INTERNATIONAL STANDARD

ISO/IEC 9594-9

First edition
1995-09-15

Information technology — Open Systems Interconnection — The Directory: Replication

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'Annuaire: Réplication

INTERNATIONAL

Reference number
ISO/IEC 9594-9:1995(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. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 9594-9 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.525.

Implementors should note that a defect resolution process exists and that corrections may be applied to this part of ISO/IEC 9594 in the form of technical corrigenda. A list of approved technical corrigenda for this part of ISO/IEC 9594 can be obtained from the subcommittee secretariat. Published technical corrigenda are available from your national standards organization.

ISO/IEC 9594 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — The Directory*:

- *Part 1: Overview of concepts, models and services*
- *Part 2: Models*
- *Part 3: Abstract service definition*
- *Part 4: Procedures for distributed operation*
- *Part 5: Protocol specifications*
- *Part 6: Selected attribute types*
- *Part 7: Selected object classes*
- *Part 8: Authentication framework*
- *Part 9: Replication*

Annex A forms an integral part of this part of ISO/IEC 9594.

Introduction

This Recommendation | International Standard, together with other Recommendations | International Standards, has been produced to facilitate the interconnection of information processing systems to provide directory services. A set of such systems, together with the directory information which they hold, can be viewed as an integrated whole, called the *Directory*. The information held by the Directory, collectively known as the Directory Information Base (DIB) is typically used to facilitate communication between, with or about objects such as application-entities, people, terminals and distribution lists.

The Directory plays a significant role in Open Systems Interconnection, whose aim is to allow, with a minimum of technical agreement outside of the interconnection standards themselves, the interconnection of information processing systems:

- from different manufacturers;
- under different managements;
- of different levels of complexity; and
- of different ages.

This Recommendation | International Standard defines the replication capabilities provided by DSAs to improve the level of service to Directory users.

Annex A, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for the directory shadow abstract service.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – THE DIRECTORY: REPLICATION

1 Scope

This Recommendation | International Standard specifies a shadow service which DSAs may use to replicate Directory information. The service allows Directory information to be replicated among DSAs to improve service to Directory users. The shadowed information is updated, using the defined protocol, thereby improving the service provided to users of the Directory.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard part. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.500 (1993) | ISO/IEC 9594-1:1995, *Information Technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.*
- ITU-T Recommendation X.501 (1993) | ISO/IEC 9594-2:1995, *Information Technology – Open Systems Interconnection – The Directory: Models.*
- ITU-T Recommendation X.511 (1993) | ISO/IEC 9594-3:1995, *Information Technology – Open Systems Interconnection – The Directory: Abstract service definition.*
- ITU-T Recommendation X.518 (1993) | ISO/IEC 9594-4:1995, *Information Technology – Open Systems Interconnection – The Directory: Procedures for distributed operation.*
- ITU-T Recommendation X.519 (1993) | ISO/IEC 9594-5:1995, *Information Technology – Open Systems Interconnection – The Directory: Protocol specifications.*
- ITU-T Recommendation X.520 (1993) | ISO/IEC 9594-6:1995, *Information Technology – Open Systems Interconnection – The Directory: Selected attribute types.*
- ITU-T Recommendation X.521 (1993) | ISO/IEC 9594-7:1995, *Information Technology – Open Systems Interconnection – The Directory: Selected object classes.*
- ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1995, *Information Technology – Open Systems Interconnection – The Directory: Authentication framework.*
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1:1995, *Information Technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*
- ITU-T Recommendation X.681 (1994) | ISO/IEC 8824-2:1995, *Information Technology – Abstract Syntax Notation One (ASN.1): Information object specification.*
- ITU-T Recommendation X.682 (1994) | ISO/IEC 8824-3:1995, *Information Technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- ITU-T Recommendation X.683 (1994) | ISO/IEC 8824-4:1995, *Information Technology – Abstract Syntax Notation One (ASN.1): Parametrization of ASN.1 specifications.*

- ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1:1995, *Information technology – Remote Operations: Concepts, model and notation.*
- ITU-T Recommendation X.881 (1994) | ISO/IEC 13712-2:1995, *Information technology – Remote Operations: OSI realizations – Remote Operations Service Element (ROSE) service definition.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.200 (1988), *Reference Model of Open Systems Interconnection for CCITT Applications.*

  ISO 7498:1984, *Information processing systems — Open Systems Interconnection — Basic Reference Model.*

3 Definitions

For the purposes of this CCITT Recommendation | International Standard, the following definitions apply.

