- equal to SimpleCredentials.validity.random2
    password    OCTET STRING -- equal to SimpleCredentials.password.unprotected
    }
```

   2. It is recommended that the values of each of the **SimpleCredentials** elements in the DSA, DOP, or DISP Bind be DER encoded. **If so encoded, the receiving DSA does not have to re-create the DER encoding. However, this is a recommendation only.**

   3. DSAs may support and use hashing algorithms other than those given in Normative Annex C; the requirements stated above represent a basic capability.

6.6.2 Responder to the Bind

The responder to the DSA, DOP, or DISP Bind shall validate the returning protected simple credentials as follows:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1. It shall determine that the credentials are invalid if the timestamp is older than the present time by more than the value of the configurable expiry period (see static conformance requirements).
2. It shall synthesise the value of **SimpleCredentials.password.protected** in accordance with the procedures of the preceding subclause, but making use of its own stored knowledge of the responding DSA's password as the notional value of **SimpleCredentials.password.unprotected**; the credentials shall be taken as invalid if the two hashed password values, as received and as synthesised, are different.
3. It shall maintain a list of information (e.g. {initiator-name, **time1** value, **random1** value} for each incoming bind for at least the time specified by the configurable expiry period, and shall detect a repetition of the combination; if repetition is detected, the credentials shall be taken as invalid

Note. This important requirement relates to the mechanism whereby the responder detects replay by an impostor that has observed a valid bind. Only the expiry of the **time1** timestamp protects against replay by simple protected authentication against a different DSA.

The responding DSA shall be capable of creating return credentials in the case of a validated Bind Request in accordance with the procedures of subclause 6.6.1, except that if two-way authentication is to be supported, then the DSA shall be able to encode the value **SimpleCredentials.validity.random1** in accordance with the requirements of subclause 6.2.

If the Initiator's credentials are invalid, or if the Bind Request is rejected, the error procedures specified in subclause 6.7 shall be followed.

6.6.3 Initiator's response to Bind Result

The initiator of the DSA, DOP, or DISP Bind shall validate the incoming protected simple credentials as follows:

1. If the incoming timestamp **time1** is older than the present time by more than the value of the configurable expiry period (see static conformance requirements), or if it is older than the time of issue of the original Bind Request by more than twice the value of the configurable expiry period, the credentials shall be taken as invalid.
2. It shall synthesise the value of **SimpleCredentials.password.protected** in accordance with the procedures of the preceding subclause; the credentials shall be taken as invalid if the two hashed password values, as received and as synthesised, are different.
3. If two-way authentication is to be supported, then the DSA shall be able to decode and validate the incoming value of **random1** in accordance with the requirements of subclause 6.2.

If the responder's credentials are invalid, or if the Bind Request is to be rejected, the error procedures specified in subclause 6.7.1 shall be followed.

6.7 Strong Authentication in the DSA, DOP, or DISP Bind

6.7.1 Initiator of the Bind

The initiator shall support the following procedures:

1. The initiator shall comply with procedures laid down in:
   - [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 11.1
   - [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 8.1.2 3rd paragraph.
   - [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] subclauses 10.2 or 10.3 depending on whether two one-way authentications or two-way authentication is required.

   If two-way authentication is to be supported, then the DSA shall be able to encode this element in accordance with the requirements of subclause 6.2.
2. The initiator shall either include **StrongCredentials.certification-path** or **StrongCredentials.name** in the value of **StrongCredentials**. Both may also be included, but if this is the case, the value of **StrongCredentials.certification-path.SIGNED.subject** shall be identical to that of **StrongCredentials.name.** This name shall be the name of the initiator DSA (i.e. the Directory distinguished name corresponding to the DSA as an AE).
3. The inclusion of **StrongCredentials.certification-path.theCACertificates** is optional, but, if included, all certificates shall be subject to the restrictions specified in subclause 6.6.1.

6.7.2 Responder to the Bind

The responder DSA shall support the following procedures for validating the incoming Strong Credentials:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1. The responder shall check that the **bind-token.algorithm** is supported (i.e. that the signature can be evaluated using this algorithm), that the **bind-token.name** value is identical to the name of the responder (i.e. the Directory distinguished name corresponding to the DSA as an AE)., and that the **bind-token.time** (the expiry time) is later than the present time; otherwise, the credentials shall be taken as invalid.
2. The responder shall check that the signature of the initiator is correct by means of pre-stored certificate information, or by other means that do not require Directory operations; if the signature is found to be incorrect in this way, the credentials shall be taken as invalid.
3. The responder shall maintain a list of information (e.g. {initiator-name, **bind-token.random** value}) for each incoming bind for at least the time preceding **bind-token.time**, and shall detect a repetition of the combination; if repetition is detected, the credentials shall be taken as invalid.
4. The responder shall optionally check the initiator's certificate (including validation against the appropriate Revocation Lists), but shall not be required to do so before the DSP, DOP, or DISP association has been established. This presumes that the certificate has been acquired using an adequately secure bilateral procedure.

DSAs shall be capable of demonstrating that they are capable of checking the certificate, together with associated certificates, by reference, as necessary, to revocations lists, and that they can close down the DSP, DOP, or DISP association if an error is found.

The responder DSA shall support the procedures for creating returning strong credentials defined for the initiator in the preceding subclause. If two-way authentication is to be supported, then the DSA shall be able to encode the value **bind-token.random** in accordance with the requirements of subclause 6.2.

If the Initiator's credentials are invalid, or if the Bind Request is rejected, the error procedures specified in subclause 6.7 shall be followed.

6.7.3 Initiator's response to Bind Result

The initiator of the bind shall validate the incoming strong credentials as follows:

1. The initiator shall check that the **bind-token.algorithm** is supported, that the **bind-token.name** value is identical to that of the initiator, and that the **bind-token.time** is later than the present time; otherwise, the credentials shall be taken as invalid.
2. The initiator shall check that the signature of the responder is correct by means of pre-stored certificate information, or by other means that do not require Directory operations; otherwise, the credentials shall be taken as invalid.
3. The responder shall optionally check the initiator's certificate (including validation against the appropriate Revocation Lists), but shall not be required to do so before the DSP, DOP, or DISP association has been established.
4. If two-way authentication is to be supported, then the DSA shall be able to decode and validate the incoming value of **random1** in accordance with the requirements of subclause 6.2.

