INTERNATIONAL STANDARD

ISO/IEC 9594-5

Sixth edition
2008-12-15

Information technology — Open Systems Interconnection — The Directory: Protocol specifications

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Spécifications du protocole

Reference number
ISO/IEC 9594-5:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published by ISO in 2009

Published in Switzerland

CONTENTS

Page

Foreword v
Introduction vi
1 Scope 1
2 References 1
2.1 Normative references 1
2.2 Non-normative references 2
3 Definitions 2
3.1 Basic Directory definitions 3
3.2 Distributed Operation Definitions 3
3.3 Protocol specification definitions 3
4 Abbreviations 4
5 Conventions 4
6 Common protocol specification 5
6.1 Directory associations and operations 5
6.2 Specification for Directory operations 5
6.3 Directory protocol overview 7
6.4 Operation codes 8
6.5 Error codes 8
6.6 Abstract syntaxes 9
7 Directory protocols using the OSI stack 9
7.1 OSI-PDUs 9
7.2 Directory PDU structure 9
7.3 Session PDUs 10
7.4 OSI addressing 10
7.5 Procedure and sequencing 10
7.6 Directory PDU specifications 11
8 Directory protocol mapping onto OSI services 24
8.1 Abstract syntaxes and transfer syntaxes 24
8.2 Application-contexts 25
8.3 Session Layer specification 26
8.4 Use of transport service 32
8.5 OSI Transport Layer on top of TCP 33
9 IDM protocol 47
9.1 IDM-PDUs 47
9.2 Sequencing requirements 49
9.3 Protocols 49
9.4 Reject reasons 50
9.5 Abort reasons 50
9.6 Mapping onto TCP/IP 51
9.7 Addressing 51
9.8 Use of TLS 51
10 Directory protocol mapping onto the IDM protocol 52
10.1 DAP-IP protocol 52
10.2 DSP-IP protocol 52
10.3 DISP-IP protocol 52
10.4 DOP-IP protocol 53

Page

11 Protocol stack coexistence 53
11.1 Coexistence between OSI and IDM stacks 53
11.2 Coexistence in the presence of LDAP 53
11.3 Defining network addresses for Internet Protocol, Version 4 support 53
11.4 Definition of NSAP like address for long addressing information 54

12 Versions and the rules for extensibility 55
12.1 DUA to DSA 55
12.2 DSA to DSA 56
12.3 Rules of extensibility for NSAP addresses 57
12.4 Rules of extensibility for object classes 57
12.5 Rules of extensibility for user attribute types 57

13 Conformance 57
13.1 Conformance by DUAs 57
13.2 Conformance by DSAs 58
13.3 Conformance by a shadow supplier 62
13.4 Conformance by a shadow consumer 62

Annex A – Common protocol specifications in ASN.1 64

Annex B – OSI Protocol in ASN.1 66

Annex C – Directory OSI Protocols in ASN.1 72

Annex D – IDM Protocol in ASN.1 75

Annex E – Directory IDM Protocols in ASN.1 78

Annex F – Directory operational binding types 80

Annex G – Amendments and corrigenda 81

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

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.

ISO/IEC 9594-5:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems,* in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.519 (11/2008).

This sixth edition cancels and replaces the fifth edition (ISO/IEC 9594-5:2005), which has been technically revised.

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: Public-key and attribute certificate frameworks*

— *Part 9: Replication*

— *Part 10: Use of systems management for administration of the Directory*

Introduction

This Recommendation | International Standard, together with the 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 specifies the application service elements and application contexts for two protocols – the Directory Access Protocol (DAP) and the Directory System Protocol (DSP). The DAP provides for access to the Directory to retrieve or modify Directory information. The DSP provides for the chaining of requests to retrieve or modify Directory information to other parts of the distributed Directory System where the information may be held.

In addition, this Recommendation | International Standard specifies the application service elements and application contexts for the Directory Information Shadowing Protocol (DISP) and the Directory Operational Binding Management Protocol (DOP). The DISP provides for the shadowing of information held in one DSA to another DSA. The DOP provides for the establishment, modification and termination of bindings between pairs of DSAs for the administration of relationships between the DSAs (such as for shadowing or hierarchical relationships).