3.1 Basic directory definitions

The following terms are defined in CCITT Rec. X.500 | ISO/IEC 9594-1;

- *(the) Directory.*

3.2 Directory model definitions

The following terms are defined in CCITT Rec. X.501 | ISO/IEC 9594-2;

a) *distinguished name;*

b) *Directory Information Tree;*

c) *DSA Specific Entry;*

d) *DSA Information Model;*

e) *DSA Information Tree;*

f) *Directory System Agent.*

3.3 Distributed operation definitions

The following terms are defined in CCITT Rec. X.518 | ISO/IEC 9594-4;

a) *access point;*

b) *knowledge information;*

c) *name resolution;*

d) *naming context;*

e) *non-specific subordinate reference;*

f) *subordinate reference.*

3.2 Replication definitions

The following terms are defined in this Recommendation | International Standard:

area prefix: The sequence of RDNs and associated administrative information common to all entries within a replicated area.

attribute completeness: Indicates whether or not all user attributes are included in an entry-copy.

cache-copy: A copy of an entry (or part of an entry) whose consistency with its corresponding entry is maintained by means outside the scope of this Directory Specification.

caching: The process of creating cache copies. This process is outside the scope of this Directory Specification.

consumer reference: The access point of the shadow consumer.

entry-copy: Shadowed information from an entry.

extended knowledge: Those subordinate and non-specific subordinate references that would be included as subordinate knowledge if the replicated area were extended to the lower boundary of the naming context.

master DSA: The DSA which has administrative authority for a naming context. All adds, deletes and modifications to entries in this naming context are done by the master DSA. The master DSA may enter into shadowing agreements with other DSAs to provide copies of a subset of a naming context (see unit of replication).

primary shadowing: Shadowing where the shadow supplier is the master DSA.

replicated area: A subtree of the DIT for purposes of shadowing.

replication: The process by which copies of entry and operational information are held by DSAs other than the master DSA.

replication basc entry: The distinguished name of the root vertex of a replicated area.

secondary shadowing: Shadowing where the shadow supplier is not the master DSA.

shadow consumer: A DSA that receives shadowed information.

shadow operational binding: The relationship between two DSAs, one acting as a supplier of replicated information and the other as its consumer.

shadow service: The service provided to perform shadowing between two DSAs that have entered into one or more shadowing agreements.

shadow supplier: A DSA that provides shadowed information. This DSA may or may not be the master DSA.

shadowed DSA specific entry (SDSE): A unit of shadowed information which is associated with a specific name; it represents the information taken from a DSE which is shadowed.

shadowed information: The complete set of information associated with a unit of replication. Shadowed information is conceptually held both by the shadow supplier and the shadow consumer for the purposes of the shadow protocol and comprises a tree shaped structure of shadowed DSEs.

shadowing: Replication between two DSAs whereby shadowed information is copied and maintained using the Directory Information Shadowing Protocol.

shadowing agreement: The terms specific to a particular agreement required for shadowing to occur between a pair of DSAs.

subordinate completeness: Indicates whether or not subordinate knowledge is complete for an entry-copy.

supplier reference: The access point of the shadow supplier.

unit of replication: A specification of the information to be shadowed, including (optionally) subordinate knowledge information.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ACI	Access Control Information
DIB	Directory Information Base
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DSA	Directory System Agent
DSE	DSA Specific Entry
DUA	Directory User Agent
RDN	Relative Distinguished Name
SDSE	Shadowed DSA Specific Entry

5 Conventions

With minor exceptions this Directory Specification has been prepared according to the "Presentation of ITU-T | ISO/IEC common text" guidelines in the Guide for ITU-TS and ISO/IEC JTC 1 Cooperation, March 1993.

The term "Directory Specification" (as in "this Directory Specification") shall be taken to mean ITU-T Rec. X.525 | ISO/IEC 9594-9. The term "Directory Specifications" shall be taken to mean the X.500-Series Recommendations and all parts of ISO/IEC 9594.

This Directory Specification uses the term "1988 edition systems" to refer to systems conforming to the previous (1988) edition of the Directory Specifications, i.e. the 1988 edition of the series of CCITT X.500 Recommendations and the ISO/IEC 9594:1990 edition. Systems conforming to the current Directory Specifications are referred to as "1993 edition systems".

If the items in a list are numbered (as opposed to using "–" or letters), then the items shall be considered steps in a procedure.

This Directory Specification defines directory operations using the Remote Operation notation defined in ITU-T Rec. X.880 | ISO/IEC 9072-1.

6 Replication in the Directory

Replicated (copied) information can exist in the Directory. Shadowing is the mechanism for replication defined in this Directory Specification. Directory information can also be replicated by means outside this Directory Specification, such as caching. Any such alternative means of replication will need to ensure that exactly one instance of each replicated entry is identified as the master copy if the Directory and DSA Abstract Services are to be used.

Service controls provide the ability to control whether replicated information may be used in support of directory operations, regardless of the replication mechanism used to acquire the copy.

6.1 Caching

One method of replicating directory information is caching. Caching procedures are considered to be almost entirely governed by local policies, and therefore outside the scope of this Directory Specification.

6.2 Shadowing

Another method of replicating directory information is shadowing. An overview of the Directory information shadow service is found in clause 7. Before shadowing can occur, an agreement, covering the conditions under which shadowing may occur is required. Although such agreements may be established in a variety of ways, such as policy statements covering all DSAs within a given DMD, the shadowing is always between a pair of DSA. The technical parameters for the subsequent shadowing are specified as part of the resulting shadowing agreement. Components of the shadowing agreement are defined in clause 9.

Once the terms of the agreement have been established, the DSAs may initiate, modify and subsequently terminate the shadowing agreement. This may be done through a shadow operational binding as defined in clause 8.

This shadowing service for the Directory is based on the models established in ITU-T Rec. X.501 | ISO/IEC 9594-2, to satisfy the requirements outlined in ITU-T Rec. X.500 | ISO/IEC 9594-1. The protocol specification for shadowing and conformance requirements are provided in ITU-T Rec. X.519 | ISO/IEC 9594-5. In addition, this Directory Specification provides the definition of an operational binding for the purpose of initiating, modifying, and terminating shadowing agreements between DSAs. This operational binding type is defined using the tools specified in ITU-T Rec. X.501 | ISO/IEC 9594-2.

The directory information shadow service is defined in clause 10. The actual shadowing occurs through the set of operations defined in clause 11. These operations accommodate the transfer of Directory information and updates to the shadowed information.

The use of shadowed information by a DSA to satisfy a Directory request is described in ITU-T Rec. X.518 | ISO/IEC 9594-4.

6.3 Shadowing functional model

In the standardized form of Directory replication, termed *shadowing*, a DSA may assume the role of *shadow supplier*, the source of shadowed information, or *shadow consumer*, the recipient of shadowed information. The role played by a DSA when engaging in standardized replication activities (shadow supplier or shadow consumer) is always with respect to another DSA which plays the reciprocal role (shadow consumer or shadow supplier).

A given DSA may assume both roles, either

- with respect to different DSAs for the same or different units of replication; or
- with respect to a single DSA (which plays the reciprocal role) for different units of replication.

The Shadowing functional model addresses two approaches to shadowing Directory information:

- a *primary shadowing* policy requires that each shadow consumer receives its updates directly from the master DSA for the unit of replication;
- a *secondary shadowing* policy permits a shadow consumer to assume the shadow supplier role with respect to shadow consumers not having a shadowing agreement directly with the master DSA.

The characteristics of these two policies and their approach to addressing performance, availability, reliability and recovery are described below.

6.3.1 Primary shadowing

Figure 1 depicts primary shadowing. In this case the shadowing policy in effect has the following characteristics:

a) the master DSA is the only shadow supplier for a replicated area;

b) each shadow consumer has a direct shadowing agreement with the master DSA;

c) only read, compare, search, and list operations may be performed at a shadow consumer holding shadowed information. All modification operations are directed to the master DSA.

Because it allows for the placement of copies of often requested information, or knowledge of it, closer to the requester, this approach may be used to satisfy the performance requirement. Also, because this approach provides for the redundancy of individual entry or knowledge information, it is possible, in a primitive sense, to provide for availability, reliability, and recovery.

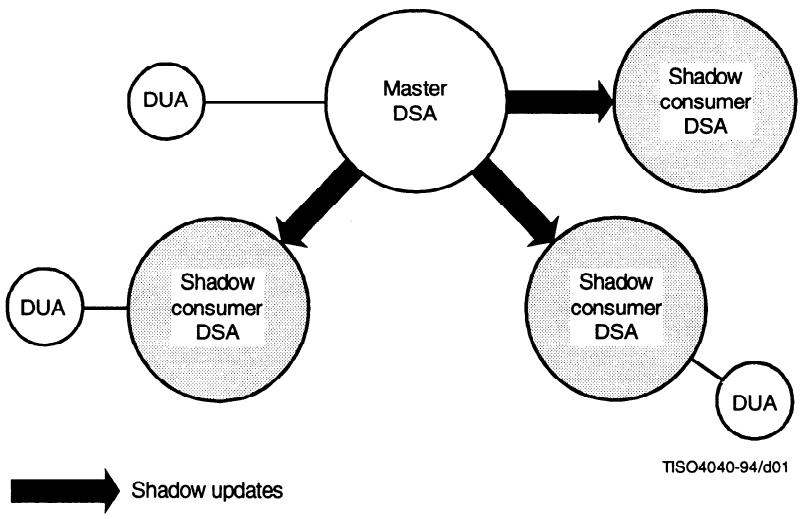

Figure 1 – Primary shadowing

6.3.2 Secondary shadowing

Figure 2 depicts secondary shadowing. In this case the shadowing policy in effect has the following characteristics:

a) The master DSA is not the only shadow supplier for a replicated area. Only some shadow consumers have a direct shadowing agreement with the master DSA as their shadow supplier.

b) Other shadow consumers may have a shadowing agreement with a shadow supplier that is not the master for the unit of replication. The shadowing agreements between the master DSA and its direct shadow consumers may, however, have an impact on secondary shadowing agreements.

c) Only read, compare, search, and list operations may be performed at a shadow consumer holding shadowed information. All modification operations are directed to the master DSA, either directly (if a secondary shadow consumer DSA has knowledge of the master DSA) or indirectly via the shadow supplier DSA(s).

Secondary shadowing is very similar to primary shadowing in the way that it provides for performance, availability, reliability and recovery. It differs in that it relieves the single master DSA of the burden of directly supplying all shadow consumers with the shadowed information. This is a desirable combination in environments where a large number of shadow consumers are holding the same shadowed information.

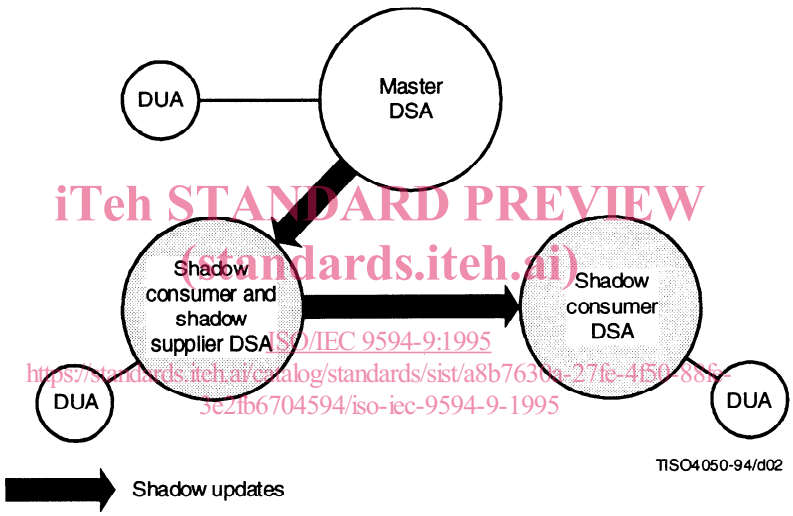

Figure 2 – Secondary shadowing

7 Shadowing in the Directory

The directory information shadow service defined here provides the Directory with a standardized mechanism to provide and support shadowed information. In outline, the shadow supplier maintains, for each shadowing agreement, information which is to be shadowed (the shadowed information). This information is replicated by protocol exchange between the shadow supplier and the shadow consumer. The information to be shadowed is all or a subset of the information held by the shadow supplier's DSA Information Tree. The shadow consumer's shadowed information becomes part of its DSA Information Tree.

To use the directory information shadow service, the Administrative Authorities of two DSAs must first reach an agreement on the terms under which shadowing will take place. This agreement, and the technical specification related to this agreement (the shadowing agreement), is discussed in 7.1. A description of the manner in which shadowed information is represented for the purposes of shadowing is provided in 7.2. The actual transfer of this shadowed information from the shadow supplier to the shadow consumer is accomplished by means of a set of shadow operations, which are introduced in 7.3.

The use of shadowed information to satisfy Directory requests is described in ITU-T Rec. X.518 | ISO/IEC 9594-4.

7.1 Shadowing agreement

Before shadowing can occur, an agreement for shadowing is established between the Administrative Authorities of the Directory Management Domains involved in the shadowing. This agreement for shadowing may be multilateral with respect to DSAs, in that it may cover all shadowing permitted among the set of DSAs concerned. The agreement may include any set of terms acceptable to the Administrative Authorities. For example, the agreement may specify policy information related to security, charging, or other special conditions.

A shadowing agreement is the specific agreement for a particular instance of shadowing between a pair of DSAs (the shadow consumer DSA and the shadow supplier DSA). This agreement may be explicit (e.g. contractual) or implicit (e.g. covered by the general terms of an agreement for shadowing as defined above). Each shadowing agreement has a unique identifier used in all protocol exchanges associated with the agreement. Other parameters of a shadowing agreement include a specification of the unit of replication, the update mode and possibly the access point of the master DSA for the shadowed information. Access control information is always included in shadowed information and therefore need not be explicitly specified.

Initially the representation of the shadowing agreement within a DSA (shadow supplier or shadow consumer) is created by an off-line administrative process. It represents essentially a template whose technical parameter values are subsequently validated during the initiating phase of the agreement and possibly modified during modification operations on the agreement. The method of storing this agreement is beyond the scope of this Directory Specification. Some technical aspects of the shadowing agreement may be exchanged via protocol and are discussed in detail in clause 9.

It must be noted that although the shadowing agreement will normally provide a true representation of the technical parameters related to the directory information shadow service, there may be exceptional cases in which policy overrides the technical specification resulting in a service inconsistency. For example, there may be certain attributes or attribute values that must be withheld for security reasons. It may be the case that security policy prevents disclosing the mere existence of these attributes, in which case it would be a violation to represent in the shadowing agreement the fact that they are being withheld. In this type of situation, the behavior of the shadow supplier DSA will be as if the technical specification were a true representation. Thus, users with access to the sensitive data will receive different views of the affected entries, depending on whether they access the master or a shadow consumer.

7.2 Shadowed information

Shadowed information is the logical set of information which is replicated by the shadow consumer. A replicated area is a subtree of the DIT defined for purposes of shadowing. The three components of shadowed information are:

a) *Prefix information:* Information relevant to entries within the replicated area which, with respect to the DSA information model, is positioned between the area prefix and the root DSE. This may contain administrative entry and subentry information.

b) *Area information:* Information about DSEs whose names fall within the replicated area.

c) *Subordinate information:* Information about knowledge references subordinate to the replicated area.

Figure 3 illustrates the derivation of shadowed information.

As illustrated at the left of Figure 3, the replicated area is always fully contained within a single naming context. The root of the subtree representing the replicated area is called the *Replication Base Entry*. Subordinate knowledge may also be replicated. This knowledge, the refined replicated area, and the area prefix constitute the unit of replication. This means that the specification of a unit of replication may extend beyond the naming context; however the replicated area itself is limited to the naming context. From this unit of replication specification, the shadow supplier can derive a representation of the shadowed information, which, as shown at the right of the figure, includes the prefix information, the area information (representing information held by DSEs in the replicated area), and (optionally) subordinate information. This shadowed information is subsequently conveyed by protocol to the shadow consumer which then integrates the information into its own DSA information tree. The shadowed information is built out of shadowed DSEs (SDSEs), which are discussed in 7.2.1. The establishment of shadowed information is discussed in 7.2.2.