DSAs shall demonstrate that they are capable of checking the certificate, together with associated certificates, by reference, as necessary, to revocation lists, and that they can close down the DSP, DOP, or DISP association in consequence.

If the responder's credentials are invalid, or if the Bind Request is to be rejected, the error procedures specified in subclause 6.7 shall be followed.

6.8 Signed DSP or DISP operations

6.8.1 Invoker of the Operation

The invoking DSA shall support the following procedures for creating a signed DSP or DISP operation over and above the stipulations of [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 7.10 (these apply also for DISP):

In **ChainingArguments**:

- **securityParameters** shall be present
- In **securityParameters.certification-path** (which must be present in accordance with [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 7.10) the name of the subject of the certificate shall be equal to the name of the invoking DSA and the restrictions of subclause 6.6.1 shall apply.
- **securityParameters.time** shall be present and shall be the expiry time of the validity of the signature·

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- **securityParameters.random** shall be present. If two-way authentication is to be supported, then the DSA shall be able to encode this element in accordance with the requirements of subclause 6.2.
- **securityParameters.protectionRequest** is optional and may be ignored.

Note. This last element appears to apply to the request for the DAP return result to be signed, rather than the DSP or DISP return result. In these procedures, a signed invoke is always followed by a signed return result.

6.8.2 Performer of the operation

The performer DSA shall support the following procedures for validating the incoming signed DSP or DISP operations:

1. The performer shall check that the subject name of the certificate (if present) is identical to the name of the invoking DSA, as determined by the authentication process for the preceding DSA, DOP, or DISP Bind; otherwise, the signature shall be taken as invalid.

   Note. In consequence, a signed DSP or DISP operation shall not be accepted if the DSA or DISP Bind was anonymous.

2. The performer shall check that the signature of the invoke is correct, by means of pre-stored certificate information, or by other means; otherwise, the signature shall be taken as invalid.

3. The performer shall maintain a list of information (e.g. {invoker-name, **securityParameters.random** value}) for each incoming operation for at least the time preceding **securityParameters.time**, and shall detect a repetition of the combination on any association, and not distinguishing between invoker and performer for the specific DS or DISP operation; if repetition is detected, the signature shall be taken as invalid.

4. The performer shall check the invoker's certificate (including validation against the appropriate Revocation Lists) before responding to the operation, by reference to locally cached information that is refreshed from time to time, DSAs shall demonstrate that they can close down the DSP, DOP, or DISP association as a result of a certificate error, and that they are capable of obtaining and acting on refreshed certificate or CRL information (e.g. which revokes the invoker's certificate).

5. When a return result is to be returned, the Performer shall respond to an incoming signed Invoke with a signed return result. The performer DSA shall support the procedures for creating a signed return result, as defined in the preceding subclause. If two-way authentication is to be supported, then the DSA shall be able to encode the value **securityParameters.random** in accordance with the requirements of subclause 6.2.

If the invoker's credentials are invalid, the error procedures specified in subclause 6.7 shall be followed, including closing down the association.

6.8.3 Invoker receiving signed Return Result

The invoking DSA shall support the following procedures for validating the incoming Strong Credentials of the Performer:

1. The invoker shall check that the subject name of the certificate (if present) is identical to the name of the DSA to which the DSP or DISP association has been made; otherwise, the signature shall be taken as invalid.

2. The invoker shall check that the signature of the responder is correct, by means of pre-stored certificate information, or by other means; otherwise, the signature shall be taken as invalid.

3. The invoker shall maintain a list of information (e.g. {performer-name, **securityParameters.random** value}) for each incoming operation for at least the time preceding **securityParameters.time**, and shall detect a repetition of the combination on any association, and not distinguishing between invoker and performer for the specific DSP or DISP operation; if repetition is detected, the signature shall be taken as invalid.

4. The invoker shall check the responder's certificate (including validation against the appropriate Revocation Lists) before responding to the corresponding inward operation, by reference to locally cached information that is refreshed from time to time. DSAs shall demonstrate that they can close down the DSP or DISP association as a result of a certificate error, and that they are capable of obtaining and acting on refreshed certificate or CRL information (e.g. which revokes the invoker's certificate).

5. If two-way authentication is to be supported, then the DSA shall be able to decode and validate the incoming value of **random1** in accordance with the requirements of subclause 6.2.

If the performer's credentials are invalid, the error procedures specified in subclause 6.7 shall be followed, including closing down the association.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

6.9 Merging signed results

When a DSA must merge signed partial results for a list or search operation, it shall retain the signature and include each item in **uncorrelatedListInfo** or **uncorrelatedSearchInfo**, as appropriate. However, a DSA is permitted to discard a complete partial result if not doing so would result in excessive information being returned.

6.10 Certificates

6.10.1 Certification Path Creation

There is no requirement to generate the following elements:

- **Credentials.strong.certification-path.theCACertificates**
- **SecurityParameters.certification-path.theCACertificates**

However, these elements may be supplied in accordance with an algorithm of the implementor's choosing.

If supplied, they shall be subject to the following general requirements:

- Forward certificates shall represent a single unbroken directed graph (i.e. the subject of each certificate shall be the issuer of another forward certificate or of the originator's certificate)
- A reverse certificate shall match the corresponding forward certificate if both are present in a single **CertificatePair** element (i.e. the issuer of the one is the subject of the other)

6.10.2 Certification Path Use

There is no requirement to use the following elements:

- **Credentials.strong.certification-path.theCACertificates**
- **SecurityParameters.certification-path.theCACertificates**

However, these elements may be used in accordance with an algorithm of the implementor's choosing.

6.10.3 Certificate Processing

The processing of Certificates shall be carried out in accordance with the principles of [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] subclause 11.2.

In cases where the unique identifier is available, e.g.:

- In a Version 2 certificate or later and **xxxUniqueIdentifier** is present
- When available without a further Directory operation in a corresponding attribute value (e.g. **uniqueIdentifier** - see ISO/IEC [ISO/IEC 9594-6 : 1995 | ITU-T Rec. X.520 (1993)] subclause 5.2.7)

the two unique identifiers shall match.

DSAs shall be capable of configuration to match issuer or subject names when the name matches, but the **xxxUniqueIdentifier** is unknown or cannot be obtained without a Directory operation.

