BS ISO/IEC 9594-9:2017

BSI Standards Publication

Information technology — Open Systems Interconnection — The Directory

Part 9: Replication

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9594-9:2017

National foreword

This British Standard is the UK implementation of ISO/IEC 9594-9:2017. It supersedes BS ISO/IEC 9594-9:2014, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/6, Data communications.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017
Published by BSI Standards Limited 2017

ISBN 978 0 580 96324 7

ICS 35.100.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2017.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9594-9:2017

INTERNATIONAL STANDARD

ISO/IEC 9594-9

Seventh edition
2017-05

Information technology — Open Systems Interconnection — The Directory —

Part 9: Replication

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire —

Partie 9: Duplication

Reference number
ISO/IEC 9594-9:2017(E)

Documents
Document Sharing Hub
© ISO/IEC 2017

Full document details: BS ISO/IEC 9594-9:2017

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9594-9:2017

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This seventh edition cancels and replaces the sixth edition (ISO/IEC 9594-9:2014), which has been technically revised.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T X.525 (10/2016).

A list of all parts in the ISO/IEC 9594 series, published under the general title *Information technology — Open Systems Interconnection — The Directory*, can be found on the ISO website.

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9594-9:2017

CONTENTS

Page

1 Scope 1

2 Normative references 1
2.1 Identical Recommendations | International Standards 1

3 Definitions 1
3.1 Basic Directory definitions 1
3.2 Directory model definitions 2
3.3 Abstract service definitions 2
3.4 Distributed operation definitions 2
3.5 Protocol definitions 2
3.6 Replication definitions 2

4 Abbreviations 3

5 Conventions 3

6 Replication in the Directory 4
6.1 Caching 4
6.2 Shadowing 4
6.3 Shadowing functional model 5

7 Shadowing in the Directory 6
7.1 Shadowing agreement 6
7.2 Shadowed information 7
7.3 Shadow operations 10
7.4 DSA Shadow Bind and DSA Shadow Unbind operation 11

8 Shadow operational binding 11
8.1 Shadow operational binding type characteristics 11
8.2 DSA procedures for operational binding management 12
8.3 Operational binding 13

9 Shadowing agreement 14
9.1 Shadowing agreement specification 14
9.2 Unit of replication 15
9.3 Update mode 20

10 Directory information shadow service 21
10.1 Shadow supplier initiated service 21
10.2 Shadow consumer initiated service 22

11 Shadow operations 22
11.1 Coordinate Shadow Update operation 22
11.2 Request Shadow Update operation 24
11.3 Update Shadow operation 26

12 Shadow error 29
12.1 Shadow error problems 30
12.2 Last update 30
12.3 Update window 30
12.4 Common results 30

Annex A – Directory shadow abstract service in ASN.1 31

Annex B – Amendments and corrigenda 37

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9594-9:2017

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 that 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 Directory system agents (DSAs) to improve the level of service to Directory users.

This Recommendation | International Standard provides the foundation frameworks upon which industry profiles can be defined by other standards groups and industry forums. Many of the features defined as optional in these frameworks may be mandated for use in certain environments through profiles. This eighth edition technically revises and enhances the seventh edition of this Recommendation | International Standard.

This eighth edition specifies versions 1 and 2 of the Directory protocols.

The first and second editions specified only version 1. Most of the services and protocols specified in this edition are designed to function under version 1. However, some enhanced services and protocols, e.g., signed errors, will not function unless all Directory entities involved in the operation have negotiated version 2. Whichever version has been negotiated, differences between the services and between the protocols defined in the eight editions, except for those specifically assigned to version 2, are accommodated using the rules of extensibility defined in Rec. ITU-T X.519 | ISO/IEC 9594-5.

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

Annex B, which is not an integral part of this Recommendation | International Standard, lists the amendments and defect reports that have been incorporated to form this edition of this Recommendation | International Standard.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 9594-9:2017

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection – The Directory: Replication

1 Scope

This Recommendation | International Standard specifies a shadow service which Directory system agents (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. 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 edition 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

– Recommendation ITU-T X.500 (2016) | ISO/IEC 9594-1:2017, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.*

– Recommendation ITU-T X.501 (2016) | ISO/IEC 9594-2:2017, *Information technology – Open Systems Interconnection – The Directory: Models.*

– Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

– Recommendation ITU-T X.511 (2016) | ISO/IEC 9594-3:2017, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition.*

– Recommendation ITU-T X.518 (2016) | ISO/IEC 9594-4:2017, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation.*

– Recommendation ITU-T X.519 (2016) | ISO/IEC 9594-5:2017, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications.*

– Recommendation ITU-T X.520 (2016) | ISO/IEC 9594-6:2017, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types.*

– Recommendation ITU-T X.521 (2016) | ISO/IEC 9594-7:2017, *Information technology – Open Systems Interconnection – The Directory: Selected object classes.*

– Recommendation ITU-T X.680 (2015) | ISO/IEC 8824-1:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

3 Definitions

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

3.1 Basic Directory definitions

The following term is defined in Rec. ITU-T X.500 | ISO/IEC 9594-1:

– *(the) Directory*.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017

3.2 Directory model definitions

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

a) distinguished name;

b) Directory information tree (DIT);

c) DSA-specific entry (DSE);

d) DSA information model;

e) DSA information tree;

f) Directory system agent (DSA).

