INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 15125-10

First edition
1999-03-01

Information technology — International Standardized Profiles ADYnn — OSI Directory —

Part 10:
ADY51 — Shadowing using ROSE

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

Partie 10: ADY51 — Suivi utilisant ROSE

Reference number
ISO/IEC ISP 15125-10:1999(E)

Contents

Foreword

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

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

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

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

International Standardized Profile ISO/IEC ISP 15125-10 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 the 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 subsets*

— *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 a normative part of this part of ISO/IEC ISP 15125.

Introduction

The concept and structure of International Standardized Profiles for Information Systems are laid down in the Technical Report ISO/IEC TR 10000. The purpose of an International Standardized Profile is to recommend when and how certain information technology standards shall be used.

The International Standardized Profile, ISO/IEC ISP 15125, consists of a set of International Standardized Profile parts relating to the Directory as defined in the Technical Report ISO/IEC TR 10000-2.

This part of ISO/IEC ISP 15125 specifies application profile ADY51 (see TR 10000-2) which defines a set of capabilities and constraints on support of Directory Information Shadowing Protocol (DISP) by Directory System Agent (DSA) implementations when operating DISP over the Remote Operations Service Element (ROSE).

Information technology — International Standardized Profiles ADYnn — OSI Directory —

Part 10:
ADY51 — Shadowing using ROSE

1 Scope

1.1 General

This part of ISO/IEC ISP 15125 defines a set of DISP capabilities and constraints which a DSA implementation may support over ROSE. These capabilities and constraints cover the following areas:

- shadow supplier and consumer roles
- primary and secondary shadowing
- association initiator and responder functions
- all DISP operations
- error handling and recovery

The objective of this part of ISO/IEC ISP 15125 is therefore to define a level of DISP capability such that conforming DSA implementations shall be capable of establishing and maintaining DISP associations over ROSE together in a consistent manner.

ISO/IEC ISP 15125-11 defines the level of DISP capability which a DSA implementation may support over the Reliable Transport Service Element (RTSE).

This part of ISO/IEC ISP 15125 does not specify any requirements related to the administrative, management or functional capabilities associated with shadowed information transferred using DISP. Those aspects are covered by ISO/IEC ISP 15125-14 (ADY62 - Establishment and Utilisation of Shadowing Agreements) and ISO/IEC ISP 15125-12 (ADY53 - Shadowing Subsets).

1.2 Position within the taxonomy

This part of ISO/IEC ISP 15125 is identified in ISO/IEC TR 10000-2 as ADY51 "The Directory - Shadowing Capabilities - Shadowing using ROSE".

1.3 Scenario

In the Directory, replication of information between DSAs can be achieved by use of the standardized shadowing mechanism defined in ISO/IEC 9594-9: 1995 | ITU-T X.525: 1993 using DISP (see Figure 1).

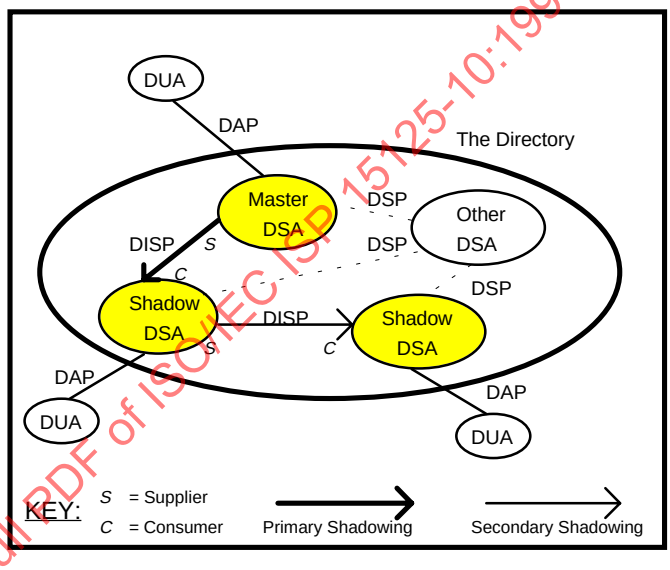

Figure 1- Shadowing using DISP

A shadowing agreement must be established between two DSAs and the role of each of the DSAs identified, that is which DSA is to operate as the shadow supplier and which as the shadow consumer.

A single DSA may operate as a shadow supplier in some agreements and as a shadow consumer in other agreements.

Primary shadowing occurs when a DSA supplies information mastered by that DSA to a shadowing DSA.