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 sixth edition technically revises and enhances, but does not replace, the fifth edition of this Recommendation | International Standard. Implementations may still claim conformance to the fifth edition. However, at some point, the fifth edition will not be supported (i.e., reported defects will no longer be resolved). It is recommended that implementations conform to this sixth edition as soon as possible.

This sixth 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 six editions, except for those specifically assigned to version 2, are accommodated using the rules of extensibility defined in this edition of ITU-T Rec. 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 common specifications for the Directory protocols.

Annex B, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for the OSI protocol specification.

Annex C, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for the Directory OSI protocols.

Annex D, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for the IDM protocol specification.

Annex E, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for the Directory IDM protocols.

Annex F, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module which contains all the ASN.1 object identifiers assigned to identify operational binding types in this series of Recommendations | International Standards.

Annex G, 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.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection – The Directory: Protocol specifications

1 Scope

This Recommendation | International Standard specifies the Directory Access Protocol, the Directory System Protocol, the Directory Information Shadowing Protocol, and the Directory Operational Binding Management Protocol fulfilling the abstract services specified in ITU-T Rec. X.511 | ISO/IEC 9594-3, ITU-T Rec. X.518 | ISO/IEC 9594-4, ITU-T Rec. X.525 | ISO/IEC 9594-9, and ITU-T Rec. X.501 | ISO/IEC 9594-2.

2 References

2.1 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.

2.1.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model.*
- ITU-T Recommendation X.213 (2001) | ISO/IEC 8348:2002, *Information technology – Open Systems Interconnection – Network service definition.*
- ITU-T Recommendation X.214 (1995) | ISO/IEC 8072:1996, *Information technology – Open Systems Interconnection – Transport service definition.*
- ITU-T Recommendation X.500 (2008) | ISO/IEC 9594-1:2008, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.*
- ITU-T Recommendation X.501 (2008) | ISO/IEC 9594-2:2008, *Information technology – Open Systems Interconnection – The Directory: Models.*
- ITU-T Recommendation X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*
- ITU-T Recommendation X.511 (2008) | ISO/IEC 9594-3:2008, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition.*
- ITU-T Recommendation X.518 (2008) | ISO/IEC 9594-4:2008, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation.*
- ITU-T Recommendation X.520 (2008) | ISO/IEC 9594-6:2008, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types.*
- ITU-T Recommendation X.521 (2008) | ISO/IEC 9594-7:2008, *Information technology – Open Systems Interconnection – The Directory: Selected object classes.*
- ITU-T Recommendation X.525 (2008) | ISO/IEC 9594-9:2008, *Information technology – Open Systems Interconnection – The Directory: Replication.*
- ITU-T Recommendation X.530 (2008) | ISO/IEC 9594-10:2008, *Information technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory.*

- ITU-T Recommendation X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*
- ITU-T Recommendation X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*
- ITU-T Recommendation X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- ITU-T Recommendation X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*
- ITU-T Recommendation X.690 (2008) | ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

2.1.2 ISO/IEC Standards

- ISO/IEC 10646:2003, *Information technology – Universal Multiple-Octet Coded Character Set (UCS).*

2.1.3 Other references

- ITU-T Recommendation E.164 (2005), *The international public telecommunication numbering plan.*
- ITU-T Recommendation X.121 (2000), *International numbering plan for public data networks.*
- IETF RFC 2025 (1996), *The Simple Public-Key GSS-API Mechanism (SPKM).*
- IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program – Protocol Specification.*
- IETF RFC 1738 (1994), *Uniform Resource Locators (URL).*
- IETF RFC 2246 (1999), *The TLS Protocol Version 1.0.*
- IETF RFC 4511 (2006), *Lightweight Directory Access Protocol (LDAP): The Protocol.*
- IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions.*
- IETF RFC 3986 (2005), *Uniform Resource Identifier (URI): Generic Syntax.*

2.2 Non-normative references

- ITU-T Recommendation X.217 (1995) | ISO/IEC 8649:1996, *Information technology – Open Systems Interconnection – Service definition for the Association Control Service Element.*
- ITU-T Recommendation X.224 (1995) | ISO/IEC 8073:1997, *Information technology – Open Systems Interconnection – Protocol for providing the connection-mode transport service.*
- ITU-T Recommendation X.225 (1995) | ISO/IEC 8327-1:1996, *Information technology – Open Systems Interconnection – Connection-oriented Session protocol: Protocol specification.*
- ITU-T Recommendation X.226 (1994) | ISO/IEC 8823-1:1994, *Information technology – Open Systems Interconnection – Connection-oriented Presentation protocol: Protocol specification.*
- ITU-T Recommendation X.227 (1995) | ISO/IEC 8650-1:1996, *Information technology – Open Systems Interconnection – Connection-oriented protocol for the Association Control Service Element: Protocol specification.*
- ITU-T Recommendation X.881 (1994) | ISO/IEC 13712-2:1995, *Information technology – Remote Operations: OSI realizations – Remote Operations Service Element (ROSE) service definition.*
- IETF RFC 1006 (1987), *ISO Transport Service on top of the TCP Version: 3.*
- IETF RFC 1277 (1991), *Encoding Network Addresses to Support Operation over Non-OSI Lower Layers.*
- IETF RFC 2126 (1997), *ISO Transport Service on top of TCP (ITOT).*

3 Definitions

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

3.1 Basic Directory definitions

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

a) *the Directory*;

b) *(Directory) user*;

c) *Directory System Agent (DSA)*;

d) *Directory User Agent (DUA)*.

3.2 Distributed Operation Definitions

The following terms are defined in ITU-T Rec. X.518 | ISO/IEC 9594-4:

a) *chaining*;

b) *referral*.

3.3 Protocol specification definitions

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

NOTE – The terms defined in this subclause are generalized definitions to cover both the OSI and the TCP/IP case, except exceptions as indicated.

3.3.1 abstract syntax: The specification of a data types and/or data values by using notation rules which are independent of the encoding technique used to represent them.

3.3.2 application-association: A cooperative relationship between two application-entities established by the Bind operation.

3.3.3 application-context: (OSI only definition) A set of rules shared in common by two application-entities in order to support an application-association.

3.3.4 application-context-name: An ASN.1 object identifier that identifies (names) an application-context.

3.3.5 Application Layer: The top layer of the OSI seven layer model representing the semantics of the communication.

3.3.6 application-entity: A representation of the external behaviour of an application process in the form of its communication capabilities.

3.3.7 application-entity title: The Directory distinguished name of an application-entity, and in particular, an application-entity representing a Directory application process.

3.3.8 application process: A process within a system which performs information processing for a particular purpose, in particular processing Directory operations.

3.3.9 Bind operation: An operation type used for establishing an application-association.

3.3.10 Directory operation: An operation type for exchange of Directory information.

3.3.11 directory protocol-data-unit: A unit of data for a Directory protocol consisting of control information and in the general case also application data as specified by Directory operations.

NOTE 1 – A Directory PDU in the OSI environment includes all the protocol elements of the OSI Presentation Layer and if relevant, protocol elements of ACSE in addition to the Directory-specific protocol elements.

NOTE 2 – The term "application-protocol-data-unit (APDU)" is a unit of data defined by an OSI application protocol. This term is not used for edition 5 and subsequent editions of these Directory Specifications. However, the abbreviation may appear in certain ASN.1 elements.

3.3.12 initiator: The application process that initiates an application-association by issuing a Bind request.

3.3.13 local matter: A decision made by a system concerning its behaviour that is not subject to the requirements of these Directory Specifications.

3.3.14 operation: An exchange between two application processes to perform a particular task. It consists of a request from one application-process to the other one and the return of zero or more responses (result and/or errors). An operation implies a certain process to be performed by the application process receiving the request.

3.3.15 protocol-data-unit: Comprised of the presentation protocol elements or the ACSE protocol elements of a Directory protocol-data-unit.

3.3.16 **Presentation Layer**: The sixth layer of the OSI Reference Model.

3.3.17 **protocol error**: An unrecognized or unexpected protocol-data-unit or a protocol-data-unit with an unexpected or invalid parameter is received.

3.3.18 **responder**: The application-process that receives a Bind request and either accepts or refuses the application-association.

NOTE – Initiator and responder are defined with respect to a single transport-connection. The initiator is also the application process that initiated the transport-connection (see 8.4). A DSA can be both an initiator and responder simultaneously.

3.3.19 **session layer**: The fifth layer of the OSI Reference Model.

3.3.20 **session-protocol-data-unit**: (OSI only definition) A unit of data at the OSI Session Layer consisting of control information and in the general case also carries a Directory protocol-data-unit.

4 Abbreviations

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

AC	Application Context
ACSE	Association Control Service Element
AE	application-entity
AFI	Authority and Format Identifier
APDU	application-protocol-data-unit
DAP	Directory Access Protocol
DISP	Directory Information Shadowing Protocol
DOP	Directory Operational Binding Management Protocol
DSA	Directory System Agent
DSP	Directory System Protocol
DSP	Domain Specific Part
DUA	Directory User Agent
IDI	Initial Domain Identifier
IDM	Internet Directly Mapped
IPv4	Internet Protocol, Version 4
IPv6	Internet Protocol, Version 6
ITOT	ISO Transport Service on top of TCP
LDAP	Lightweight Directory Access Protocol
NSAP	Network-Service-Access-Point
PDU	protocol-data-unit
PPDU	presentation-protocol-data-unit
SPDU	session-protocol-data-unit
TCP/IP	Transmission Control Protocol/Internet Protocol
TPDU	transport-protocol-data-unit
TPKT	Transport Packet
TSDU	transport-service-data-unit
URI	Uniform Resource Identifier

5 Conventions

The term "Directory Specification" (as in "this Directory Specification") shall be taken to mean ITU-T Rec. X.519 | ISO/IEC 9594-5. 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 series of CCITT X.500 Recommendations and the ISO/IEC 9594:1990 edition.

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 series of ITU-T X.500 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 series of ITU-T X.500 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 ITU-T Recs X.500, X.501, X.511, X.518, X.519, X.520, X.521, X.525, and X.530, the 2000 edition of ITU-T Rec. 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 series of ITU-T X.500 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 series of ITU-T X.500 Recommendations and the ISO/IEC 9594:2008 edition.

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

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 Common protocol specification

6.1 Directory associations and operations

The protocols for these Directory Specifications are described as a set of *operations*. An operation is defined in terms of a request sent from one system to another system expecting this other system to process the request, and if applicable, returns one or more replies constituting the result. An operation can either be a *Bind operation* or an operation invoked to access Directory information (a *Directory operation*).

If exception conditions are encountered, one or more errors may be returned instead of or in addition to possible results.

NOTE 1 – The currently defined operations will return either one or more results or a single error.

Directory protocols defined by these Directory Specifications may use an OSI protocol stack, a TCP/IP protocol stack or both. The specification provided by this clause is independent of the particular protocol stack. The OSI specific specification is given in clauses 7 and 8, while the TCP/IP specific specification is given in clauses 9 and 10.

A process within a system that processes Directory operations is called an *application process*. An *application-entity* is the reflection of the external behaviour of an application process.

Before Directory operations can be invoked between two Directory application processes, an *application-association* has to be established between the corresponding application-entities. An application-association is a cooperative relationship between two application-entities formed by exchange of control information within the request and result of a Bind operation and by the use of a common underlying service.

NOTE 2 – This is a modified definition of application-association as given by ITU-T Rec. X.217 | ISO/IEC 8649, and is intended to cover both the use of an underlying OSI protocol stack and an underlying TCP/IP stack.

An application-association is terminated using an unbind exchange. The unbinding of an application-association is not defined as an operation.

6.2 Specification for Directory operations

These Directory Specifications specify several operation types. An operation type is specified by the **OPERATION** ASN.1 information object class. Possible errors associated with an operation type are defined by the **ERRORS** ASN.1 information object class.

```
OPERATION  ::=  CLASS {
        &ArgumentType       OPTIONAL,
        &ResultType         OPTIONAL,
        &Errors             ERROR OPTIONAL,
        &operationCode      Code UNIQUE OPTIONAL }
WITH SYNTAX {
        [ARGUMENT &ArgumentType]
        [RESULT             &ResultType]
        [ERRORS             &Errors]
        [CODE               &operationCode] }

ERROR  ::=  CLASS {
        &ParameterType,
        &errorCode          Code UNIQUE OPTIONAL }
WITH SYNTAX {
        PARAMETER           &ParameterType
        [CODE               &errorCode] }

Code ::=  CHOICE  {
        local           INTEGER,
        global          OBJECT IDENTIFIER }
```

The **OPERATION** information object class is a convenient way to express the syntax of Directory requests, results and errors for a particular operation type.

This ASN.1 information object class has the following fields:

a) The **&ArgumentType** field specifies an open data type for the request part of an operation.

b) The **&ResultType** field specifies an open data type for one or more replies constituting the result of the request. If this field is absent, there is no result associated with the operation.

c) The **&Errors** field specifies one or more errors that can occur as the result of processing the request. If this field is absent, there is no error associated with the operation.

d) The **&operationCode** field specifies the type of Directory operation to be performed. This field is absent for the Bind operation. See 6.4 for currently defined operation codes.

Directory operations may in principle be performed in two different modes:

a) if a Directory operation shall be completed before a new Directory operation may be invoked, the mode of operation is *synchronous*; or

b) if several operations may be in progress at the same time, the mode of operation is *asynchronous*.

If all Directory operations defined for a particular type of application-association:

a) consist of both a request and one or more results and/or errors; and

b) only are allowed to be invoked by a designated system,

such operation may be executed in either synchronous or asynchronous mode. Otherwise, the mode of operation is always asynchronous.

The **OPERATION** information object class does not in itself imply any sequencing. A Directory request may have no result and/or error, or a request may have several results and/or errors. However, it does tie together a request with possible responses (results and errors) by carrying the same operation code and the same invoke id (see below). However, specification of a particular operation type may dictate sequencing restrictions.

An error is a report of the unsuccessful performance of an operation. An error is represented by the **ERROR** ASN.1 Information Object Class. The different fields are described below:

a) the **&ParameterType** field specifies the data type of the parameter of the error specifying the nature of the error; and

b) the **&errorCode** field specifies the code that identifies the error (see 6.5 for the defined error codes).

Although not reflected by the **OPERATION** or the **ERRORS** information object classes, each invocation of a Directory operation is assigned an **InvokeId**, which is carried in the protocol. This makes it possible to indicate to what Directory operation a particular request, result or error belongs. The definition of the **InvokeId** is as follows:

```
InvokeId  ::=  CHOICE {
        present         INTEGER,
        absent          NULL }
```

If an operation type does not specify an **&operationCode**, operations of this type cannot have **InvokeId** assigned.

6.3 Directory protocol overview

6.3.1 Use of underlying services

When two application processes from different open systems interact, the application-association is realized as an Application Layer protocol using either an OSI or a TCP/IP underlying service.

Details on the use of the OSI service are given in clause 8, while the details on the use of the TCP/IP service are given in clause 10.

The OSI Transport Layer may either be supported using the service as defined in ITU-T Rec. X.214 | ISO/IEC 8072 or by using the specification in 8.5. In this latter case, the OSI upper layer protocols stack are placed on the top of a TCP/IP protocol stack.

6.3.2 The Directory Access Protocol (DAP)

Before a DUA and a DSA from different open systems can interact, a Bind operation has to be invoked between them to establish an application-association supporting a Directory protocol called the Directory Access Protocol (DAP).

The Bind operation (**directoryBind**) for establishing a DAP application-association is defined in clause 8 of ITU-T Rec. X.511 | ISO/IEC 9594-3.

This edition and all previous editions of the Directory Specifications only allow a DUA to invoke a Bind operation and to initiate subsequent Directory operations. If the OSI underlying stack is used, Directory operations may be invoked either in synchronous mode or in asynchronous mode. If the TCP/IP underlying stack is used, Directory operations are always invoked in asynchronous mode.

All Directory operations require either a single reply or a single error to be returned.

6.3.3 The Directory System Protocol (DSP)

Before a pair of DSAs from different open systems can interact, a Bind operation has to be invoked between them to establish an application-association supporting a Directory protocol called the Directory System Protocol (DSP).

The Bind operation (**dSABind**) for establishing a DSP application association is defined in clause 11 of ITU-T Rec. X.518 | ISO/IEC 9594-4.

Either DSA may invoke a Bind operation. Both the initiating and responding DSA may invoke subsequent Directory operations. Directory operations are always invoked in asynchronous mode on the DSP.

All Directory operations require either a single reply or a single error to be returned.

6.3.4 The Directory Information Shadowing Protocol (DISP)

Before a pair of DSAs from different open systems can interact for the purpose of exchanging shadowing information, a Bind operation has to be invoked between them to establish an application-association supporting a Directory protocol called the Directory Information Shadowing Protocol (DISP).

The Bind operation (**dSAShadowBind**) for establishing a DISP application-association is defined in clause 7.4.1 of ITU-T Rec. X.525 | ISO/IEC 9594-9.

If the OSI underlying stack is used, the mode of operation is synchronous or asynchronous depending on the application-context selected for the Bind operation. If the TCP/IP underlying stack is used, Directory operations are always invoked in asynchronous mode.

All Directory operations require either a single reply or a single error to be returned.

6.3.5 The Directory Operational Binding Management Protocol (DOP)

Before a pair of DSAs from different open systems can interact for the purpose of maintaining operational bindings, a Bind operation has to be invoked to establish an application-association supporting a Directory protocol called the Directory Operational Binding Management Protocol (DOP).

The DSA that may assume the role of initiator of the Bind operation depends on the DSA roles assigned for the operational binding(s) to be managed using the Directory operations on the application-association. Only the initiator may invoke Directory operations. More than one operational binding type may only be managed within this application-association if the DSA roles for the distinct types are compatible (e.g., a DSA assumes Role A for each binding type).

All Directory operations require either a single reply or a single error to be returned.

6.4 Operation codes

6.4.1 Operation codes for DAP and DSP

The following operation codes are used in the DAP and the DSP:

id-opcode-read **Code ::= local : 1**
id-opcode-compare **Code ::= local : 2**
id-opcode-abandon **Code ::= local : 3**
id-opcode-list **Code ::= local : 4**
id-opcode-search **Code ::= local : 5**
id-opcode-addEntry **Code ::= local : 6**
id-opcode-removeEntry **Code ::= local : 7**
id-opcode-modifyEntry **Code ::= local : 8**
id-opcode-modifyDN **Code ::= local : 9**

The use of these operation codes is specified in ITU-T Rec. X.511 | ISO/IEC 9594-3.

6.4.2 Operation codes for DISP

The following operation codes are used in the DISP.

id-opcode-requestShadowUpdate **Code ::= local : 1**
id-opcode-updateShadow **Code ::= local : 2**
id-opcode-coordinateShadowUpdate **Code ::= local : 3**

The use of these operation codes is specified in ITU-T Rec. X.525 | ISO/IEC 9594-9.

6.4.3 Operation codes for DOP

The following operation codes are used in the DOP.

id-op-establishOperationalBinding **Code ::= local : 100**
id-op-modifyOperationalBinding **Code ::= local : 102**
id-op-terminateOperationalBinding **Code ::= local : 101**

The use of these operation codes is specified in ITU-T Rec. X.501 | ISO/IEC 9594-2.

6.5 Error codes

6.5.1 Error codes for DAP and DSP

The following error codes are used in the DAP and the DSP. The code **id-errcode-referral** is only used in the DAP. The code **id-opcode-dsaReferral** is only used in the DSP:

id-errcode-attributeError **Code ::= local : 1**
id-errcode-nameError **Code ::= local : 2**
id-errcode-serviceError **Code ::= local : 3**
id-errcode-referral **Code ::= local : 4**
id-errcode-abandoned **Code ::= local : 5**
id-errcode-securityError **Code ::= local : 6**
id-errcode-abandonFailed **Code ::= local : 7**
id-errcode-updateError **Code ::= local : 8**
id-errcode-dsaReferral **Code ::= local : 9**

6.5.2 Error codes for DISP

The following error code is used in the DISP:

id-errcode-shadowError **Code ::= local : 1**

6.5.3 Error codes for DOP

The following error code is used in the DOP:

id-err-operationalBindingError **Code ::= local : 100**

6.6 Abstract syntaxes

A protocol specification includes a specification of the data types that may be transferred as part of the protocol exchanges. The data types are defined using an abstract notation like the ASN.1 notation and constitute the abstract syntax for the protocol. The abstract syntaxes are quite similar for OSI communication and for TCP/IP communication, although there are differences. Four abstract syntaxes are defined for each of these types of communication corresponding to the four different Directory protocols. Only for the OSI communication are the abstract syntaxes assigned object identifiers. When establishing an OSI application-association the relevant object identifier for the abstract syntax is signalled in the Bind (see 7.6.1).

7 Directory protocols using the OSI stack

This clause defines the Directory protocols and their mapping onto the OSI Session Protocol. It incorporates the relevant elements of the OSI Presentation Protocol as defined by ITU-T Rec. X.226 | ISO/IEC 8823-1 and the Association Control Service Element (ACSE) as defined by ITU-T Rec. X.227 | ISO/IEC 8650-1.

The relevant part of the OSI session protocol is defined in 8.3.

7.1 OSI-PDUs

The messages of the OSI based protocols are conveyed over an OSI application-association as Directory protocol-data-units represented by the **OSI-PDU** data type as follows:

```
OSI-PDU {APPLICATION-CONTEXT:protocol}::= TYPE-IDENTIFIER.&Type (
        OsiBind { {protocol} } |
        OsiBindResult { {protocol} } |
        OsiBindError { {protocol} } |
        OsiOperation { {protocol.&Operations} } |
        PresentationAbort )
```


7.2 Directory PDU structure

A Directory PDU in the OSI environment consists of protocol elements from the OSI Presentation Layer as defined by ITU-T Rec. X.226 | ISO/IEC 8823-1, of ACSE protocol elements as defined by ITU-T Rec. X.227 | ISO/IEC 8650-1, if relevant, and Directory specific protocol elements for the protocol in question.

The **OsiBind**, the **OsiBindResult** and the **OsiBindError** have presentation protocol elements and ACSE protocol elements in addition to the Directory specific protocol elements, while the **OsiOperation** only has presentation protocol elements in addition to the Directory specific protocol elements. The **PresentationAbort** has only presentation protocol elements.

The Presentation Layer protocol elements included within a specific Directory PDU comprise a PPDU.

NOTE 1 – The term PPDU (presentation-protocol-data-unit) is introduced here, as it is referenced when discussing presentation protocol errors and by the **Abort-reason** data type. The term is otherwise not relevant for these Directory Specifications.

The ACSE protocol elements included within a specific Directory PDU comprise an ACSE PDU.

NOTE 2 – ITU-T Rec. X.227 | ISO/IEC 8650-1 uses the term APDU (application-protocol-data-unit) for an ACSE PDU. As the Directory specific protocol elements of a specific Directory PDU in principle also comprise an APDU, the term ACSE PDU is used here to avoid confusion.

The following PPDUs are used by this Directory Specification:

a) CP PPDU, which is reflected by the **CP-type** data type defined by ITU-T Rec. X.226 | ISO/IEC 8823-1. It is a part of the **OsiBind** data type;

b) CPA PPDU, which is reflected by the **CPA-PPDU** data type defined by ITU-T Rec. X.226 | ISO/IEC 8823-1. It is a part of the **OsiBindResult** data type;

c) CPR PPDU, which is reflected by the **CPR-PPDU** data type defined by ITU-T Rec. X.226 | ISO/IEC 8823-1. It is part of the **OsiBindError** data type;

d) TD PPDU, which is reflected by the **User-data** data type defined by ITU-T Rec. X.226 | ISO/IEC 8823-1. It is part of the **OsiOperation** data type;

e) ARU PPDU, which is reflected by the **ARU-PPDU** defined by ITU-T Rec. X.226 | ISO/IEC 8823-1. It is part of the **ARU-PPDU** data type as defined by this Directory specification; and

f) ARP PPDU, which is reflected by the **ARP-PPDU** defined by ITU-T Rec. X.226 | ISO/IEC 8823-1. It constitutes the **ARP-PPDU** data type as defined by this Directory specification.