A Version 3 certificate shall be taken as invalid if an unsupported critical extension is defined for it, in accordance with the corresponding Technical Corrigendum. When an implementation processing a certificate does not recognise an extension, if the extension is non-critical, it may ignore that extension, and can consider the certificate to be valid. If the extension is critical, and the particular extension type is not recognised by the DSA, then the certificate should be considered invalid.

6.10.4 Revocation List Processing

Processing of Revocation Lists shall be carried out in accordance with the principles of [ISO/IEC 9594-8 : 1995 | ITU-T Rec. X.509 (1993)] subclause 11.2. The following stipulations also apply.

A DSA shall be capable of detecting the presence of a certificate on a Revocation List by scanning the complete list of serial numbers, and shall then consider it revoked, whether or not critical extensions are supported.

A DSA shall be capable of detecting whether a Revocation List has expired by analysis of the **nextUpdate** element of the **CertificateList** value. However, certificates revoked by an expired Revocation List shall be taken as invalid.

A certificate found to be revoked by a Revocation List for which the signature cannot be validated or which appears to be invalid in any other way may optionally be considered to be actually revoked.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A certificate for which the corresponding Revocation List cannot be read from the Directory, or which can be read, but is found to have expired may optionally be considered to be revoked.

6.11 Access Control Identity in the Distributed Directory

This subclause relates to the access control identity associated with a DAP or DSP operation. The issues addressed are:

- What name associated with the originator of an operation should to be used as the access control identity?
- If different originator names present, is this acceptable, or should a DSA take it as a sign of potential security breach.

6.11.1 Sources of originator information

The following are defined as indicating the source of an operation**:**

Element	Standards references	Assessment
The authenticated identity associated with the DAP association within which the DAP operation occurs	[ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 8.1.1: *The* **credentials** *argument of the* **DirectoryBindArgument** *allows the Directory to establish the identity of the user...* [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.5o1 (1993)] subclause 15.2.1 last para: *In general, there will be a mapping function from the authenticated identity to the access control identity (e.g. the distinguished name of an entry, together with an optional unique identifier, representing the user. This mapping does not fall within the scope of this Directory Specification. However, a particular security policy may state that the authenticated identity and the access control identity are the same.* [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)] subclause 15.2.1 2nd note: *Local administrative policy may stipulate that authentication taking place in certain other DSAs (e.g. DSAs in other DMDs) is to be disregarded.*	The bound identity is clearly indicated as a positive and specific identification of the user. A non-trivial mapping function from the authenticated identity to the access control identity is not consistent with other requirements and implications (see below). DSAs conformant to this part of ISO/IEC ISP 15125 shall therefore support the case where the bound identity is the same as the authenticated identity.
The **requestor** argument in an operation's **CommonArguments**	[ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 7.3 4th para: *The* **requestor** *Distinguished Name identifies the originator of a particular operation. It holds the name of the user as identified at the time of binding to the Directory. It may be required when the request is to be signed,*	The **requestor** element must correspond to the DAP bound identity, according to the definitions. If different, the DSA to which the DAP bind takes place should refuse to accept the operation on grounds of potential security breach. If the operation is unsigned the **requestor** argument in an incoming DSP operation can be regarded as

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Element	Standards references	Assessment
	and shall hold the name of the user who initiated the request. [ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 a): *If* **requestor** *is present in* **CommonArguments**, *[the* **originator***] argument may be omitted.*	advisory at best, in the absence of corroborative evidence. If the operation is signed, the **requestor** argument is redundant, since the originator of the signature is already defined (see below). DSAs conformant to this part of ISO/IEC ISP 15125 should check the **requestor** element, but should not regard it as authoritative. There is no conformance requirement in respect of this assessment.
In a signed operation, by **SecurityParameters.certification-path.userCertificate.SIGNED. subject**	[ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] subclause 7.10: *The* **CertificationPath** *component consists of the sender's certificate, and, optionally, a sequence of certificate pairs. The certificate is used to associate the sender's public key and distinguished name, and may be used to verify the signature on the argument or result. This parameter shall be present if the argument or result is signed.*	This identifier appears to be the most authoritative for a signed operation, and should probably be used in preference to **requestor**, or any other element, since it is the only identity that is confirmed (rather than just asserted) in the signed operation. The **subject** cannot represent a different identity to the bound identity. DSAs conformant to this part of ISO/IEC ISP 15125 shall therefore support **SecurityParameters.certification-path.userCertificate.SIGNED. subject** as the authenticated identity. DSAs may take it as an error situation if this identity is different to the bound identity or the identity given by the **originator** element.
In a DSP operation, by the **originator** argument	[ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 a): *The* **originator** *component conveys the name of the (ultimate) originator of the request unless already specified on the security parameters. If* **requestor** *is present in* **CommonArguments**, *[the* **originator***] argument may be omitted.*	The **originator** argument is only used in the context of simple authentication, and is the only way in which DSA can pass on access control identity to their own satisfaction. However, since **requestor** (see below) is equated to originator, and also to bound identity, there is evidently an equivalence between all three of bound identity, **originator** value and access control identity. DSAs conformant to this part of ISO/IEC ISP 15125 shall be capable of demanding that there is no difference between values that are available.
In a DSP operation, by the **uniqueIdentifier** argument	[ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 n): **UniqueIdentifier** *is optionally supplied when it is required to*	When strong authentication is used (in the bind or in signed operations), **UniqueIdentifier** is made available as a by-product of validation of the subject's certificate. This is the only

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Element	Standards references	Assessment
	confirm the originator name.	reliable way in which the value of **UniqueIdentifier** can be determined. DSAs claiming conformance to support of **UniqueIdentifier** shall support this means of finding it.

In addition, **authenticationLevel** is relevant.

Element	Standards references	Assessment