Secondary shadowing occurs when a DSA supplies shadowed information on to a shadowing DSA.

The transfer of information being shadowed (either primary or secondary) between supplier and consumer DSAs is achieved by use of DISP, which may operate over either ROSE or RTSE. This part of ISO/IEC ISP 15125 relates to DISP when operating over ROSE.

DISP is specified in ISO/IEC 9594-5: 1995 | ITU-T X.519: 1993.

2 Normative references

The following documents contain provisions which, through reference 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.

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.*

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

ISO/IEC 9594-2: 1995 | ITU-T Recommendation X.501: 1993, *Information technology - Open Systems Interconnection - The Directory: Models.*

ISO/IEC 9594-3: 1995 | ITU-T Recommendation X.511: 1993, *Information technology - Open Systems Interconnection - The Directory: Abstract service definition.*

ISO/IEC 9594-4: 1995 | ITU-T Recommendation X.518: 1993, *Information technology - Open Systems Interconnection - The Directory: Procedures for distributed operation.*

ISO/IEC 9594-5: 1995 | ITU-T Recommendation X.519: 1993, *Information technology - Open Systems Interconnection - The Directory: Protocol specifications.*

ISO/IEC 9594-6: 1995 | ITU-T Recommendation X.520: 1993, *Information technology - Open Systems Interconnection - The Directory: Selected attribute types.*

ISO/IEC 9594-7: 1995 | ITU-T Recommendation X.521: 1993, *Information technology - Open Systems Interconnection - The Directory: Selected object classes.*

ISO/IEC 9594-8: 1995 | ITU-T Recommendation X.509: 1993, *Information technology - Open Systems Interconnection - The Directory: Authentication framework.*

ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993, *Information technology - Open Systems Interconnection - The Directory: Replication.*

ISO/IEC 13712-1:1995 | ITU-T Recommendation X.880: 1994, *Information technology - Remote Operations: Concepts, model and notation.*

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

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

ISO/IEC 13248-4:—[1)], *Information technology - Open Systems Interconnection - The Directory: Protocol Information Conformance Statement (PICS) for the Directory Information Shadowing Protocol.*

Note. Relevant technical corrigenda which apply to the base standards included above are listed in Annex B of this part of ISO/IEC ISP 15125.

3 Definitions

Terms used in this part of ISO/IEC ISP 15125 are as defined in the Directory base standard, the following terms are as defined in ISO/IEC 9594-1: 1995 | ITU-T Recommendation X.500: 1993:

a) (the) Directory

The following terms are as defined in ISO/IEC 9594-2: 1993 | ITU-T Recommendation X.501: 1993:

a) Directory Information Tree

b) Directory System Agent

The following terms are as defined in ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993:

a) master DSA

b) primary shadowing

c) replication

d) secondary shadowing

e) shadow consumer

f) shadow supplier

g) shadowed DSA specific entry (SDSE)

h) shadowed information

i) shadowing

j) shadowing agreement

k) unit of replication

3.1 General

The following additional terms are defined for use in this part of ISO/IEC ISP 15125.

3.1.1 Manager Advice Action

A local action, outside the scope of this part of ISO/IEC ISP 15125, which a DSA implementation may optionally perform in order to notify the manager or administrator of the DSA that an error or unexpected occurrence has been detected in relation to procedures defined by this part of ISO/IEC ISP 15125.

1) To be published.

3.1.2 Protocol Action

An action which a DSA implementation may perform upon detection of an error or unexpected occurrence in relation to a particular shadowing agreement, resulting in the generation of one or more protocol exchanges on the relevant association.

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 : Support of this feature must be implemented by a DSA.

3.2.2 optional; o : Support of the feature is left to the implementor of the DSA.

3.2.3 conditional; c : The requirement to support the feature is dependent on a specified condition. The condition and the resulting support requirements are stated separately.

3.2.4 out of scope; i : Support of the feature is outside the scope of this part of ISO/IEC 15125.

4 Abbreviations

APDU	Application Protocol Data Unit
DAP	Directory Access Protocol
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DSA	Directory System Agent
DSE	DSA-Specific Entry
DSP	Directory System Protocol
DUA	Directory User Agent
ISP	International Standardized Profile
PICS	Protocol Implementation Conformance Statement
PRL	Profile Requirements List
ROSE	Remote Operations Service Element
RTSE	Reliable Transport Service Element
SDSE	Shadowed DSA-Specific Entry

5 Conformance

This part of ISO/IEC ISP 15125 states requirements upon DSA implementations in order to achieve DISP interworking. DUA conformance is not applicable.

