

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



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

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.

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.

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”.

¹When 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).

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).

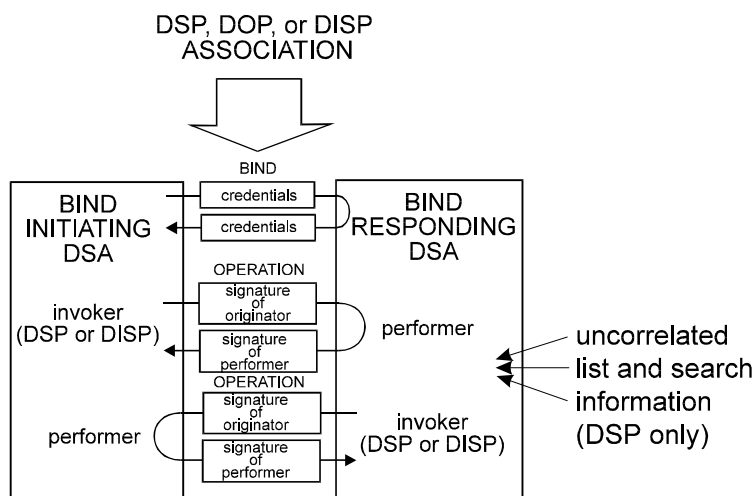


Figure 1 — Scenario

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.*

[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)

- 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 1 below. 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

²This specification defines Version 1 Certificates.

³ To be published.

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)

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:

- 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 accepted⁴
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.

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.

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:

⁶For 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.

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.

- 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.

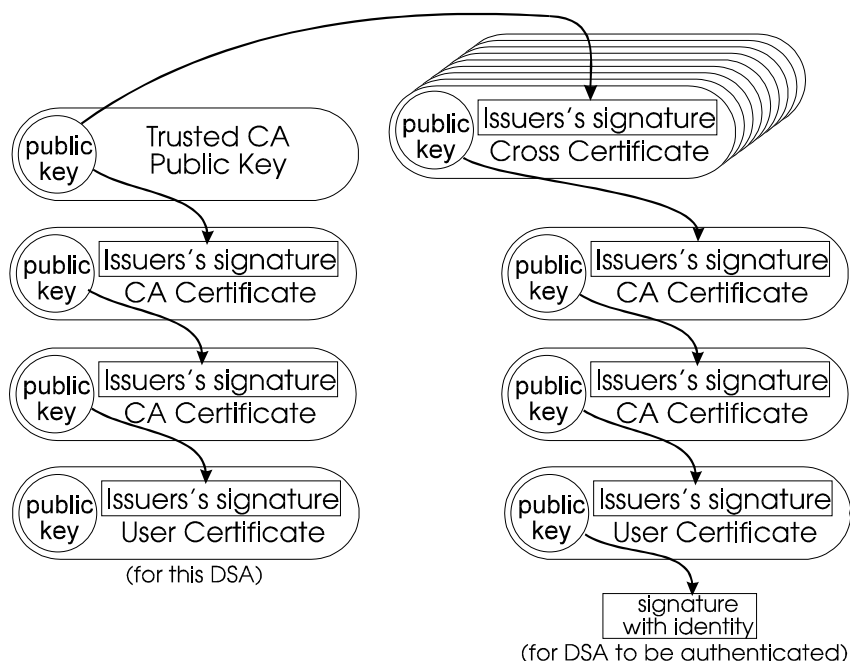


Figure 2 — Certificate Hierarchies and evaluation paths

There are two arrangements of CA that must be supported:

- 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.

- 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):

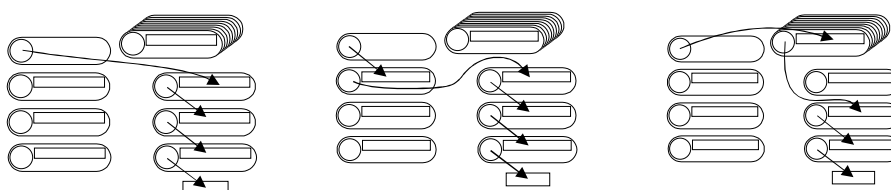


Figure 3 — Validation strategies

- 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

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.