authenticationLevel	[ISO/IEC 9594-4 : 1995 | ITU-T Rec. X.518 (1993)] subclause 10.3 m): **AuthenticationLevel** *is optionally supplied when it is required to indicate the manner in which authentication has been carried out.* [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)] subclause 16.4.2.3: *When* **basicLevels** *is used, an* **AuthenticationLevel** *consisting of a* **level** *and optional* **localQualifier** *shall be assigned to the requestor to the DSA according to local policy*	**AuthenticationLevel** can be used by a DSA to which a DAP bind exists to indicate the authentication level of that bind. DSAs receiving this information can amend it downwards for access control purposes or for chaining on. DSAs should be able to carry out this downgrading, but no conformance requirement is defined in respect of downgrading.

6.11.2 Omission or variation of originator element in chaining arguments

The inclusion of the **originator** element in chaining arguments can be assumed to identify that a satisfactory simple-authentication in the DAP bind took place, from the viewpoint of the originating DSA. The value of this element shall be used as the basis of the access control identity.

The **authenticationLevel** component may optionally be used, particularly when it is required to indicate a stronger level of authentication than simple.

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. When this is done, the value of the requestor element shall not be taken as representing the originator.

According to [ISO/IEC 9594-2 : 1995 | ITU-T Rec. X.501 (1993)] subclause 15.2.1 third paragraph, DSAs are apparently permitted to evaluate the to a name that is not the same as the name used for logging in. However, the considerations identified in the tables of subclause 6.11.1 do not consistently support this viewpoint, and DSAs conformant with this part of ISO/IEC ISP 15125 shall ensure that (as far as can be determined) **originator** is the same as the authenticated identity.

The use of the **requestor** argument is not recommended as a source of access control identity.

6.12 Error Handling

6.12.1 Error Handling for DSA, DOP, or DISP Binds

6.12.1.1 Error Semantics

The three errors that are permitted as Bind Errors shall be used as follows:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 2 — Error semantics

Error	Semantics
Security-error–inappropriate authentication	The level of security is inappropriate (see [ISO/IEC 9594-3 : 1995 | ITU-T Rec. X.511 (1993)] 12.7 a))
Security-error–invalid credentials - DSA, DOP, or DISP Bind	The supplied credentials were invalid, in that no DSA, given all of the necessary information about the originator, and his/her/its certificates, and an unlimited capability to process them, could determine that they were valid.
Security-error–invalid credentials - Signed operations	The supplied user credentials were invalid. This error response is therefore not an appropriate response for failed DSP, DOP, or DISP signed operations, since the invalid party is the DSA and not the user.
Service-error–unavailable	All other errors, including the case where it cannot be determined if Security-error - invalid credentials is the correct error

Note. It is recommended that Service-error–unavailable shall take precedence over other errors.

6.12.1.2 Errors for Simple Protected Authentication in a DSA, DOP, or DISP Bind - Responder

If simple protected credentials were expected and simple unprotected credentials, or other form of credentials were supplied, Security-error–inappropriate-authentication shall be used.

If the algorithm named in the **SIGNATURE** element is known to be inappropriate (e.g. it is an object identifier that does not identify a hash and fill algorithm) Security-error–invalid-credentials should be used. However, a DSA shall not be obliged to check the nature of the object identifier, so there is no conformance requirement.

If the algorithm named in the **SIGNATURE** element is unidentified and is also unsupported, Service-error–unavailable shall be used. However, because of the previous paragraph, Security-error–invalid-credentials shall also be acceptable in a conformance test.

If the protected simple credentials carry a time-stamp outside the configured validity period, Security-error–invalid-credentials shall be used.

If a DSA is not in possession of the password of the other DSA, Service-error–unavailable shall be used.

Other error situations shall be handled in accordance with 6.12.1.1.

6.12.1.3 Errors for Strong Authentication in a DSA, DOP, or DISP Bind - Responder

If strong credentials was expected and another form of credentials were supplied, Security-error–inappropriate-authentication shall be used.

If the algorithm named in the **token**'s **SIGNATURE,** or for the **SIGNATURE** of any other signed element is known to be inappropriate (e.g. it is an object identifier that does not identify an appropriate strong authentication method, hash and fill algorithm) security-error–invalid credentials should be used. However, a DSA shall not be obliged to check the nature of the object identifier, so there is no conformance requirement.

If the algorithm named in any **SIGNATURE** element is unidentified and is also unsupported,. Service-error–unavailable shall be used. However, because of the previous paragraph, Security-error–invalid credentials shall also be acceptable in a conformance test.

If the received **StrongCredentials** element contains neither **certification-path** nor **name**, the credentials are invalid, and Security-error–invalid-credentials shall be used.

Note. **StrongCredentials.name** and **StrongCredentials.bind-token.name** should not be confused. The former is the name of the requesting DSA, while the latter is the name of the target DSA.

If **StrongCredentials.bind-token.name** does not match the name of the target DSA, the credentials are invalid, and Security-error–invalid credentials shall be used.

If the responding DSA is not capable of completing the process of validation of the credentials, but all steps of the process that have been completed are correct, Service-error–unavailable shall be used. Specifically, a failure to obtain a revocation list or to validate the signature on a revocation list that does not contain a reference to the certificate being validated shall be signalled by this error.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Note. A revocation list with an un-validated or failed signature that contains a reference to a certificate being validated may optionally be taken as making the certificate invalid.

Other error situations shall be handled in accordance with 6.12.1.1.

6.12.1.4 Errors for Strong Authentication in a DSA, DOP, or DISP Bind - Initiator

This subclause applies to Initiator DSAs that were unable to establish a DSP, DOP, or DISP association for reasons specified in this part of ISO/IEC ISP 15125.

The initiator shall respond to operations that would have been chained using the DSP, DOP, or DISP Association as if the responding DSA had been unavailable.

The initiator shall respond to operations from the responder either with a Service-Error–unavailable or by premature termination of the association by an Abort.

Note. These operations are possible because, once the responder has sent back a bind result, the association exists as far as the responder is concerned, and the DSA can chain operations onto it.

6.12.2 Errors in Signed DSP or DISP Operations

6.12.2.1 Errors in a Signed DSP or DISP Operation - Performer

A DSA shall respond to an invalid or inadequately validated signed invoke by closing down the association.

The DSA may respond with Service-Error–unavailable or other appropriate Service Error to the current operation and to all operations not yet responded to before terminating the association. Security-error–invalid credentials shall not be used (see Table 2 above).

6.12.2.2 Errors in a Signed DSP or DISP Operation - Invoker

A DSA shall respond to an invalid or inadequately validated signed response by closing down the association.

In the case of a DSP operation, a DSA shall respond to the originator of the operation, after receiving an invalid or inadequately validated signed return result as if a Service-Error–unavailable had been received, and in particular, the error passed back to the original source of the invoke as a direct consequence of this failure to validate shall not be Security-error–invalid credentials. With DISP, a similar indication may be made to the shadowing mechanisms that initiated the operation.