A claim of conformance to this part of ISO/IEC ISP 15125 is a claim that all requirements in the base standard, ISO/IEC 9594: 1995 | ITU-T Recommendation Series X.500: 1993, are satisfied and that all requirements in the following clauses and in Annex A of this part of ISO/IEC ISP 15125 are also satisfied.

Annex A states the relationship between the requirements of this part of ISO/IEC ISP 15125 and those of the base standard.

5.1 Conformance statement

For each DSA implementation claiming conformance to this part of ISO/IEC ISP 15125, an appropriate PICS shall be produced stating support or non-support of each option identified in this part of ISO/IEC ISP 15125.

The PICS shall satisfy the requirements of the PRL in Annex A of this part of ISO/IEC ISP 15125. The PICS shall also satisfy all requirements defined in either 9.3.1 (for shadow supplier conformance) or 9.4.1 (for shadow consumer conformance) or both 9.3.1 and 9.4.1 (for shadow supplier and consumer conformance) in ISO/IEC 9594-5: 1995 | ITU-T Recommendation X.519: 1993.

5.2 Conformance requirements

To conform as a shadow supplier to this part of ISO/IEC ISP 15125, a DSA implementation shall conform to the static requirements defined in 9.3.2 and the dynamic requirements defined in 9.3.3 of ISO/IEC 9594-5: 1995 | ITU-T Recommendation X.519: 1993, including all requirements referenced directly and indirectly from those clauses for support of one or both of the application contexts, **shadowSupplierInitiatedAC** and **shadowConsumerInitiatedAC**.

To conform as a shadow consumer to this part of ISO/IEC ISP 15125, a DSA implementation shall conform to the static requirements defined in 9.4.2 and dynamic requirements defined in 9.4.3 of ISO/IEC 9594-5: 1995 | ITU-T Recommendation X.519: 1993, including all requirements referenced directly and indirectly from those clauses for support of one or both of the application contexts, **shadowSupplierInitiatedAC** and **shadowConsumerInitiatedAC**.

A DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 which supports the application context **shadowSupplierInitiatedAC** may optionally support the variant asynchronous application context **shadowSupplierInitiatedAsynchronousAC**.

A DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 which supports the application context **shadowConsumerInitiatedAC** may optionally support the variant asynchronous application context **shadowConsumerInitiatedAsynchronousAC**.

A DSA implementation may therefore claim conformance to this part of ISO/IEC ISP 15125 as either a shadow supplier or a shadow consumer (or both), supporting either the supplier initiated or consumer initiated (or both) application contexts and optionally (if the relevant synchronous application context is supported) either of the asynchronous

supplier initiated or asynchronous consumer initiated application contexts.

The procurer of DSA products which claim conformance to this part of ISO/IEC ISP 15125 is therefore recommended to ensure that the products conform to the particular roles and application contexts which will permit interworking within the procurer's environment. In summary, DSA products must conform to mutually acceptable roles and the same application context in order to permit interworking.

6 Static conformance requirements

In addition to the conformance requirements stated in clause 5 above, a DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 shall also conform to the static requirements specified in the remainder of this clause 6 and in the PRL, Annex A.

6.1 Security Level

To conform to this part of ISO/IEC ISP 15125, a DSA implementation shall be capable of performing DISP peer entity authentication of DSAs using the following security level:

- simple authentication with unprotected password

To conform to this part of ISO/IEC ISP 15125, a DSA implementation shall conform to the simple unprotected authentication requirements specified in ISO/IEC ISP 15125-7.

Support of the following security levels is optional:

- simple authentication without password
- simple authentication with protected password
- strong authentication

A DSA implementation which supports one or more of the simple authentication without password, simple authentication with protected password or strong authentication security levels shall conform to the corresponding requirements for those levels specified in ISO/IEC ISP 15125-7.

It is recommended that when a DSA implementation conforming to this part of ISO/IEC ISP 15125 does support the optional simple authentication without password security level, that level should only be exploited by the procurer when operating within a controlled and trusted environment.

The remaining security levels are outside the scope of this part of ISO/IEC ISP 15125, namely:

- none
- external authentication procedures

Note. The security level "none" is deemed out of scope as the standardized shadowing mechanism defined in ISO/IEC 9594-9: 1995 | ITU-T X.525: 1993 requires that a shadowing agreement identifier be unique within the relationship between a shadow supplier and shadow consumer DSA. In order to meet that requirement it shall be necessary that DSA names are known.