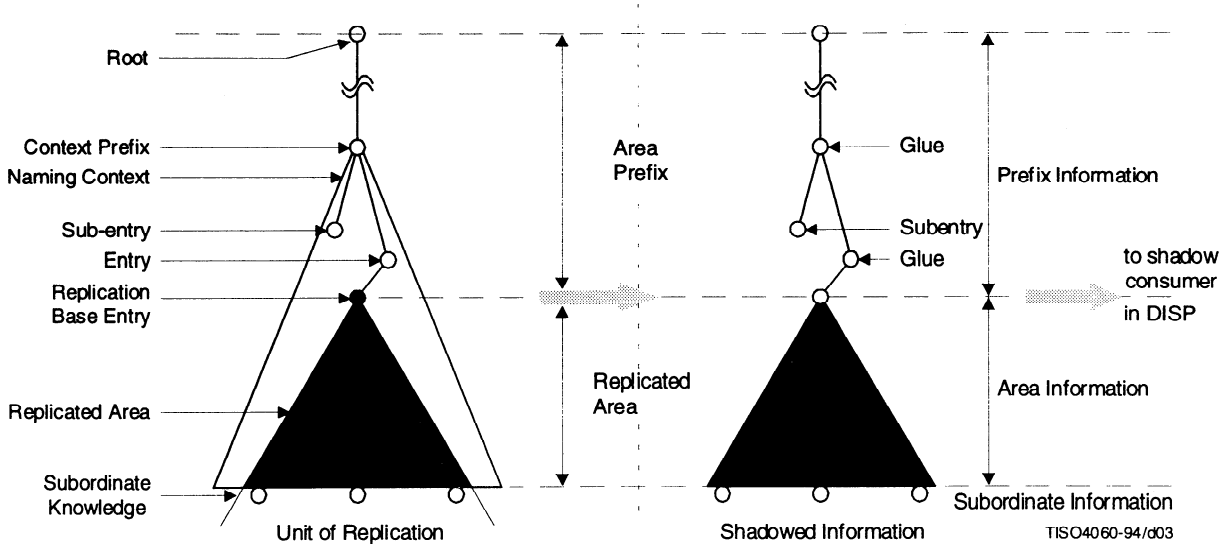

Figure 3 – Shadow supplier derivation of shadowed information

Figure 4 illustrates the derivation of shadowed information where extended knowledge is included.

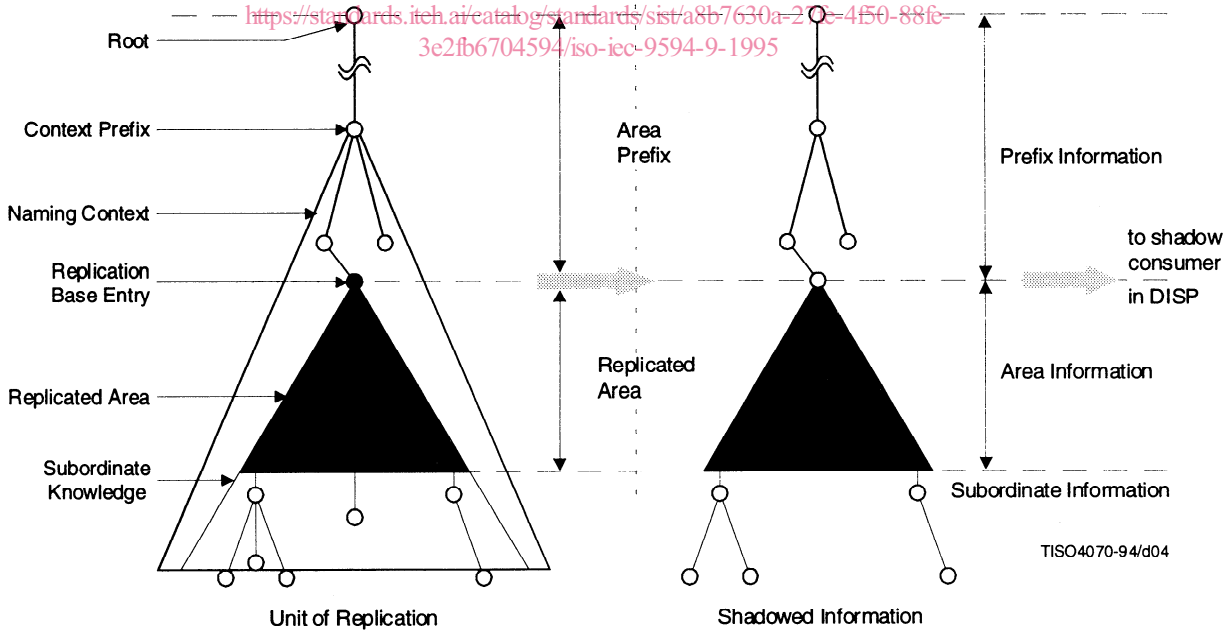

Figure 4 – Shadow supplier derivation of shadowed information with extended knowledge

7.2.1 SDSEs

Shadowed DSE (SDSE): That information being shadowed that is associated with a specific name. The SDSE represents the information shadowed from a DSE in the shadow supplier to a DSE in the shadow consumer, and is therefore not part of the DSA Information Model.

An SDSE is analogous to a DSE and consists of:

- SDSE type (always);
- user attributes (derived from entry information for DSEs corresponding to entries that are to be shadowed);
- operational attributes (present as required);
- subordinate-completeness flag (for area and subordinate information only);
- attribute-completeness flag (present for area information only).

7.2.1.1 SDSE type

DSE types are defined in ITU-T Rec. X.501 | ISO/IEC 9594-2. SDSE type, as specified in 11.3.1.1, is analogous to DSE type, but has fewer relevant options; **glue, cp, entry, alias, subr, nssr, admPoint, subEntry** and **sa**.

7.2.1.2 Subordinate-completeness flag

The subordinate-completeness flag is a boolean that is present for SDSEs within the area information and subordinate information. If the shadow supplier does not intend to provide information about subordinate completeness, the value **FALSE** is used for each SDSE. Otherwise the flag has the following semantics:

The flag is **TRUE** only if one of the following conditions is met for a particular SDSE:

a) it represents a leaf entry;

b) the replicated area contains SDSEs for each subordinate entry and each subordinate reference known to the master DSA, and if the SDSE represents an NSSR, this knowledge is represented in the SDSE.

The flag is **FALSE** if one of the following conditions is met for a particular SDSE:

a) the subordinates known to the master for that particular SDSE are not all present in the shadowed information;

b) in the case of a shadow supplier DSA performing secondary shadowing, if its shadow supplier had set the flag to **FALSE** or if its shadow supplier had set the flag to **TRUE** and the secondary shadow supplier chooses to set its to **FALSE**.

7.2.1.3 Attribute-completeness flag

The attribute completeness flag is a boolean and is **TRUE** if and only if all user attributes of the entry and all relevant collective attributes are present for the SDSE. It is only present for SDSEs containing entry information.

The attribute-completeness flag is not used with respect to Directory operational attributes; it is always assumed that they are not all present in the SDSE.

7.2.2 Establishment of shadowed information

The shadowed information represents three basic types of information: prefix information, area information, and subordinate information. Each of these is discussed in the following subclauses.

7.2.2.1 Prefix information

If the replicated area does not start immediately below the root of the DIT, the shadowed information will include SDSEs for each entry that is part of the area prefix of the replicated area (the path down from the root of the DIT to, but not including, the replication base entry, and any relevant subentries). SDSEs for prefix information are constructed as shown below.

a) If the DSE is an administrative point that has attributes pertaining to the replicated area, or that has one or more associated subentries whose subtree scope includes some or all of the replicated area, the SDSE is of type **admPoint**. If the DSE is also of type **cp**, the corresponding SDSE is of additional type **cp**. Any attributes that are relevant for the replicated area are included in the SDSE. The **administrativeRole** attribute shall be included in all administrative point SDSEs which are relevant to the shadowed information.