Note. This may be conformance tested by the Tester returning a bad DSP or DISP return-result signature to the IUT following an original invoke of a simple operation (read, compare, modify-entry).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 this part of ISO/IEC ISP 15125 on what shall or may appear in an Implementors' PICS for an implementation conformant to autonomous DUA procedures.

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

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

Profile Requirements List

A.1 Identification of the implementation

A.1.1 Identification of PICS

This part of ISO/IEC ISP 15125 is based on:

- ISO/IEC JTC1/SC CD13248-2: The Directory: Protocol Implementation Conformance Statement (PICS) Proforma for the Directory System Protocol
- ISO/IEC JTC1/SC CD13248-3: The Directory: Protocol Implementation Conformance Statement (PICS) Proforma for the Directory Operational Binding Management Protocol
- ISO/IEC JTC1/SC CD13249: The Directory: Protocol Implementation Conformance Statement (PICS) Proforma for the Directory Information Shadowing Protocol

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	Note 1
8	Other information	

Notes:

1. DSAs shall conform as a precondition to the following ISPs:

   ADY22

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.2 Identification of the protocol

A.2.1 Identification of the protocol - DSP

Item no	Question	Response
1	Title, Reference No., publication date of the protocol standard	[ISO/IEC 9594 : 1995 | ITU-T Rec. X.518 (1993)], Information Technology — Open Systems Interconnection — The Directory: Procedures for Distributed Operation
2	Protocol Version Number	Version 1
3	Implemented Addenda	
4	Implemented Defect Reports (Reference No.)	See Annex B
5	Implementor's Guide Version Number	9

A.2.2 Identification of the protocol - DOP

Item no	Question	Response
1	Title, Reference No., publication date of the protocol standard	[ISO/IEC 9594 : 1995 | ITU-T Rec. X.501 (1993)], Information Technology — Open Systems Interconnection — The Directory: The Models
2	Protocol Version Number	Version 1
3	Implemented Addenda	
4	Implemented Defect Reports (Reference No.)	See Annex B
5	Implementor's Guide Version Number	9

A.2.3 Identification of the protocol - DISP

Item no	Question	Response
1	Title, Reference No., publication date of the protocol standard	[ISO/IEC 9594 : 1995 | ITU-T Rec. X.525 (1993)], Information Technology — Open Systems Interconnection — The Directory: Replication
2	Protocol Version Number	Version 1
3	Implemented Addenda	
4	Implemented Defect Reports (Reference No.)	See Annex B
5	Implementor's Guide Version Number	9

A.3 Global statements of conformance

A.3.1 Global statement of conformance - DSP

Item No.	Question	D	P	Predicate Name or note	Response
1.	Does the DSA support DSA Binds in the initiator role?	o	o	p_dsa_bind_ini	
2.	Does the DSA support DSA Binds in the responder role?	o	o	p_dsa_bind_resp	

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Item No.	Question	D	P	Predicate Name or note	Response
3.	Does the DSA support DSA Binds using simple protected credentials in the initiator role?	o	o	p_dsa_simp_prot_ini	
4.	Does the DSA support DSA Binds using simple protected credentials in the responder role?	o	o	p_dsa_simp_prot_resp	
5.	Does the DSA support DSA Binds using strong credentials in the initiator role?	o	o	p_dsa_strong_ini	
6.	Does the DSA support DSA Binds using strong credentials in the responder role?	o	o	p_dsa_strong_resp	
7.	Does the DSA support the invoker role in DSP operations?	o	o	p_dsp_invoker	
8.	Does the DSA support signed DSP operations in both invoker and performer roles	o	o	p_signed_dsp	
9.	Does the DSA support unique identifiers in ChainingArguments?	o	o	p_dsp_unique_names	
10.	Does the DSA support authentication level in ChainingArguments	o	o	p_dsp_auth_level	

A.3.2 Global statement of conformance - DOP

Item No.	Question	D	P	Predicate Name or note	Response
1.	Does the DSA support Operational Binding type: **shadowOperationalBindingID**	o	o	p_sob	
2.	Does the DSA support Operational Binding type: **SpecificHierarchicalBindingID**	o	o	p_shob	
3.	Does the DSA support Operational Binding type: **Non-specificHierarchicalBindingID**	o	o	p_nshob	
4.	Does the DSA support DOP Binds in the initiator role?	o	o	p_dop_bind_ini	
5.	Does the DSA support DOP Binds in the responder role?	o	o	p_dop_bind_resp	
6.	Does the DSA support DOP Binds using simple protected credentials in the initiator role?	o	o	p_dop_simp_unprot_ini	
7.	Does the DSA support DOP Binds using simple protected credentials in the responder role?	o	o	p_dop_simp_unprot_resp	
8.	Does the DSA support DOP Binds using strong credentials in the initiator role?	o	o	p_dop_strong_ini	
9.	Does the DSA support DOP Binds using strong credentials in the responder role?	o	o	p_dop_strong_resp	

A.3.3 Global statement of conformance - DISP

Item No.	Question	D	P	Predicate Name or note	Response
1.	Does the DSA support the application-context: **shadowSupplierInitiatedAC**?	o	o	p_disp_sup_ini	

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Item No.	Question	D	P	Predicate Name or note	Response
2.	Does the DSA support the application-context: **reliableshadowSupplierInitiatedAC?**	o	o	p_disp_rel_sup_ini	
3.	Does the DSA support the application-context: **shadowConsumerInitiatedAC**?	o	o	p_disp_cons_ini	
4.	Does the DSA support the application-context: **reliableshadowConsumerInitiatedAC**?	o	o	p_disp_rel_cons_ini	
5.	Does the DSA support DISP Binds in the initiator role?	o	o	p_disp_bind	
6.	Does the DSA support DISP Binds in the responder role?	o	o	p_disp_simp_unprot_resp	
7.	Does the DSA support DISP Binds at least using simple protected credentials in the initiator role?	o	o	p_disp_simp_unprot_in	
8.	Does the DSA support DISP Binds at least using simple protected credentials in the responder role?	o	o	p_disp_simp_unprot_resp	
9.	Does the DSA support DISP Binds at least using strong credentials in the initiator role?	o	o	p_disp_strong_ini	
10.	Does the DSA support DISP Binds at least using strong credentials in the responder role?	o	o	p_disp_strong_resp	
11.	Does the DSA support signed DISP operations in both invoker and performer roles	o	o	p_signed_disp	

A.3.4 Global statement of conformance - all supported protocols

Item No.	Question	D	P	Predicate Name or note	Response
1.	Does the DSA support two-way authentication in simple protected authentication?	o	o	p_2way_simp_prot	
2.	Does the DSA support two-way authentication in strong binds?	o	o	p_2way_strong	
3.	Does the DSA support two-way authentication in signed operations?	o	o	p_2way_signed	
4.	Does the DSA support Certificates Version 1	o	o	p_cert_v1	
5.	Does the DSA support Certificates Version 2	o	o	p_cert_v2	
6.	Does the DSA support Certificates Version 3	o	m	p_cert_v3	
7.	Does the DSA support Certificate Revocation Lists Version 1	o	o	p_crl_v1	
8.	Does the DSA support Certificate Revocation Lists Version 2	o	o	p_crl_v2	
9.	Does the DSA support Certificate Revocation Lists Version 3	o	m	p_crl_v3	

A.4 DSP

For the purposes of this subclause and its subclauses in turn:

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

p_simp_unprot = p_dsa_bind_ini AND p_dsa_bind_resp
p_simp_prot = p_dsa_simp_prot_ini AND p_dsa_simp_prot_resp
p_strong = p_dsa_strong_ini AND p_dsa_strong_resp
p_signed = p_signed_dsp

A.4.1 Capabilities and options

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

Column heading:	Rel (relaying)	Act (acting)	Resp (responding)
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

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.4.1.1Operations

DSAs shall conform to ADY22 as a precondition

Item No.	Protocol Element	DSP D Rel	DSP D Act	DSP D Resp	DSP P Rel	DSP P Act	DSP P Resp	Reference/Notes
1	DirectoryBind	m	m	m	c1	c1	m	Note 1
2	DirectoryUnbind	m	m	m	c1	c1	m	Note 1
3	ChainedRead	o	o	m	c1	c1	m	Note 1
4	ChainedCompare	o	o	m	c1	c1	m	Note 1
5	ChainedAbandon	o	o	m	c1	c1	m	Note 1
6	ChainedList	o	o	m	c1	c1	m	Note 1