6.2 Unit of replication

In order to define to what degree the unit of replication is supported, a DSA implementation shall claim conformance to at least one of the functional shadowing subsets defined in ISO/IEC ISP 15125-12.

Note. In order to allow interworking, the procurer of DSA products which claim conformance to this part of ISO/IEC ISP 15125 is recommended to ensure that those products also conform to compatible functional shadowing subsets defined in ISO/IEC ISP 15125-12.

6.3 Secondary Shadowing

A DSA implementation may optionally provide the capability to support secondary shadowing, that is to act as a shadow supplier of a replicated area within the DIT which has been obtained as a shadow consumer.

7 Dynamic conformance requirements

In addition to the conformance requirements stated in clauses 5 and 6 above, a DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 shall also conform to the dynamic requirements specified in the remainder of this clause 7.

A DSA implementation shall support all procedures and capabilities specified in the Directory base standard, ISO/IEC 9594: 1993 | ITU-T Recommendation Series X.500: 1993, which relate to DISP operations and protocol elements for which support is claimed in the PICS.

A DSA implementation shall also conform to the requirements specified in the following clauses and in the PRL, Annex A, and to all procedures specified in the Directory base standard as amended by the corrigenda and defect reports listed in Annex B.

7.1 Operational exchange

A DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 shall be capable, when operating in an initiator role, of supporting at least one operational exchange within a single, established DISP association, consisting of either a **coordinateShadowUpdate** or a **requestShadowUpdate** operation (depending on the application context in use on the association) plus an **updateShadow** operation. When operating in a responder role, a DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 may support one or more of such operational exchanges.

The following sub-clauses define conformance requirements for each of the **coordinateShadowUpdate**, **requestShadowUpdate** and **updateShadow** operations. The use of **EXTERNAL** strategy types in conjunction with each of these operations is outside the scope of this part of ISO/IEC ISP 15125. In order to provide efficient Directory shadowing, it is recommended, but not mandated, that DSA implementations support the incremental update strategy type.

7.1.1 CoordinateShadowUpdate operation

A DSA shall be capable of supporting the standard update strategy types, **noChanges** and **total**. A DSA may optionally support the standard update strategy type, **incremental**.

A DSA shall always include the **lastUpdate** time element except when coordinating the first update within a shadowing agreement or when the shadow consumer requires that a full update be coordinated.

7.1.2 RequestShadowUpdate operation

A DSA shall be capable of supporting the standard requested strategy type, **total**. A DSA may optionally support the standard requested strategy type, **incremental**.

A DSA shall always include the **lastUpdate** time element except when requesting the first update within a shadowing agreement or when requesting a full update.

7.1.3 UpdateShadow operation

A DSA shall be capable of supporting the standard updated information types, **noRefresh** and **total**. A DSA may optionally support the standard updated information type, **incremental**.

A DSA receiving an **updateShadow** request shall return a succesful result on receipt of the complete APDU unless it is invalid or one of the error conditions defined in clause 8.3 has been detected.

Note. A successful response therefore means that the updates have been received; it does not guarantee that they have been applied.

7.2 Limits

This part of ISO/IEC ISP 15125 does not define any specific limits to which a DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 shall adhere but does include recommendations related to limits in 7.2.1 and 7.2.2 below.

7.2.1 DISP APDU size

It is recommended that a supplier or consumer DSA implementation claiming conformance to this part of ISO/IEC ISP 15125 should be capable of handling a single DISP APDU of at least 50 megabytes.

7.2.2 Local limits

A DSA implementation may impose minimum or maximum limits locally, for example on the number of defined shadowing agreements or the number of concurrently open DISP associations.

It is recommended that if a local limit is exceeded which indicates a transient condition within a DSA implementation, an **insufficientResources** shadow problem should be notified.

It is recommended that if a local limit is exceeded which indicates a permanent condition within a DSA implementation, an **unwillingToPerform** shadow problem should be notified and the association aborted.

The procurer of a DSA product is recommended to ensure that any local limits imposed by a DSA implementation do not conflict with the requirements of the procurer.

7.3 Shadow update requests - no changes

A DSA which conforms to this part of ISO/IEC ISP 15125 and supports the application context **shadowConsumerinitiatedAC** or **shadowConsumerinitiatedAsynchronousAC** shall, as a shadow supplier, accept a **requestShadowUpdate** operation when no modifications have been applied to the replicated information since the last shadow update.