3.3 Abstract service definitions

The following term is defined in Rec. ITU-T X.511 | ISO/IEC 9594-3:

a) request;

b) requestor.

3.4 Distributed operation definitions

The following terms are defined in Rec. ITU-T 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.

3.5 Protocol definitions

The following term is defined in Rec. ITU-T X.519 | ISO/IEC 9594-5:

a) application-association.

3.6 Replication definitions

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

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

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

3.6.3 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.

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

3.6.5 consumer reference: The access point of the shadow consumer.

3.6.6 entry-copy: Shadowed information from an entry.

3.6.7 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.

3.6.8 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).

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

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

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017

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

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

3.6.14 shadow consumer: A DSA that receives shadowed information.

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

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

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

3.6.18 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.

3.6.19 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.

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

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

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

3.6.23 supplier reference: The access point of the shadow supplier.

3.6.24 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
DMD	Directory Management Domain
DSA	Directory System Agent
DSE	DSA-Specific Entry
DUA	Directory User Agent
LDAP	Lightweight Directory Access Protocol
RDN	Relative Distinguished Name
SDSE	Shadowed DSA-Specific Entry
TCP/IP	Transmission Control Protocol/Internet Protocol

5 Conventions

The term "Directory Specification" (as in "this Directory Specification") shall be taken to mean Rec. ITU-T 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 first edition systems to refer to systems conforming to the first edition of the Directory Specifications, i.e., the 1988 edition of the CCITT X.500-series Recommendations and the ISO/IEC 9594:1990 edition.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017

This Directory Specification uses the term second edition systems to refer to systems conforming to the second edition of the Directory Specifications, i.e., the 1993 edition of the ITU-T X.500-series Recommendations and the ISO/IEC 9594:1995 edition.

This Directory Specification uses the term third edition systems to refer to systems conforming to the third edition of the Directory Specifications, i.e., the 1997 edition of the ITU-T X.500-series Recommendations and the ISO/IEC 9594:1998 edition.

This Directory Specification uses the term fourth edition systems to refer to systems conforming to the fourth edition of the Directory Specifications, i.e., the 2001 editions of Recs ITU-T X.500, ITU-T X.501, ITU-T X.511, ITU-T X.518, ITU-T X.519, ITU-T X.520, ITU-T X.521, ITU-T X.525, and ITU-T X.530, the 2000 edition of ITU-T X.509, and parts 1-10 of the ISO/IEC 9594:2001 edition.

This Directory Specification uses the term fifth edition systems to refer to systems conforming to the fifth edition of the Directory Specifications, i.e., the 2005 edition of the ITU-T X.500-series Recommendations and the ISO/IEC 9594:2005 edition.

This Directory Specification uses the term sixth edition systems to refer to systems conforming to the sixth edition of the Directory Specifications, i.e., the 2008 edition of the ITU-T X.500-series Recommendations and the ISO/IEC 9594:2008 edition.

This Directory Specification uses the term seventh edition systems to refer to systems conforming to the seventh edition of the Directory Specifications, i.e., the 2012 edition of the ITU-T X.500-series Recommendations and the ISO/IEC 9594:2014 edition.

This Directory Specification uses the term eighth edition systems to refer to systems conforming to the eighth edition of the Directory Specifications, i.e., the 2016 edition of the ITU-T X.500-series Recommendations and the ISO/IEC 9594:2017 edition.

This Directory Specification presents ASN.1 notation in the bold Courier New typeface. When ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in the bold Courier New typeface. The names of procedures, typically referenced when specifying the semantics of processing, are differentiated from normal text by displaying them in bold Times New Roman. Access control permissions are presented in italicized Times New Roman.

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

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. DISP is protected by the underlying protocol as defined in Rec. ITU-T X.519 | ISO/IEC 9594-5.

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 Directory management domain (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.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017

This shadowing service for the Directory is based on the models established in Rec. ITU-T X.501 | ISO/IEC 9594-2, to satisfy the requirements outlined in Rec. ITU-T X.500 | ISO/IEC 9594-1. The protocol specification for shadowing and conformance requirements are provided in Rec. ITU-T 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 Rec. ITU-T 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 Rec. ITU-T 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 requestor, 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.