7	ChainedSearch	o	o	m	c1	c1	m	Note 1
8	ChainedAddEntry	o	o	m	c1	c1	m	Note 1
9	ChainedRemoveEntry	o	o	m	c1	c1	m	Note 1
10	ChainedModifyEntry	o	o	m	c1	c1	m	Note 1
11	ChainedModifyDN	o	o	m	c1	c1	m	Note 1

Conditionals

c1: if p_dsp_invoker then m else o

Notes

1. These items are defined in Part 4 of this part of ISO/IEC ISP 15125 (ADY22)

A.4.1.2Protocol Elements

A.4.1.2.1 DSA Bind Elements

A.4.1.2.1.1 DSA Bind Arguments

The column marked Init correspond to the bind initiator

Item No.	Protocol Element	DSP D Init	DSP D Resp	DSP P Init	DSP P Resp	References/Notes
1	DirectoryBindArg	m	m	m	m	A.4.1.1/1
2	credentials	c	c	m	m	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Item No.	Protocol Element	DSP D Init	DSP D Resp	DSP P Init	DSP P Resp	References/Notes
3	simple	c	c	m	m	
4	name	m	m	m	m	
5	validity	o	o	c3	c3	
6	time1	o	o	m	m	
7	time2	o	o	i	i	
8	random1	o	o	m	m	
9	random2	o	o	i	i	
10	password	o	o	m	m	
11	unprotected	o	o	m	m	
12	protected	o	o	c3	c3	
13	algorithm Identifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c5	c5	
16	certification-path	o	o	m	m	A.7.3 Note 1
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	A.7.4
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithm Identifier	m	m	m	m	A.7.4
24	encrypted	m	m	m	m	
25	name	o	o	o	m	Note 1
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Conditionals:

c3: if p_simp_prot then m else o

c4: if p_simp_unprot then m else o

c5: if p_strong then m else o

Notes

1. At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

A.4.1.2.1.2 DSA Bind Result

Item No.	Protocol Element	DSP D Init	DSP D Resp	DSP P Init	DSP P Resp	References/notes
1	DirectoryBindArg	m	m	m	m	A.4.1.2.1.1

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Item No.	Protocol Element	DSP D Init	DSP D Resp	DSP P Init	DSP P Resp	References/notes
2	credentials	c	c	m	m	
3	simple	c	c	m	m	
4	name	m	m	m	m	
5	validity	o	o	c3	c3	
6	time1	o	o	m	m	
7	time2	o	o	i	i	
8	random1	o	o	m	m	
9	random2	o	o	i	i	
10	password	o	o	m	m	
11	unprotected	o	o	m	m	
12	protected	o	o	c3	c3	
13	algorithm Identifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c5	c5	
16	certification-path	o	o	m	m	A.7.3 Note 1
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	A.7.4
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithm Identifier	m	m	m	m	A.7.4
24	encrypted	m	m	m	m	
25	name	o	o	o	m	Note 1
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Conditionals:

c3: if p_simp_prot then m else o

c4: if p_simp_unprot then m else o

c5: if p_strong then m else o

Notes

1. At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

A.4.1.2.1.3 Directory Bind Error

(void)

A.4.1.2.2 Directory Unbind Elements

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.4.1.2.3 Chained Operation Elements

tem No.	Protocol Element	DSP D Init	DSP D Resp	DSP P Rel	DSP P Act	DSP P Resp	
1	chainedXxx	c	m	c	c	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	c6	c6	c6	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.4.1.2.4
9	XxxArgument	m	m	m	m	m	Note 1
10	algorithmIdentifier	m	m	m	m	m	A.7.4
11	encrypted	m	m	m	m	m	
12	ChainingArguments	m	m	m	m	m	
13	XxxArgument	m	m	m	m	m	Note 1
14	chainedYyyResult	m	m	m	m	m	Note 2
15	unsigned (chainedYyyResult)	m	m	m	m	m	Note 2
16	ChainingResults	m	m	m	m	m	
17	YyyResult	m	m	m	m	m	Note 2
18	signed (chainedYyyResult)	o	o	c6	c6	c6	Note 2
19	ToBeSigned	m	m	m	m	m	
20	ChainingResults	m	m	m	m	m	
21	YyyResult	m	m	m	m	m	
22	algorithmIdentifier	m	m	m	m	m	A.7.4
23	encrypted	m	m	m	m	m	
24	ChainingResults	m	m	m	m	m	
25	YyyResult	m	m	m	m	m	Note 2
26	Errors	m	m	m	m	m	

Conditionals:

c6: if if p_signed then m else o

Notes.

1. Xxx is any one of:

   Read
   Compare
   List
   Search
   Addentry

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

RemoveEntry
ModifyEntry
ModifyDN

The abandon operation can be chained, however, the X.500 standards do not support digitally signing this operation

2. Yyy is any one of:

Read
Compare
List
Search
Other responses are represented by a simple NULL of no relevance to this PRL.

A.4.1.2.4 Chaining Argument Elements

Item No.	Protocol Element	DSP D Act	DSP D Resp	DSP P Rel	DSP P Act	DSP P Resp	References/notes
1.	ChainingArguments	o	m	m	m	m	A.4.1.2.3/12
2.	originator	o	m	m	m	m	
3.	targetObject	o	m	m	m	m	
4.	operationProgress	m	m	m	m	m	
5.	nameResolutionPhase	m	m	m	m	m	
6.	nextRDNToBe Resolved	o	m	m	m	m	
7.	traceInformation	m	m	m	m	m	
8.	aliasDereferenced	m	m	m	m	m	
9.	aliasedRDNs	o	m	m	m	m	
10.	returnCrossRefs	m	m	o	o	o	
11.	referenceType	m	m	m	m	m	
12.	info	o	o	o	o	m	
13.	timeLimit	o	m	m	m	m	
14.	securityParameters	m	m	c6	c6	c6	A.7.2
15.	entryOnly	m	m	m	m	m	
16.	uniqueIdentifier	o	o	c7	c7	m	
17.	authenticationLevel	o	o	c8	c8	m	
18.	exclusions	o	o	o	o	m	
19.	excludeShadows	o	m	o	o	m	
20.	nameResolveOnMaster	m	m	o	o	m	

Conditionals:

c6: if p_signed then m else o

c7: if p_dsp_unique_names then m else o

c8: if p_dsp_auth_level then m else o

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.4.1.2.5 Chaining Result Elements

Item No.	Protocol Element	D Act	D Resp	P Rel	P Act	P Resp	References/notes
1.	ChainingResults	m	m	m	m	m	
2.	info	o	o	o	o	o	
3.	crossReferences	o	o	o	o	o	
4.	securityParameters	m	m	c6	c6	c6	A.7.2
5.	alreadySearched	m	o	m	m	o	

Conditionals:

1. c6: if p_signed then m else o

A.5 DOP

Note. For the purposes of this subclause and its subclauses in turn:

p_simp_unprot = p_dop_bind_ini AND p_dop_bind_resp
p_simp_prot = p_dop_simp_prot_ini AND p_dop_simp_prot_resp
p_strong = p_dop_strong_ini AND p_dop_strong_resp

A.5.1 Capabilities and options

A.5.1.1Operations

Item No.	Protocol Element	DOP D Inv	DOP D Resp	DOP P Inv	DOP P Resp	References/notes
1	DOPBind	m	m	m	m	
2	DOPUnbind	m	m	m	m	
3	EstablishOperationalBinding	c	m	m	m	Note 1
4	ModifyOperationalBinding	c	m	m	m	Note 1
5	TerminateOperationalBinding	c	m	m	m	Note 1

Notes.

1. DOP EstablishOperationalBinding, ModifyOperationalBinding, and TerminateOperationalBinding operations do not support digitally signed operations in the ‘93 edition of the X.500 Standards.

A.5.1.3Protocol Elements

A.5.1.3.1 DOP Bind Elements

A.5.1.3.1.1 DOP Bind Arguments

The column marked Init correspond to the bind initiator

Item No.	Protocol Element	DOP D Init	DOP D Resp	DOP P Init	DOP P Resp	References/notes
1	DirectoryBindArg	m	m	m	m	A.5.1.1/1
2	credentials	c	c	m	m	
3	simple	c	c	m	m	
4	name	m	m	m	m	
5	validity	o	o	c3	c3	
6	time1	o	o	m	m	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Item No.	Protocol Element	DOP D Init	DOP D Resp	DOP P Init	DOP P Resp	References/notes
7	time2	o	o	i	i	
8	random1	o	o	m	m	
9	random2	o	o	i	i	
10	password	o	o	m	m	
11	unprotected	o	o	m	m	
12	protected	o	o	c3	c3	
13	algorithm Identifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c5	c5	
16	certification-path	o	o	m	m	A.7.3 Note 1
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	A.7.4
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithm Identifier	m	m	m	m	A.7.4
24	encrypted	m	m	m	m	
25	name	o	o	o	m	Note 1
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Conditionals

c2: if (p_simp_unprot OR p_simp_prot) then m else o

c3: if p_simp_prot then m else o

c4: if p_simp_unprot then m else o

c5: if p_strong then m else o

Notes

1. At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

A.5.1.3.1.2 DOP Bind Result

Item No.	Protocol Element	DOP D Init	DOP D Resp	DOP P Init	DOP P Resp	References/notes
1	DirectoryBindArg	m	m	m	m	A.5.1.1/1
2	credentials	c	c	m	m	
3	simple	c	c	m	m	
4	name	m	m	m	m	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Item No.	Protocol Element	DOPD Init	DOPD Resp	DOPP Init	DOPP Resp	References/notes
5	validity	o	o	c3	c3	
6	time1	o	o	m	m	
7	time2	o	o	i	i	
8	random1	o	o	m	m	
9	random2	o	o	i	i	
10	password	o	o	m	m	
11	unprotected	o	o	m	m	
12	protected	o	o	c3	c3	
13	algorithm Identifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c5	c5	
16	certification-path	o	o	m	m	A.7.3 Note 1
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	A.7.4
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithm Identifier	m	m	m	m	A.7.4
24	encrypted	m	m	m	m	
25	name	o	o	o	m	Note 1
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Conditionals:

c2: if (p_simp_unprot OR p_simp_prot) then m else o