If the requested strategy is incremental, the supplier DSA shall invoke an **updateShadow** operation with the **incrementalRefresh** set to be an empty sequence.

If the requested strategy is total, the supplier DSA shall invoke an **updateShadow** operation including a total refresh of the shadowed information.

7.4 Unknown SDSE modification

A DSA which conforms to this part of ISO/IEC ISP 15125 as a shadow consumer and which supports incremental refreshment shall, upon receipt of an incremental update containing a modification to an SDSE of which it has no record, perform the following procedure:

If there is no **rename** component within the **ContentChange** received and **attributeChanges** contains a **replace** component, the DSA shall create an appropriate SDSE. Otherwise, the DSA shall return a shadow problem, **invalidInformationReceived**, if no response has already been generated for the operation.

8 Error and recovery procedures

This clause defines the procedures that a DSA implementation conforming to this part of ISO/IEC ISP 15125 shall follow in order to handle and recover from each of the possible error conditions that may be encountered on a DISP operation.

Note. The term “suspend” is used in the remainder of this clause 8 in relation to shadowing agreements. In this case, to “suspend” a shadowing agreement means to move the shadowing agreement from the active state to the inactive state.

8.1 CoordinateShadowUpdate operation

Clause 11.1.3 of ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 defines the errors which can be returned for this operation and the circumstances under which they may occur. The following sub-clauses define how a DSA implementation which claims conformance to this part of ISO/IEC ISP 15125 shall handle and recover from each of those error conditions.

8.1.1 Invalid Agreement ID

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.1.2 Inactive Agreement

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.1.3 Unsupported Strategy

If the supplier DSA selected **incremental**, it shall invoke a further **coordinateShadowUpdate** operation within the current window, if possible, proposing an **updateStrategy** of **total**. **coordinateShadowUpdate** operations invoked in subsequent windows shall select **total updateStrategy** in preference to **incremental**.

If the supplier DSA selected **total**, the consumer DSA shall not issue the **unsupportedStrategy** error.

If the supplier DSA selected **noChange**, the consumer DSA shall not issue the **unsupportedStrategy** error.

8.1.4 Missed Previous

The shadow consumer DSA shall supply in the error the time, provided by the supplier, for the most recent successful update processed by the consumer.

The **lastUpdate** time received with the error shall be used by the supplier DSA for the next update. The **updateStrategy** used for the next update shall depend on the shadowing agreements between the DSAs. If **incremental updateStrategy** is permitted, and sufficient information about the changes to the replicated area for the revised **lastUpdate** time is held by the supplier DSA, the **incremental updateStrategy** shall be used. Otherwise the **total updateStrategy** shall be used. The supplier DSA shall invoke a further **coordinateShadowUpdate** operation within the current window, if possible.

8.1.5 Full Update Required

The supplier DSA shall use the **total updateStrategy** for the next update exchange. The supplier DSA shall invoke a further **coordinateShadowUpdate** operation within the current window, if possible, proposing an **updateStrategy** of **total**.

8.1.6 Unwilling to Perform

ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 states that interpretation of this shadow problem is outside the scope of the Directory Specifications.

This part of ISO/IEC ISP 15125 interprets the return of this shadow problem as indicating a permanent condition associated with the particular shadowing agreement. This shadow problem shall be returned for any permanent error conditions not covered by any of the other shadow problems.

The supplier DSA may take suitable Manager Advice Action and suspend the shadowing agreement, but there shall be no protocol action taken.

8.1.7 Unsuitable Timing

The shadow consumer DSA shall propose a suitable time in the error response.

The supplier DSA shall reschedule the update to occur at the proposed time if it is suitable. If the proposed time is unsuitable, the supplier DSA may take Manager Advice Action, but there shall be no protocol action taken. The next update shall occur at the next scheduled time.

8.1.8 Update Already Received

There are several reasons why a consumer DSA may return the **UpdateAlreadyReceived** error. These include:

- The supplier DSA's Information Tree has been restored from a backup. For a primary shadow, this implies that the information held in the consumer DSA is invalid and should be replaced by a update using the **total updateStrategy**. For a secondary shadow, no action needs to be taken, because the supplier DSA should eventually be brought up to date with the master DSA.

- The consumer DSA received the last update and successfully stored it in its DSA Information Tree, but the positive response to the **updateShadow** operation was lost in transit. No action needs to be taken.

Because the different scenarios require differing actions for recovery, and the DSAs cannot distinguish between the different scenarios, manual management intervention is required. Therefore, no action shall be taken other than a suitable Manager Advice Action.

Note. ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 only recognises use of the **lastUpdate** element with the **missedPrevious** problem. This part of ISO/IEC ISP 15125 recommends that the consumer DSA supplies a **lastUpdate** value with the **updateAlreadyReceived** problem to aid possible resynchronisation.

8.1.9 Invalid Sequencing

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.1.10 Insufficient Resources

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.2 RequestShadowUpdate operation

Clause 11.2.3 of ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 defines the errors which can be returned for this operation and the circumstances under which they may occur. The following sub-clauses define how a DSA implementation which claims conformance to this part of ISO/IEC ISP 15125 shall handle and recover from each of those error conditions.

8.2.1 Invalid Agreement ID

The consumer DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the consumer DSA may optionally suspend the agreement.

8.2.2 Inactive Agreement

The consumer DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the consumer DSA may optionally suspend the agreement.

8.2.3 Unsupported Strategy

If the consumer DSA selected **incremental**, it shall invoke a further **requestShadowUpdate** operation within the current window, if possible, proposing an **updateStrategy** of **total**. **requestShadowUpdate** operations invoked in subsequent windows shall select **total updateStrategy** in preference to **incremental**.

If the consumer DSA selected **total**, the supplier DSA shall not issue the **unsupportedStrategy** error.

If the consumer DSA selected **noChange**, the supplier DSA shall not issue the **unsupportedStrategy** error.

8.2.4 Full Update Required

The consumer DSA shall use the **total updateStrategy** for the next update exchange. The consumer DSA shall invoke a further **requestShadowUpdate** operation within the current window, if possible, proposing an **updateStrategy** of **total**.

8.2.5 Unwilling to Perform

ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 states that interpretation of this shadow problem is outside the scope of the Directory Specifications.

This part of ISO/IEC ISP 15125 interprets the return of this shadow problem as indicating a permanent condition associated with the particular shadowing agreement. This shadow problem shall be returned for any permanent error conditions not covered by any of the other shadow problems.

The consumer DSA may take suitable Manager Advice Action and suspend the shadowing agreement, but there shall be no protocol action taken.

8.2.6 Unsuitable Timing

The shadow supplier DSA shall propose a suitable time in the error response.

The consumer DSA shall reschedule the update to occur at the proposed time if it is suitable. If the proposed time is unsuitable, the consumer DSA may take Manager Advice Action, but there shall be no protocol action taken. The next update shall occur at the next scheduled time.

8.2.7 Invalid Sequencing

The consumer DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the consumer DSA may optionally suspend the agreement.

8.2.8 Insufficient Resources

The consumer DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.3 UpdateShadow operation

Clause 11.3.3 of ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 defines the errors which can be returned for this operation and the circumstances under which they may occur. The following sub-clauses define how a DSA implementation which claims conformance to this part of ISO/IEC ISP 15125 shall handle and recover from each of those error conditions.

8.3.1 Invalid Agreement ID

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.3.2 Inactive Agreement

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.3.3 Invalid Information Received

ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 states that interpretation of this shadow problem is outside the scope of the Directory Specifications.

According to clause 7.1.3 of this part of ISO/IEC ISP 15125, a consumer DSA shall return a successful response to an **updateShadow** request on receipt of a complete APDU unless it is invalid or one of the error conditions defined in this clause 8.3 has been detected. This part of ISO/IEC ISP 15125 therefore recognises that an error condition which would result in an **invalidInformationReceived** shadow problem shall typically not be detected until after a successful response has been returned. It is recommended that the consumer DSA takes suitable Manager Advice Action upon detection of such a condition, but there shall be no protocol action taken.

8.3.4 Unwilling to Perform

ISO/IEC 9594-9: 1995 | ITU-T Recommendation X.525: 1993 states that interpretation of this shadow problem is outside the scope of the Directory Specifications.

This part of ISO/IEC ISP 15125 interprets the return of this shadow problem as indicating a permanent condition associated with the particular shadowing agreement. This shadow problem shall be returned for any permanent error conditions not covered by any of the other shadow problems.

The supplier DSA may take suitable Manager Advice Action and suspend the shadowing agreement, but there shall be no protocol action taken.

8.3.5 Invalid Sequencing

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

8.3.6 Insufficient Resources

The supplier DSA may take suitable Manager Advice Action, but there shall be no protocol action taken.

In order to avoid a possible loop situation, whereby this error is being returned every time the operation is issued for a particular shadowing agreement, the supplier DSA may optionally suspend the agreement.

Annex A

(normative)

Profile Requirements List for ADY51 Shadowing using ROSE

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 15125 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 implementor´s PICS for an implementation conformant to this part of ISO/IEC ISP 15125.

The abbreviations used in the table headings in this Annex are as follows:

D - conformance requirement as defined in the base standard, ISO/IEC 9594: 1995 | ITU-T Recommendation series X.500: 1993

P - conformance requirement as defined in this part of ISO/IEC ISP 15125

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

Conformance requirements apply to both initiator and responder roles. Where protocol elements are nested, the conformance requirements are of relevance only when the immediately containing protocol element is transmitted or received.

A.1 Identification of the Implementation

A.1.1 Identification of PICS

(void)

A.1.2 Identification of the implementation and/or system

(void)

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

(void)

A.2 Identification of the Protocol

Ref.No.	Question	Response
1	Title, Reference Number and publication date of the protocol standard	ISO/IEC 9594: 1995 | ITU-T Recommendation series X.500: 1993, *Information technology - Open Systems Interconnection - The Directory* Directory Information Shadowing Protocol
2	Protocol Version Number	Version 1
3	Implemented Addenda	None
4	Implementor's Guide Version Number	See Annex B
5	Implemented Defect Reports (Ref.No.)	See Annex B

A.3 Global Statement of Conformance

Ref.No.	Question	D	P	Predicate	Notes
1	Is security level "none" for peer entity authentication supported?	o.1	i		
2	Is security level "simple without password" for peer entity authentication supported?	o.1	o	Simp-no-pass	
3	Is security level "simple with unprotected password" for peer entity authentication supported?	o.1	m	Simp-unprotect	
4	Is security level "simple with protected password" for peer entity authentication supported?	o.1	o	Simp-protect	
5	Is security level "strong" for peer entity authentication supported?	o.1	o	Strong-auth	
6	Are signed DISP operations supported?	o	o	Signed-ops	
7	Is the incremental update strategy supported?	o	o	Inc-updates	
8	Is secondary shadowing supported?	o	o		

o.1 : At least one of the security levels for peer entity authentication shall be supported.

A.4 Capabilities and Options

A.4.1 Supported Application Contexts

Ref.No.	Application Context	D	P
1	Shadow Supplier Initiated application context	o	o.2
2	Shadow Supplier Initiated Asynchronous application context	o	c.1
3	Shadow Consumer Initiated application context	o	o.2
4	Shadow Consumer Initiated Asynchronous application context	o	c.2
5	Reliable Shadow Supplier Initiated application context	o	i
6	Reliable Shadow Consumer Initiated application context	o	i

o.2 : At least one of the Shadow Supplier initiated or Shadow Consumer initiated application contexts shall be supported.

c.1 : If the response to A.4.1/1 is "Yes" then o else i.

c.2 : If the response to A.4.1/3 is "Yes" then o else i.

A.4.2 Operations

Ref.No.	Operation	Reference	D	P
1	DSA Bind	A.4.3.1	m	m
2	DSA Unbind	A.4.3.2	m	m
3	Coordinate Shadow Update	A.4.3.3	c.1	c.1
4	Request Shadow Update	A.4.3.4	c.2	c.2
5	Update Shadow	A.4.3.5	m	m

c.1 : If the response to A.4.1/1 is "Yes" then m else o.

c.2 : If the response to A.4.1/3 is "Yes" then m else o.

A.4.3 Protocol Elements

A.4.3.1 DSA Bind Protocol Elements

A.4.3.1.1 DSA Bind Arguments

Ref.No.	Element	Reference	D	P	Supported[1] Values or Notes
1	Directory Bind Argument		m	m	
2	credentials		c.3	m	
3	simple		c.4	m	
4	name		m	m	
5	validity		o	c.5	
6	time1		o	m	
7	time2		o	i	
8	random1		o	m	
9	random2		o	i	
10	password		c.6	m	
11	unprotected		c.7	m	
12	protected		c.5	c.5	
13	algorithm identifier		m	m	
14	encrypted		m	m	
15	strong		c.8	c.8	
16	certification-path		o	m	
17	bind-token		m	m	
18	to-be-signed		m	m	
19	algorithm		m	m	
20	name		m	m	
21	time		m	m	
22	random		m	m	
23	algorithm identifier		m	m	
24	encrypted		m	m	
25	name		o	m	
26	externalProcedure		i	i	
27	versions		m	m	v1(0)

Note 1. Only the specified values shall be supported unless noted otherwise.

c.3 : If Simp-no-pass or Simp-unprotect or Simp-protect or Strong-auth then m else o.

c.4 : If Simp-no-pass or Simp-unprotect or Simp-protect then m else o.

c.5 : If Simp-protect then m else o.

c.6 : If Simp-unprotect or Simp-protect then m else o.

c.7 : If Simp-unprotect then m else o.

c.8 : If Strong-auth then m else o.

A.4.3.1.2 DSA Bind Result

Ref.No.	Element	Reference	D	P	Supported[1] Values or Notes
1	Directory Bind Argument		m	m	
2	credentials		c.3	m	
3	simple		c.4	m	
4	name		m	m	
5	validity		o	c.5	
6	time1		o	m	
7	time2		o	i	
8	random1		o	m	
9	random2		o	i	
10	password		c.6	m	
11	unprotected		c.7	m	
12	protected		c.5	c.5	
13	algorithm identifier		m	m	
14	encrypted		m	m	
15	strong		c.8	c.8	
16	certification-path		o	m	
17	bind-token		m	m	
18	to-be-signed		m	m	
19	algorithm		m	m	
20	name		m	m	
21	time		m	m	
22	random		m	m	
23	algorithm identifier		m	m	
24	encrypted		m	m	
25	name		o	m	
26	externalProcedure		i	i	
27	versions		m	m	v1(0)

Note 1. Only the specified values shall be supported unless noted otherwise.

c.3 : If Simp-no-pass or Simp-unprotect or Simp-protect or Strong-auth then m else o.

c.4 : If Simp-no-pass or Simp-unprotect or Simp-protect then m else o.

c.5 : If Simp-protect then m else o.

c.6 : If Simp-unprotect or Simp-protect then m else o.

c.7 : If Simp-unprotect then m else o.

c.8 : If Strong-auth then m else o.

A.4.3.1.3 DSA Bind Error

Ref.No.	Element	Reference	D	P	Supported[1] Values or Notes
1	Directory Bind Error		m	m	
2	versions		m	m	v1(0)[2]
3	error		m	m	
4	serviceError		m	m	unavailable
5	securityError		m	m	inappropriate-Authentication, invalid-Credentials

Note 1. Only the specified values shall be supported unless noted otherwise.

Note 2. When indicating a Directory bind error, a DSA implementation may indicate versions that it supports other than those within the scope of this part of ISO/IEC ISP 15125.

A.4.3.2 DSA Unbind Protocol Element

DSA Unbind has no protocol elements (refer to clause 11.2 of ISO/IEC 9594-4: 1995 | ITU-T Recommendation X.518: 1993).

A.4.3.3 Coordinate Shadow Update Protocol Elements

Ref.No.	Element	Reference	D	P
1	Coordinate Shadow Update Argument		o	c.1
2	unsigned		o	m
3	argument (coordinateShadowUpdateArgument)		o	m
4	signed		c.9	c.9
5	to-be-signed		m	m
6	argument (coordinateShadowUpdateArgument)		m	m
7	algorithm-identifier		m	m
8	encrypted		m	m
9	agreementID		o	m
10	lastUpdate		o	m
11	updateStrategy		i	m
12	standard		o	m
13	other		o	i
14	securityParameters		c.9	c.9
15	certification-path		o	m
16	name		m	m
17	time		m	m
18	random		m	m
19	target		o	o
20	Coordinate Shadow Update Result		o	c.1

c.1 : If the response to A.4.1/1 is "Yes" then m else o.

c.9 : If Signed-ops then m else o.

A.4.3.4 Request Shadow Update Protocol Elements

Ref.No.	Element	Reference	D	P
1	Request Shadow Update Argument		o	c.2
2	unsigned		o	m
3	argument (requestShadowUpdateArgument)		o	m
4	signed		c.9	c.9
5	to-be-signed		m	m
6	argument (requestShadowUpdateArgument)		m	m
7	algorithm-identifier		m	m
8	encrypted		m	m
9	agreementID		o	m
10	lastUpdate		o	m
11	requestedStrategy		o	m
12	standard		o	m
13	other		i	i
14	securityParameters		c.9	c.9
15	certification-path		o	m
16	name		m	m
17	time		m	m
18	random		m	m
19	target		o	o
20	Request Shadow Update Result		o	c.2

c.2 : If the response to A.4.1/3 is "Yes" then m else o.

c.9 : If Signed-ops then m else o.