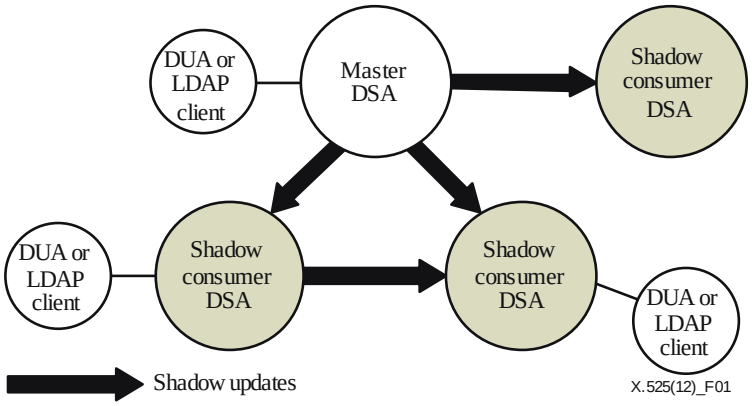

Figure 1 – Primary shadowing

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017

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.

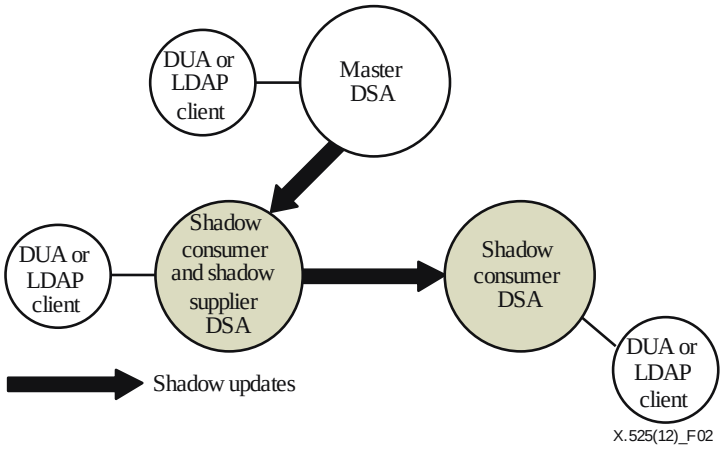

Figure 2 – Secondary shadowing

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 Rec. ITU-T 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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017

(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.

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 are 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 behaviour 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 DSA-specific entry (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.

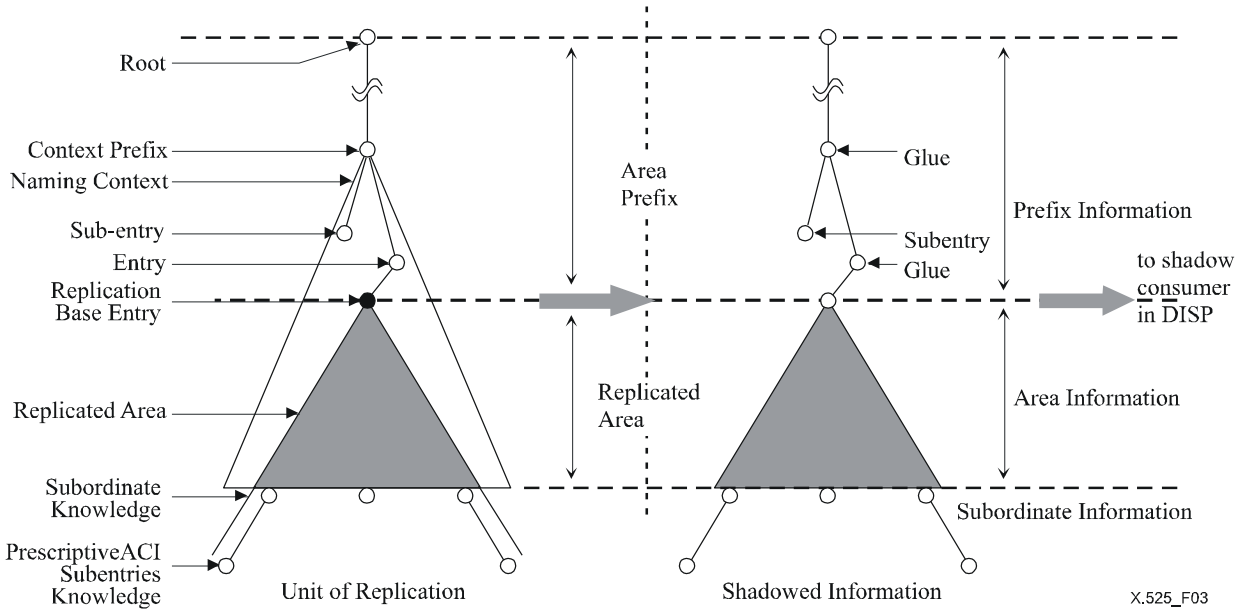

Figure 3 – Shadow supplier derivation of shadowed information

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. Implicit in the subordinate knowledge is the access control information which governs access to the relative distinguished name (RDN) of the subordinate knowledge. When the subordinate entry is an administrative point in another DSA, then part of this access control information may be held in **`prescriptiveACI`** in subentries beneath the subordinate knowledge. This knowledge, the refined replicated area, and the area prefix constitute the unit of replication.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 9594-9:2017