c3: if p_simp_prot then m else o

c4: if p_simp_unprot then m else o

c5: if p_strong then m else o

Notes

1. At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

A.5.1.3.2 Directory Unbind Elements

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

A.6 DISP

Note. For the purposes of this subclause and its subclauses in turn:

p_simp_unprot = p_dsa_bind_ini AND p_dsa_bind_resp
p_simp_prot = p_dsa_simp_prot_ini AND p_dsa_simp_prot_resp
p_strong = p_dsa_strong_ini And p_dsa_strong_resp
p_signed = p_signed_dsp

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.6.1 Capabilities and options

A.6.1.1Operations

Item No.	Protocol Element	DISPD Rel	DISPD Resp	DISPP Rel	DISPP Resp	References/notes
1	DSAShadowBind	m	m	m	m	
2	DSAShadowUnbind	m	m	m	m	
3	coordinateShadowUpdate	m	m	m	m	
4	updateShadow	m	m	m	m	
5	requestShadowUpdate	m	m	m	m	

A.6.1.2Protocol Elements

A.6.1.2.1 DSA Shadow Bind Elements

A.6.1.2.1.1 DSA Shadow Bind Arguments

The column marked Init correspond to the bind initiator

Item No.	Protocol Element	DISPD Init	DISPD Resp	DISPP Init	DISPP Resp	Reference/notes
1	DirectoryBindArg	m	m	m	m	A.6.1.1/1
2	credentials	c	c	m	m	
3	simple	c	c	m	m	
4	name	m	m	m	m	
5	validity	o	o	c3	c3	
6	time1	o	o	m	m	
7	time2	o	o	i	i	
8	random1	o	o	m	m	
9	random2	o	o	i	i	
10	password	o	o	m	m	
11	unprotected	o	o	o	m	
12	protected	o	o	c3	c3	
13	algorithm Identifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c5	c5	
16	certification-path	o	o	m	m	A.7.3 Note 1
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	A.7.4
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithm Identifier	m	m	m	m	A.7.4

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Item No.	Protocol Element	DISP D Init	DISP D Resp	DISP P Init	DISP P Resp	Reference/notes
24	encrypted	m	m	m	m	
25	name	o	o	o	m	Note 1
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Conditionals:

c2: if (p_simp_unprot OR p_simp_prot) then m else o

c3: if p_simp_prot then m else o

c4: if p_simp_unprot then m else o

c5: if p_strong then m else o

Notes

1. At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

A.6.1.2.1.2 DSA Shadow Bind Result

Item No.	Protocol Element	DISP D Init	DISP D Resp	DISP P Init	DISP P Resp	References/notes
1	DirectoryBindArg	m	m	m	m	A.6.1.1/1
2	credentials	c	c	m	m	
3	simple	c	c	m	m	
4	name	m	m	m	m	
5	validity	o	o	c3	c3	
6	time1	o	o	m	m	
7	time2	o	o	i	i	
8	random1	o	o	m	m	
9	random2	o	o	i	i	
10	password	o	o	m	m	
11	unprotected	o	o	m	m	
12	protected	o	o	c3	c3	
13	algorithm Identifier	m	m	m	m	
14	encrypted	m	m	m	m	
15	strong	c	c	c5	c5	
16	certification-path	o	o	m	m	A.7.3
17	bind-token	m	m	m	m	
18	toBeSigned	m	m	m	m	
19	algorithm	m	m	m	m	A.7.4
20	name	m	m	m	m	
21	time	m	m	m	m	
22	random	m	m	m	m	
23	algorithm	m	m	m	m	A.7.4

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Item No.	Protocol Element	DISP D Init	DISP D Resp	DISP P Init	DISP P Resp	References/notes
	Identifier					
24	encrypted	m	m	m	m	
25	name	o	o	o	m	
26	externalProcedure	i	i	i	i	
27	versions	m	m	m	m	

Conditionals:

c2: if (p_simp_unprot OR p_simp_prot) then m else o

c3: if p_simp_prot then m else o

c4: if p_simp_unprot then m else o

c5: if p_strong then m else o

Notes

1. At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

A.6.1.2.2 Directory Shadow Unbind Elements

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

A.6.1.2.3 DSA Shadow Operation Elements

Item No.	Protocol Element	DISP D Init	DISP D Resp	DISP P Init	DISP P Resp	References/notes
1	xxx-operation	c	m	m	m	A.6.1.1/3-5 Note 1
2	xxx-operation-argument	c6	c6	c6	c6	Note 1
3	unsigned	m	m	m	m	Note 1
4	argument (xxx-argument)					
5	signed					
6	ToBeSigned					
7	argument (xxx-argument)					
8	algorithmIdentifier	m	m	m	m	A.7.4
9	encrypted					
10	xxx-argument	m	m	m	m	
11	securityParameters					A.7.2
12	xxx-result	m	m	m	m	

Conditionals:

c6: if p_signed then m else o

Notes.

1. xxx is any one of:

   coordinateShadowUpdate
   updateShadow
   requestShadowUpdate

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.7 Common Elements

The elements in the following subclauses are shared by more than one protocol.

A.7.1 Extensibility

The The DSP, DOP and DISP protocols require general conformance to the principles of extensibility, as defined in [ISO/IEC 9594-5 : 1995 | ITU-T Rec. X.519 (1993)].

A.7.2 Security Parameters

Item No.	Protocol Element	D Inv	D Resp	P Inv	P Resp	References/notes
1.	SecurityParameters	m	m	m	m	
2.	certification-path	c	c	c7	c7	
3.	name	m	m	c7	c7	
4.	time	m	o	c7	c7	
5.	random	m	o	c7	c7	
6.	target	c	c	o	o	

Conditionals:

c7: if p_signed_dsp then m else o

A.7.3 Certification Path

Item No.	Protocol Element	D Init	D Resp	P Init	P Resp	References/notes
1	CertificationPath	c	m	m	m	
2	Certificate	m	m	m	m	
3	toBeSigned	m	m	m	m	
4	algorithmIdentifier	m	m	m	m	A.7.4
5	encrypted	m	m	m	m	
6	version	m	m	m	m	Note 1
7	serialNumber	m	m	m	m	
8	signature	m	m	m	m	
9	issuer	m	m	m	m	
10	validity	m	m	m	m	
11	notBefore	m	m	m	m	
12	notAfter	m	m	m	m	
13	subject	m	m	m	m	
14	subjectPublicKey Info	m	m	m	m	
15	algorithm	m	m	m	m	
16	subjectPublicKey	m	m	m	m	
17	issuerUnique Identifier	o	o	o	o	Note 2
18	subjectUnique Identifier	o	o	m	m	Note 2

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Item No.	Protocol Element	D Init	D Resp	P Init	P Resp	References/notes
19	extension	o	c	m	m	Note 2
20	CertificatePair	o	o	o	o	
21	forward	o	o	o	o	Note 3
22	reverse	o	o	o	o	Note 3

Notes:

1. Must be 1, 2, or 3.
2. If either present, version must be least v2. See also A.3.4
3. At least one must be present. If both are present, issuer shall match subject.

A.7.4 Algorithm Identifier

Item No.	Protocol Element	D Init	D Resp	P Init	P Resp	Reference	Note
1	AlgorithmIdentifier	m	m	m	m	See above	Note 1
2	algorithm	-	-	m	m		
3	parameters	-	-	o	o		

Notes.

1. This is required for all the forms of authentication covered by this part of ISO/IEC ISP 15125.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex B
(normative)
Amendments and Technical Corrigenda

International standards are subject to constant review and revision by ISO/IEC Technical Committee concerned and by ITU-T. The following amendments and corrigenda are approved by ISO/IEC JTC1 and by ITU-T, but at the date of publication of this part of ISO/IEC ISP 15125 they were not yet incorporated in the text of the corresponding base standards as referenced in this part of ISO/IEC ISP 15125. The amendments and corrigenda as listed below are considered as normative references by 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)
- 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)
- 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)
- 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)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(informative)
Commonly Used Algorithms

This annex identifies commonly used algorithms. It is not necessary to follow the recommended practices when claiming conformance to this profile. Unless explicitly indicated, all algorithms have a NULL parameter.

C.1 Message Digests Algorithms

The following message digests algorithms may be used:

- Square mod N (as registered in X.509 (88)): deprecated
- MD2: { rsadsi digestAlgorithm(2) 2 }
- MD4: { rsadsi digestAlgorithm(2) 4 }
- MD5: { rsadsi digestAlgorithm(2) 5 }
- SHA: { algorithm 18 } Note: This is the NIST Secure Hash Algorithm
- MDC-2: { algorithm 19 } Note: DES-based hash algorithm (ANSI X93.1 Part 2)
- SHA-1: { algorithm 26 } Note: Fixed version of SHA

C.2 Reversible Public Key Algorithms

The following reversible public key algorithms may be used :

- RSA: Registration from X.509. The text suggests “rsaEncryption” might be better, as X.509 specifies no padding rules.
- RSA Encryption: per PKCS #1 (available from pkcs@rsa.com). OID is { rsadsi pkcs(1) pkcs-1(1) 1 }
- RSA Signature: ISO 9766 w/ signing and verifying functions. This is being published as ANSI X9.31 Part 1. { algorithm 11 }

C.3 Irreversible Public Key Algorithms

The following irreversible public key algorithms may be used :

- EIGamal: { dssig-algorithm encryption-algorithm(1) 1 }
- DSA: This is the NIST Digital Signature Algorithm, also X.9.30-1: { algorithm 12 }

  It carries a parameter, of type:

```
DSAParameters ::= SEQUENCE {
    modulusLength     INTEGER,  -- length of p in bits
    prime1        INTEGER,  -- modulus p
    prime2        INTEGER,  -- modulus q
    base      INTEGER }   -- base g
```

  Another version assumes the parameters are distributed by external means. This one is deprecated, since it can use the dsa ID.

```
dsa-common
    PARAMETER NULL ::= { algorithm 20 }
```

C.4 Key Agreement Algorithms

The following key agreement algorithms may be used :

- Diffie-Hellman:

```
Parameters ::= SEQUENCE {
    prime       INTEGER,  -- p
    base      INTEGER,  -- g
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

privateValueLength INTEGER OPTIONAL }

{ rsadsi pkcs(1) pkcs-3(3) 1 }

- Diffie-Hellman w/ Common Parameters (no parameter); deprecated:

  { algorithm 16 }

C.5 Signature Algorithms

The following signature algorithms may be used. These combine a hash and public key algorithm and are what is used in the "signature" field in a certificate, etc.

- Square-mod-n with RSA: From X.509 (deprecated).
- MD2 with RSA: This uses the X.509 version of RSA.

  { dssig-algorithm signatureAlgorithm(3) 1 }
- MD4 with RSA: { algorithm 2 }
- MD5 with RSA: { algorithm 3 }
- MD2 with RSA Encryption: Uses PKCS version of RSA.

  { rsadsi pkcs(1) pkcs-1(1) 2 }
- MD4 with RSA Encryption: Uses PKCS version of RSA.

  { algorithm 4 }
- MD5 with RSA Encryption: Uses PKCS version of RSA.

  { rsadsi pkcs(1) pkcs-1(1) 4 }
- MD2 with EIGamal:

  { dssig-algorithm signatureAlgorithm(3) 2 }
- DSA with SHA: (Carries DSAParameters) { algorithm 2 }
- DSA with SHA-1: { algorithm 27 }
- DSA Common With SHA: (DSA with common parameters) (deprecated) { algorithm 21 }
- MDC-2 with RSA Signature: { algorithm 14 }
- SHA with RSA Signature: { algorithm 15 }
- SHA-1 with RSA Signature: { algorithm 29 }
- MD2 with RSA Signature: { algorithm 22 }
- MD5 with RSA Signature: { algorithm 23 }

C.6 Symmetric Algorithms

The following symmetric algorithms may be used.

- DES-ECB: { algorithm 6 }
- DES-CBC: { algorithm 7 }; Carries an IV as a parameter
- DES-OFB: { algorithm 8 }; Carries an FBParameter as a parameter.

  FBParameter ::= SEQUENCE {

  iv IV,

  numberOfBits NumberOfBits }

  IV ::= OCTET STRING

  NumberOfBits ::= INTEGER -- Number of feedback bits (1-64)
- DES-CFP: { algorithm 9 }; Carries an FBParameter as the parameter.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- DES-MAC: { algorithm 10 }; Carries an INTEGER parameter, the length of the MAC (constrained by comment to 16, 24, 32, 40, 48, or 64 bits).
- DES-EDE: { algorithm 17 }; Triple DES in ECB mode, per ANSI X9.17.
- RC2-CBC: Proprietary symmetric block encryption algorithm from RSADSI:

  { rsadsi encryptionAlgorithm(3) 2 }

- RC4: Proprietary stream cipher algorithm from RSADSI:

  { rsadsi encryptionAlgorithm(3) 4 }

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

© ISO/IEC

ICS 35.100.05

Price based on 46 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale