TR 101 153-2 V1.1.1 (1998-01)

Technical Report

Users' views on addressing and directories; Part 2: Guidelines to the users designing a private directory system

European Telecommunications Standards Institute

Reference

DTR/USER-00002-2 (aoci0ics.PDF)

Keywords

Addressing, Directory

ETSI Secretariat

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

X.400

c= fr; a=atlas; p=etsi; s=secretariat

Internet

secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr).

Pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

This document was prepared jointly by OSITOP and ETSI and is a common property of these two associations.

Foreword

This ETSI Technical Report (TR) has been produced by ETSI User Group supported by OSITOP and EWOS/EG DIR.

The present document, Part 2 of a two-part Technical Report was prepared jointly by OSITOP and ETSI and is a common property of these two associations.

Introduction

The present document is the result of the work of a Topic Group (TG) supported by the User Group and OSITOP which in particular encouraged its members to take part in a survey among European companies to identify their needs related to the directory systems, regarding their content, their interworking and their management.

EWOS/EG DIR has also provided key contributions in several parts of this work.

Starting from the results of this work, the TG endeavoured to identify which solutions are able to fulfil the identified requirements.

The present document is Part 2 of a two-part document related to addressing and directory issues. While Part 1 contains requirements to the providers and standard makers, the purpose of Part 2 is to help users in designing properly a directory system and in asking themselves the right questions: it does not however pretend to give an answer to each of these questions. In particular, the aim is to facilitate interworking between different systems.

The reader may find in annex A of Part 1 an abstract of the survey carried out among the European companies.

Annex A of the present document contains tutorial material on X.500 technology whose concepts are often referred to as key elements for interworking.

1 Scope

The present document summarizes the users' views on the main issues related to private directory systems from a functional point of view. It deals with the design of these systems, their interworking as well as interworking between private directory systems and public ones.

The present document is applicable to private directory system design and provision. It should be seen as a source of guidelines to users.

A corporate directory is an implementation of a private directory for large companies. It is here defined as a repository for information shared by all departments in a corporation, an organization, or an institution.

A corporate directory is in contrast to the situation where different departments and functions maintain their own directories for their own purposes, and where such directories are not integrated to constitute an integrated appearance to all users.

This does not necessarily imply that a corporate directory needs to be centralized or centrally managed.

There are several directory technologies available. Issues concerning establishing a corporate directory are to some degree dependent on the selected technology. Most concepts given in the present document refer to the X.500 directory technology. It does not assume that the reader has a deep understanding of that technology. It is the intention here to keep the technical details down to a minimum. However, it is not possible to discuss deployment of a directory without referring to some X.500 directory concepts, like naming and information structures. Annex A gives a short introduction to the basic X.500 concepts for the benefit of those readers not familiar with such concepts.

Although EWOS closed in 1997 and a new organization ISSS (Information Society Standardization System) has been set up to continue producing specifications in same area, EWOS publications remain available for downloading. Therefore, some additional tutorial information can be found on the EWOS Web-pages:

http://www.ewos.be/dir/gtop.htm [12]

Nevertheless, as indicated in subclause 6.4 "Directory schema", interworking between the different directory systems implies conformance to some X.500 key concepts. In the remainder of the present document, concepts like Directory Information Tree (DIT), directory entry, Distinguished Name (DN), Relative Distinguished Name (RDN), Directory System Agent (DSA), Directory User Agent (DUA), Directory Management Domain (DMD), etc. are assumed to be known by the reader.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ITU-T Recommendation X.500 (1993) | ISO/IEC 9594-1 (1995): "Information technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Services".

[2] ITU-T Recommendation X.501 (1993) | ISO/IEC 9594-2 (1995): "Information technology - Open Systems Interconnection - The Directory: Models".

[3] ITU-T Recommendation X.511 (1993) | ISO/IEC 9594-3 (1995): "Information technology - Open Systems Interconnection - The Directory: Abstract Service Definition".

[4] ITU-T Recommendation X.518 (1993) | ISO/IEC 9594-4 (1995): "Information technology - Open Systems Interconnection - The Directory: Procedures for Distributed Operation".

[5] ITU-T Recommendation X.519 (1993) | ISO/IEC 9594-5 (1995): "Information technology - Open Systems Interconnection - The Directory: Protocol Specifications".

[6] ITU-T Recommendation X.520 (1993) | ISO/IEC 9594-6 (1995): "Information technology - Open Systems Interconnection - The Directory: Selected Attribute Types".

[7] ITU-T Recommendation X.521 (1993) | ISO/IEC 9594-7 (1995): "Information technology - Open Systems Interconnection - The Directory: Selected Object Classes".

[8] ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8 (1995): "Information technology - Open Systems Interconnection - The Directory: Authentication Framework".

[9] ITU-T Recommendation X.525 (1993) | ISO/IEC 9594-9 (1995): "Information technology - Open Systems Interconnection - The Directory: Replication".

[10] ITU-T Recommendation X.402 (1995) | ISO/IEC 10021-2 (1996): "Information technology - Message Handling Systems (MHS) - Overall Architecture".

[11] EWOS/ETG 027: "Security Architecture for the Directory".

[12] http://www.ewos.be/dir/gtop.htm.

[13] http://www.ema.org/html/at_work/dirsync.htm.

[14] Internet specification RFC-1274 (1991): "The COSINE and Internet X.500 Schema".

[15] TR 101 153-1 (1998): "Users' views on addressing and directories; Part 1: Requirements for design and interworking".

[16] ITU-T Recommendation I.112 (1993): "Vocabulary of terms for ISDN".

[17] ITU-T Recommendation I.510 (1993): "Definitions and general principles for ISDN interworking".

3 Definitions, symbols and abbreviations

In the present document, particular attention should be given to the meaning of the word "private" which, in this context, has been used to indicate that a directory was designed and build by a company or an individual for his own purpose. Where information with privacy aspects is contained in one part of a directory, this part is referred as "restricted use directory".

NOTE: This document makes frequent mention of the "X.500 standard" and similar terms relating to "X.500". In the absence of any more precise reference, the occurrence of such an expression in this text may be taken as referring the **X.500 series of ITU-T Recommendations**, which include [1] to [9].

3.1 Definitions

For the purposes of the present document, the definitions of Part 1 (TR 101 153-1 [15]) apply:

business user: User using telecommunication product/services while performing business tasks which have no direct relationship with the telecommunication business.

corporate directory: An implementation of a private directory for large companies. A corporate directory is here defined as a repository for information shared by all departments, subsidiaries, etc. in a corporation, an organization, or an institution. These different elementary parts are often placed in different countries and may have separate directory systems interconnected and managed in an harmonized way to build a corporate directory.

directory: System or service allowing users and applications to find information related to a category of people, e.g. employee of a company, subscriber of a network, etc. In the following clauses, unless otherwise specified, the word **directory** will be used for **corporate directory**.

end-user: A person or machine delegated by a customer to use the service facilities of a telecommunication network, (term 401 of ITU-T Recommendation I.112 [16]) e.g. consumer, residential or business user without any technical knowledge of telecommunication technology using telecommunication terminals.

interface: The common boundary between two associated systems (term 408 of ITU-T Recommendation I.112 [16]).

interoperability: The ability to communicate between end-users across a mixed environment of various domains, networks, facilities, equipment, etc. from different manufacturers.

interworking: Interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication (ITU-T Recommendation I.510 [17]).

IT&T manager: Person responsible in a company for telecommunication and information technology activities.

personal directory: Directory managed by an individual for his own use. In general, this is achieved with a personal computer connected to available databases (e.g. public and private directories) and appropriate software to process the local database and add the additional information needed.

private directory: Directory built and managed for private purposes. This may be achieved for home use or business use.

public directory: Directory built and managed for public use.

residential user: User using telecommunication means in private premises.

restricted use directory: Directory containing information with privacy aspects. This may be handled as a "restricted part" of a private directory. In any case this means that it contains information which should not be known outside a small group of people. This can be information on individuals or business information containing competitive aspects.

Service (Telecommunication Service): That which is offered by an Administration or ROA to its customers in order to satisfy a specific telecommunication requirement (term 201 of ITU-T Recommendation I.112 [16]).

NOTE: Bearer service and teleservice are types of telecommunication service. Other types of telecommunication service may be identified in the future.

single-location directory: Directory related to users in a single location within a single ownership/business.

user: Without specific addition this word is used to identify the telecommunication user community in general, e.g. end-users and IT&T managers. It means user of products or services possibly conforming to standards.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ADDMD	Administration Directory Management Domain
API	Application Programming Interface
CD ROM	Compact Disk Read Only Memory
CSV	Comma Separated Value
DAP	Directory Access Protocol
dap	Directory Access Protocol
DIB	Directory Information Base
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DMD	Directory Management Domain
DN	Distinguished Name
DNS	Domain Name Server
DSA	Directory System Agent
DSP	Directory System Protocol
DUA	Directory User Agent

ECMA	European Computer Manufacturers Association
EDP	Electronic Data Processing
EIDQ	European International Directory Inquiry
e-mail	Electronic mail
ETSI	European Telecommunications Standards Institute
EWOS	European Workshop for Open Systems
EWOS/EG DIR	EWOS Expert Group on Directories
ID	IDentifier
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISP	International Standardized Profile
ISSS	Information Society Standardization System
IT&T	Information Technology and Telecommunications
ITU-T	International Telecommunication Union - Telecommunication Standardization Bureau
JTC1	ISO/IEC Joint Technical Committee No. 1
LAN	Local Area Network
ldap	Lightweight Directory Access Protocol
MHS	Message Handling System
NDS	Network Directory System
OCG	Operational Co-ordination Group
OSI	Open Systems Interconnection
OSITOP	European User Group for Open Systems
PBX	Private Branch Exchange
PC	Personal Computer
PNO	Public Network Operator
PRDMD	Private Directory Management Domain
RDN	Relative Distinguished Name
RFC	Request For Comment (Internet Society)
SME	Small and Medium Enterprises
SMTP	Simple Mail Transfer Protocol.
SNADS	System Network Architecture Distribution Services.
SOHO	Small Office, Home Office.
TG	Topic Group
UPT	Universal Personal Telecommunications
VAT	Value-Added Tax
WWW	World-Wide Web

4 General considerations

Probably the first question to arise when designing a directory system is why a new directory system is needed when there are already so many in the company. The answer may be that a single suitable directory is far better than several outdated ones. The following set of considerations should help in designing a reliable one.

4.1 Who will use the directory system?

Several types of users may be identified: the end user or their secretary, switch board attendant, people in charge of the administrative management in the company, people in charge of the technical management of information.

In fact, among the operators and service providers there are also of course people in charge of directory management but this is not the purpose of our study, which is user oriented.

In addition, it should be recalled that directory information is not only used by **people** but also by **applications** (for instance e-mail, videoconferencing, workgroup software and automatic information desks).

Obviously, these different users need different information types.

4.2 What is needed in a directory?

A directory is vital to find additional information related to a person, or to something else, on whom/which the enquirer has some piece of information:

- someone (or an application) known by name; or
- has activities or competencies in a given area; or
- is in charge of a department; or
- lives or works in a given geographical district, in your or another company, in a private or public area, etc...

4.3 What for?

- to get more information;
- to pay a visit to someone;
- to call someone by phone;
- to access a database, a server;
- to send a document by mail, fax or e-mail;
- to update some information;
- to send a purchase order;
- to pay a bill via electronic means; or
- to manage a commercial transaction.

4.4 How is updating to be managed?

The following aspects of management have to be considered:

- data management;
- management of the directory system;
- management of the directory service,

and special care should be given to the definition of who is in charge of updating each piece of information in the directory system and what level of security should be given to these tasks.

4.5 And finally, how could a directory system provide your company with competitive advantages?

A directory system can make information on a company and its products available to its customers. Should this possibility be developed with the necessary access restrictions then this could help the company's commercial communication and offer competitive advantages - provided the design is appropriate.

5 General specifications

This clause contains indications on the design of directory systems and tools for their management and automated updating.

Since paper directories are still widely used for many reasons, electronic directory systems are seen by the users as the best means to provide up-to-date information.

A unique centralized system being impracticable, the Information Technology and Telecommunications (IT&T) managers should implement tools to consolidate information from different sources inside and outside the company, since, even within the same company, there are often quite different systems from different providers where some relevant pieces of information are stored and between which interworking is needed.

The end-users (person or unit) will wish, in most cases, to put in place their own customized directory system comprising relevant elements obtained from different sources.

5.1 Content

The survey (see annex A of TR 101 153-1 [15]) gives a good idea on the main information to be included in a corporate directory.

Information about people may be classified in four categories.

5.1.1 Identification

- Mr, Mrs, Ms
- surname
- given name
- photo
- etc.

5.1.2 Geographical localization

- postal address
- physical address
- site
- room number
- building
- etc.

5.1.3 Organizational affiliation

- company
- organizational unit
- division
- function
- speciality, activity, competence area

- hierarchical position
- direct senior officer
- etc.

5.1.4 Communication means

- fixed phone
- mobile phone
- fax
- e-mail address
- secretariat
- pager
- switch board attendant
- etc.

The above elements have been proposed as a basis for standardization by ETSI of the content in order to allow information interchange tools to work between the different information sources.

5.2 Data interchange

Since there is a clear need for consolidation or synchronization of information between different sources, relevant interfaces have to be designed and implemented. This is true for corporate directories as well as for personal customized directories. Some additional information may be found at http://www.ema.org/html/at_work/dirsync.htm [13].

The standardization of these interfaces has been proposed for inclusion in the ETSI Work Programme.

5.3 Security aspects

Since there are understandable reservations about making public any information in a private directory, tools are needed to restrict access to the accredited persons only, according to the type of information concerned.

Similarly, if encryption keys for secured transactions are to be stored in a directory system, access and management of these parameters should obviously be restricted to authorized personel.

5.4 Data management

Although there is a need for a corporate directory system manager, information updating should more and more be dealt with in a decentralized way. Therefore, tools should be implemented to manage which parts of the database are allowed to be updated by each local manager.

5.5 Search tools, editing and downloading facilities

Sophisticated means are required by the end-users to allow them to find someone not only starting from the approximate spelling of the name but also from quite different criteria like function, professional skills, etc.

Editing and downloading facilities are also required to enable printing and data extraction according to end-user criteria and in order to prepare a private directory on paper.

6 Corporate naming and directory schema

6.1 Introduction

When establishing a corporate directory service, there are many aspects to be considered. This clause considers the following aspects:

- unambiguously naming all items or objects to be represented in a directory; and
- how information is structured.

The above aspects are part of what is referred to as the directory schema. Some tutorial material on directory schema definitions can be found in subclause 6.4 "Directory schema".

It is assumed here that a directory is either based on the X.500 technology or at least complies with the specifications described in subclauses 6.3 and 6.5 necessary to ensure interoperability. It is also assumed that the reader has a basic knowledge of this technology. However, it has been attempted to keep the technical details down to a minimum level.

It is important to remember that each object represented in an X.500 directory is represented by an entry in the directory and that the entries are placed in a so-called Directory Information Tree (DIT) where the placement of the entry is determined by the object's (or entry's) name.

A few notes on directory schema are presented in the following subclauses.

6.2 Understanding the directory environment

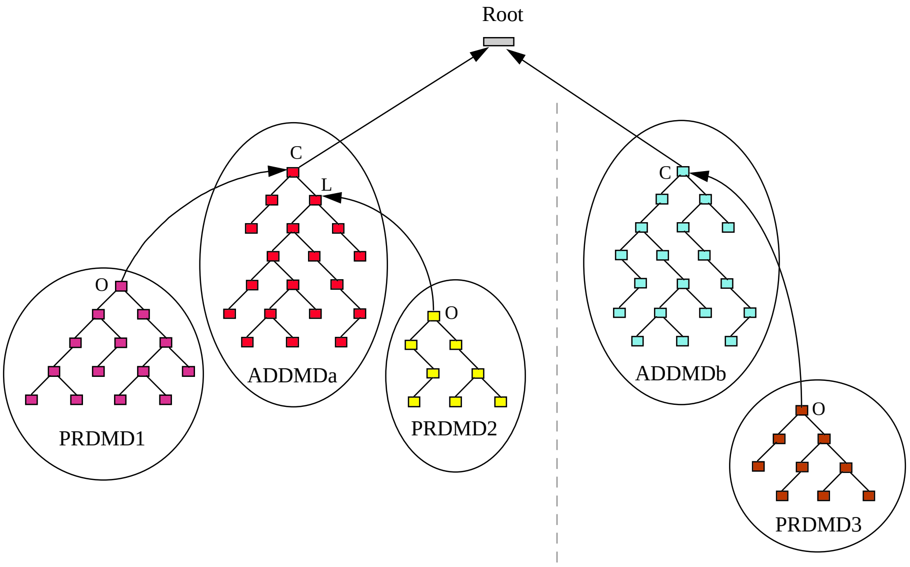

Figure 1: Scope of a corporate directory

This section describes the scope of a corporate directory with respect to a more general directory infrastructure, e.g. a pan-European Directory. This is illustrated in figure 1, where a number of Administrative Directory Management Domains (ADDMDs) and Private Directory Management Domains (PRDMDs) are shown. In this simple figure the PRDMDs represent the corporate directories, while the ADDMDs are public service provider directories. The ADDMDs have the responsibility for establishing a wider directory infrastructure and for holding the country entry, while the top entry in a PRDMD has the organization entry as the top of its tree (subtree).

It should be understood that this is quite a simplified picture. There may be several ADDMDs in a single country each wanting to hold the country entry. This introduces a number of issues, which can be more or less ignored by a corporate directory (PRDMD) and therefore are out of scope of the present document. Likewise, ADDMDs are faced with other particular issues for their interoperation, which are also outside the scope of the present document.

The scope of the corporate directory as treated in the present document represents the situation where a corporate directory is either an isolated directory not connected to any general infrastructure, or if it is connected, it is subordinate to some ADDMD. Thereby, it is shielded from the particular ADDMD problems. Connecting to a wider infrastructure will allow information provided by the corporate directory to be accessed from the outside, and it will allow corporate users to access information outside the corporate directory, e.g. information in another corporate directory or in a public directory. Even if a corporate directory is initially an isolated directory, it should be part of the planning that it may at some later time be connected to a wider directory infrastructure.

An international organization has additional issues to consider when establishing an international corporate directory. Such issues are examined in subclause 6.6 "International organizations".

6.3 Objects in a directory

6.3.1 Object classes and attribute types

As explained in subclause 6.4 "Directory schema", an entry is created based on an object class specification determining the characteristics of the entry. An organization therefore has to decide what object classes to use for the different entries.

An object class specification also determines what attribute types can be represented in an entry, i.e. it determines what kind of information can be stored in the entry in question.

The base X.500 standard defines several object classes and attribute types (see ITU-T Recommendation X.520 | ISO/IEC 9594-6 [6] and ITU-T Recommendation X.521 | ISO/IEC 9594-7 [7]). These object classes and attribute types should first be considered and used whenever possible. If they do not fulfil reasonable requirements other generally used schema elements should be used. The EWOS Web-pages [12] point to such general used schema definitions.

When deciding what object classes to use for entries in a corporate directory, it is important to know the concepts of structural object class, subclass and auxiliary object class. Tutorial material on these issues is also available on the EWOS Web pages [12].

The following subclauses further consider this issue.

6.3.1.1 Organizational persons

When creating entries for organizational persons there are several different object classes that can be considered:

- The X.500 standard defines an object class for persons in general from which the two basic object subclasses for persons, one for residential persons and one for organizational persons (**organizationalPerson**), are derived. The organizational person object class has some limitations with respect to allowable attribute types. When this object class is used, it will in most cases have to be supplemented with one or more auxiliary object classes.

- ITU-T Recommendation X.402 | ISO/IEC 10021-2 [12] defines an auxiliary object class called **mhs-user** which, when combined with a structural object class like **organizationalPerson**, allows inclusion of X.400 relevant attribute types.

- The Internet specification RFC-1274 [14] specifies a number of schema elements that are widely used, e.g. in the NameFLOW-paradise project. This RFC defines a structural object class (**pilotPerson** object class) that can contain quite a lot of useful attributes. However, it is most useful in the academic society.

- The European International Directory Inquiry (EIDQ) activity, which is making schema specifications mostly for the telephone numbering service, is also defining its own person object classes. It has defined a **fdasResPer**, which allows inclusion of several generally usable attributes, but also some that are quite EIDQ specific. The EIDQ specifications cannot be considered stable at the present time.

- An organization could define its own object class either as an auxiliary object class that can supplement some other person related object class, or it can define a complete replacement structural objects class. Defining one's own object classes should be absolutely the last choice.

- EWOS/EG DIR has defined an auxiliary object class. This auxiliary object class allows inclusion of all attribute types which have been judged useful.

6.3.2 Representation of roles

An organization may want to make a distinction between a person as an individual and as a person performing a particular role. Likewise, a user accessing the directory may at some time want information about a particular individual and at other times want information on a particular function within the organization, e.g. the person responsible for education.

A particular person may at a certain time be represented by more than one entry where only one of those is the person’s individual entry. The person "behind" a functional entry may change over time, but the entry itself is maintained.

If the same person is performing a particular function over a longer period, pointers can be established between the person's personal entry and the functional entry.

6.4 Directory schema

For directory information to be usable and accessible, it has to be organized in a pre-defined way. The rules for how directory information is organized is called the directory schema.

The directory schema is made up of several elements:

- *Object classes* are specifications of the characteristics or an object of a particular type, e.g. a residential person, and therefore determine the contents and other features of the entry representing such an object.

- The entry information is stored as a number of attributes each representing a particular piece of information. The characteristics of an attribute are determined by an *attribute type* definition, which is a specification of its structure and syntax. The syntax can be quite simple or be rather complex.

- When interrogating entry information, it is in many cases necessary to compare the value of an attribute with some data element presented in the user request. This is the case for searches where entries are selected based upon whether they fulfil certain criteria. The rules for how such a comparison shall be made are called *matching rules*. Matching rules can be quite simple like an exact match between two integers, or they can be rather complex, like a word rotation matching rule, phonetic matching rule and other approximate matching rules. While commonly recognized matching rules are implemented in all X.500 products, more special matching rules require special implementation.

- An entry's placement within the Directory Information Tree (DIT) and its name structure is determined by a *structure rule*.

All the above schema elements, and a few more, determine the characteristics of an entry and its relation to other entries.

For a Directory System Agent (DSA), i.e. a directory server, to contain a particular entry it is necessary for the DSA to have implemented all the schema elements that govern the characteristics of that entry.

For a Directory User Agent (DUA), i.e. a directory client, to access this entry and utilize the stored information, it also needs to have a pretty good understanding of all the schema elements. If users through their DUAs access different directory domains, they would expect the same type of information, like an e-mail address, to be controlled by the same schema element independent of location, otherwise the DUA may not be able to utilize the information.

If all organizations, like the Internet, private organizations, national groups, etc., each independently make their own directory schema definitions, which is somewhat the case today, it will not be possible to make a truly integrated European directory. Even though it may be possible to physically interconnect different domains, they will not be able to utilize each other's information.

6.5 Naming aspects

The X.500 Directory standard requires every object (person, organization, etc.) which is to be represented in a directory to be unambiguously named. A directory name is composed of a number of name components forming a hierarchical structure. Typically, the first component is a country code, the next a locality name, the next again the company name, and so on.

Naming is probably one of the more difficult aspects to consider when establishing a corporate directory.

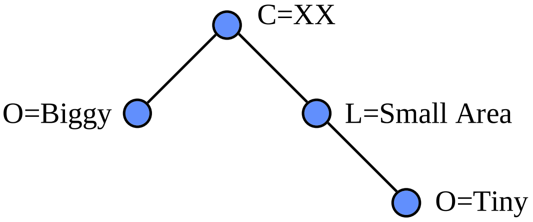

Figure 2: Location of main entry for organization

Account should be taken of the fact that the corporate directory might, in the future, connect into a wider directory infrastructure, e.g. a national or a European structure. It should be checked whether there are some national recommendations on how organizations should be named in a wider directory context. A large corporation will probably have its main entry located right under the country entry, while a smaller organization might have its entry under an entry representing a smaller area, like a postal district.

This is illustrated in figure 2. The large organization to the left has its entry just below the country entry and the name of the main entry is then: { C=XX; O=Biggy }. The organization to the right is a smaller organization represented by an entry having the somewhat longer name: { C=XX; L=Small Area; O=Tiny }.

6.5.1 Corporate subtree

6.5.1.1 General considerations

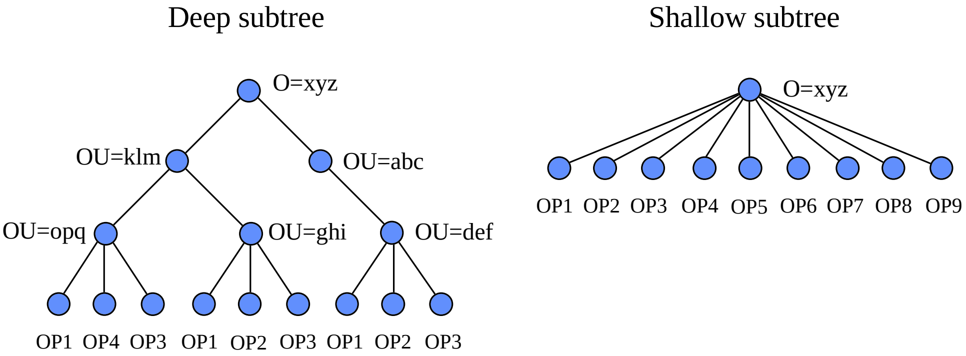
Deep subtree
O=xyz
OU=klm
OU=abc
OU=opq
OU=ghi
OU=def
OP1 OP4 OP3 OP1 OP2 OP3 OP1 OP2 OP3
Shallow subtree
O=xyz
OP1 OP2 OP3 OP4 OP5 OP6 OP7 OP8 OP9

Figure 3: Deep and shallow subtrees

Selecting a naming structure is one of the more crucial choices to be made by an organization when setting up a corporate directory. The choice of naming structure influences the usefulness of the directory, and it affects how the directory can be maintained. The organization's naming tree forms a subtree of a more global Directory Information Tree (DIT), where the organization entry is the root of that subtree as illustrated in figure 1 and as explained in the associated text.

An organization can select to make its subtree deep or shallow. Figure 3 illustrates the extremes of these two approaches.

The left side illustrates the situation where the naming structure, and thereby the information structure, reflects the structure of the organization. The naming structure will then have levels corresponding to the organization hierarchy. The right hand side of the figure shows the other extreme where the naming structure has only a single level below the organization entry. The two approaches have both advantages and disadvantages.

In each particular situation some combination or some in-between solution may be selected, taking into consideration that each approach has advantages and drawbacks. Next are some considerations on how the two approaches can be combined to cope with different situations.

The deep subtree has the following advantages compared to the shallow subtree:

- Reduced number of nodes per level:
  - Anything else equal to any particular entry, e.g. an organizational unit entry, will have fewer subordinate entries in a deep tree than in a shallow tree. This makes it easier to ensure unique naming, as name components (Relative Distinguished Names) only have to be unique with respect to the superior entry. In the shallow tree there is a larger likelihood of collapse of names. Names or identifiers, e.g. initials, may only be unique within a single department.
- Support of registration:
  - This advantage is related to the previous one. The process of establishing unique names or identifiers for persons and functions can be distributed within the organization. This advantage is of course dependent on whether there are organization-wide unique identifiers of employees in place. In many organizations each employee is given a unique identifier, most often based on initials for other purposes, such as log-on identifier on the local Information Technology system.
- To achieve geographical or organizational subdivision:
  - Large corporations may be dispersed in two ways:
    - geographically dispersed, where each location has some autonomy, e.g. own personnel department, employee policy, etc..
    - have very different objectives in the form of services provided, products, customers, etc..

In such organizations it will probably be a requirement to have separate subtrees for such dispersed units:

- To express ownership of part of the DIT:
  - Particularly in large organizations it may be a requirement that a certain department can claim ownership of its part of the DIT. This is not easily achieved if the departmental entries do not form a subtree of its own.
- Partitioning into administrative areas:
  - Different parts of the corporation may require to manage their own parts of the corporate subtree. This may be a requirement even in the case where the department does not have a DSA of its own. This will in any case require that the department needs to be represented by a subtree of its own.
- Shared information:
  - A set of entries may share some common information, e.g. a number of a fax machine serving several people. The X.500 standard has feature for supporting that, but that is most easily established if the entries sharing some piece of information form a subtree of their own.
- Access control:
  - Access control capabilities have to be specified with respect to entries to be accessed and with respect to users accessing these entries. Access control specifications are easier to make and maintain if the entries having the same access restrictions form a separate subtree and if the users (or their entries) whose access rights have to be specified also form a subtree.

- Localise a service to part of the DIT:
    - It may be convenient to have the entries representing a particular service, e.g. the Electronic Data Processing (EDP) department, in a separate subtree.
- Distribution of subtrees into different DSAs:
    - Distributing a corporate directory across several DSAs is more easily accomplished and managed if the part of the subtree to be put into a particular DSA is itself a subtree.
- Starting points for searching and browsing:
    - A corporate wide search for a particular entry may be resource demanding, especially if the corporate directory is distributed across several DSAs. By having a deep subtree, it is possible to start the search somewhere down in the subtree, thereby restricting the search to only a part of the corporate directory.
- To document the organization.

The shallow tree has different advantages:

- The organization can change without changing names:
    - A subtree that reflects the organization will have to be changed when the organization changes. All names of objects represented by entries are then changed at the same time. The need to be rebuild the directory may be a major undertaking, depending on the administrative tools available. This one aspect may be so important that it outweighs many of the advantages of a deep subtree.
- Short names:
    - A shallow tree gives shorter names. This may be an advantage in some circumstances.

Whether the deepness of a subtree affects search performance is implementation dependent. A shallow subtree does not necessarily give a better search performance than a deep subtree or vice versa.

6.5.1.2 Naming recommendations

Based on the above general considerations it is possible to make some recommendations on the allocation of names.

Distinguished names (i.e. the complete name starting from the root down to the object in question) are used to reference objects in many places. It is therefore important that names that are referenced in this way be stable over time. Examples of where distinguished names are used are listed in the following:

- Aliases:
    - An alias entry is an entry pointing to another entry thereby giving an alternative (alias) name for an object. The pointer is the distinguished name of the entry to which it points.
- Other types of pointers:
    - Some attributes are pointers to other entries. For example, the **seeAlso** attribute points to one or more other entries using the distinguished names of those entries.
- List of names:
    - It is possible to establish a list of names. Such names are distinguished names of other objects, normally persons.

Dependent on to what degree such pointer information is established in a corporate directory, it is evident that frequent changes of distinguished names result in a heavy administrative burden and a high risk of inconsistency in the directory. It is therefore essential to limit the changes of distinguished name with organizational changes to a minimum.

When establishing a DSA it has to be determined what the naming prefix is for the entries in the DSA, i.e. what are the top entries from the root down to the organization entry and how are they named. This requires the organization name to be properly registered by an external registration authority and it requires that, within the country, is established an overall structure for the top part of the country subtree. If such information cannot be established from the beginning and arbitrary choices have to be made, later changes may require considerable administrative effort (for selection of organization Relative Distinguished Name (RDN) see subclause 6.5.2.1 "Organization names").

6.5.2 Allocating names

Directory names have to be unambiguous, i.e. there may not be two objects having the same name. At each level of the corporate subtree uniqueness in naming has to be achieved. Allocating name components (RDNs) for different entries in the corporate subtree is not that difficult for objects where the naming is completely under the organization's control and where feelings are likely to be less emotional, such as names for organizational units, organization functions, e.g. accounting, servers, printers, etc. It is more difficult for the top of the subtree, i.e. the organization entry, and for the bottom of the subtree, where persons are to be named.

6.5.2.1 Organization names

The organizational entry is here assumed to be the top entry of the corporate subtree. Allocating a name for this entry is of course no problem if the corporate directory is never to be connected into a wider directory infrastructure, but such an assumption should not be made. As discussed at the start of clause 6, the organizational entry in a wider directory infrastructure will typically be subordinate to an entry representing some geographical area, either the whole country or a smaller area. The organization name needs to be unique within that area, which requires some kind of external registration authority. If such an authority is not in place for the particular area, there is a risk that the a selected name for the organization may not be unique. In such a situation the organization could consider using a protected name, if the organization name has one. As an example McDonnell would probably consider its name protected, and will sue any other company using that name. An organization could also consider using its Internet domain name, if it has one.

6.5.2.2 Naming persons

Persons are normally quite particular about their names, so giving names (RDNs) to persons can be a difficult task. Assigning unambiguous names to residential persons is especially difficult, but this is outside the scope of the present document. However, assigning names to persons in an organization also requires careful consideration.

Some personal names are quite common. Even within a somewhat small organization it is not unlikely that several people have the same name. By selecting a deep corporate subtree the likelihood of two persons having the same personal name in a small organizational unit can be made considerably smaller, but it is not zero and will have to be planned for by either attaching additional characteristics information to the personal name to make it unique, or by using a unique person identifier instead.

The first thing to consider is whether a person's full name should be used or some other unique person identification.

When assigning an RDN it is also necessary to define what attribute type(s) should be used as naming attributes. The X.500 standard defines a name form for organizational persons. This name form specifies that an attribute called **commonName** should be used as naming attribute. This name form also allows the **commonName** to be qualified by an organizational unit name, i.e. the RDN may consist of a combination of a common name component and an organizational unit name component. This may achieve unambiguous identification.

ECMA TC32 TG13 is also working on this issue and may provide some additional guidance on personal naming.

Organizations quite often assign unique identifiers to their employees. For smaller companies it may be a three character identifier (ID), whilst for larger organization more characters may be used. Such unique identifiers are used for log-on IDs, e-mailbox IDs, etc. Using such identifiers has the advantage that no additional naming registration is necessary.

6.6 International organizations

International organizations may have a directory system which encompasses several countries world-wide; therefore they need a harmonized naming policy between the related countries and thus an international, and not only European, registration authority for such naming.

6.7 Islands of directories

Private enterprises and public institutions are deploying private directory systems to satisfy internal needs. Such private directories contain information that can be relevant to provide to the outside world, such as telephone numbers for individual employees, job responsibilities, etc. On the other hand, users of a private directory may require access to information available in the global European directory.

7 Data interchange, synchronization, gateways

This text is based upon the following assumptions:

- the technical solution for data interchange, synchronization and gateways is based upon X.500 concepts;
- the directory (whether centralized or distributed) has its own database, fed by different sources.

7.1 Identification of interfaces and gateways needed

7.1.1 Between the directory server and providers of information

7.1.1.1 Inside the company

- the corporate database (staff data, etc.)
- e-mail directory
- PBX and telephone lists
- practical local information on the life of the enterprise (meeting rooms, medical services, internal mail circuits,...)

These are the different sources available to feed the corporate directory, first to initiate the population of the directory and then to regularly update it.

7.1.1.2 Outside the company

- Public directory services
- Other corporation directory services
- Internet
- Public registering systems (Name, Address, VAT, etc.)

7.1.2 Between the Directory Server and Clients

7.1.2.1 Inside the company

- e-mail
- telephone lists and systems
- groupware applications (e.g. Lotus Notes)
- security applications

- access control system
- paper extraction
- LAN, network resources directories (e.g. Novell NDS)

7.1.2.2 Outside the company

- teleworkers
- customers
- suppliers
- company's partners and subsidiaries

7.1.3 General scheme for information interchange

Figure 4 gives a general picture of the possible data interchanges between the different systems with some indication of the content of information exchanges, taking a corporate directory as an example. In this figure, the corporate directory system may or may not be centralized. This means that, if a decentralized solution is chosen, then the corporate directory system is made up of a network of several local servers with or without local replication of the entire database. In any case, the information is circulated between these local servers and possibly a corporate server.

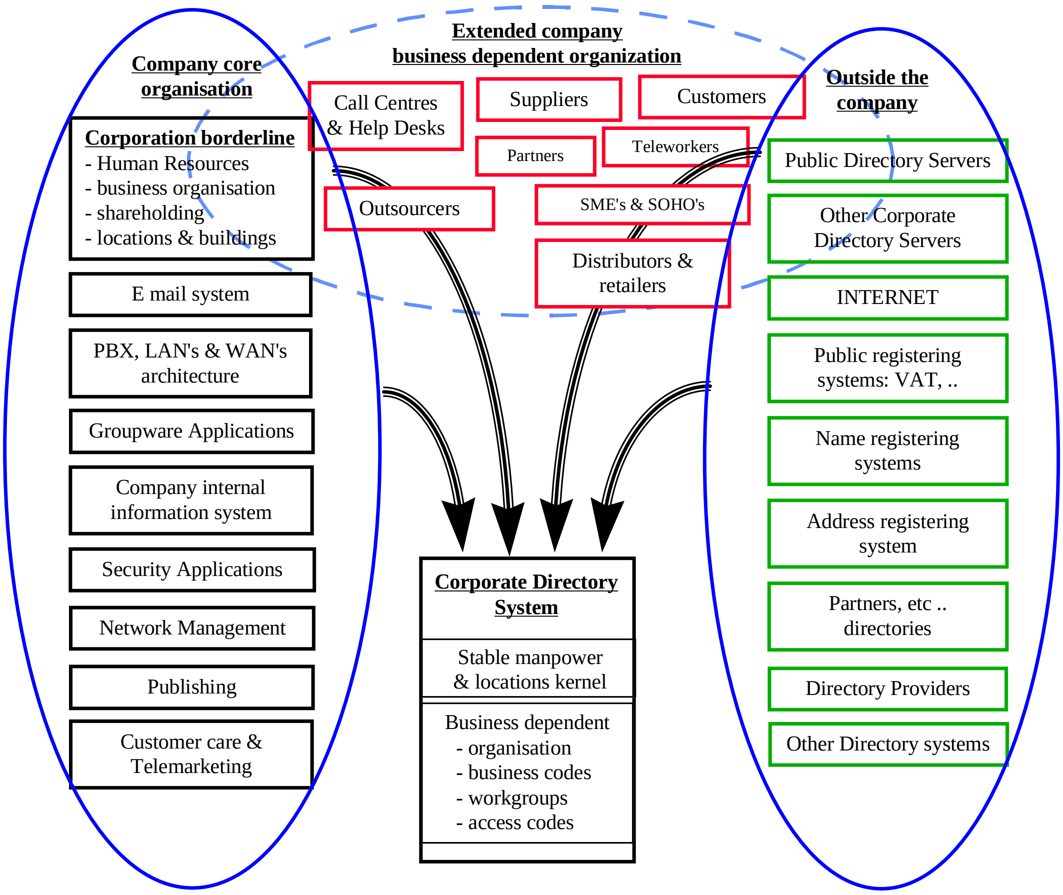

Figure 4: Information Input towards the Corporate Directory System

Table 1: Some indications on the possible content of information exchanges

Piece of information	From Inside the company	From Outside the company	To
Name, identifier	Corporate database (for ex. accounting)		The company directory server(s)
e-mail address	e-mail System	Internet or dedicated servers	The company directory server(s)
Phone number	PBX	Public directory services, other private directory servers	The company directory server(s)
Network address	Network management	Internet	The company directory server(s)
Local information	Company local information systems		The company directory server(s)
Updates	Any company directory server		Any other directory server in the company
Every "public" piece of information	The company directory server(s)		Public directory services, other private directory servers, any user

7.2 Objectives

7.2.1 Functional

Most of the applications listed in subclause 7.1 are based on their own directories, which may be outdated, encumbered with information about persons that have left the company, or who were transferred from one organizational unit to another.

To all these clients, the corporate directory can provide periodic information on the presence of a person within an organizational unit so that they can update their own information. All updating efforts may then be made only on the corporate directory, which then propagates the changes to its clients. The update is most likely to be decentralized, with the exception of the smallest organizations.

7.2.2 Technical

Formats and syntax have to be defined to allow easy data interchange between the different sources and clients. Technical solutions exist, the issue is to agree on which one should be adopted and possibly standardized.

7.2.3 Organizational

Related to naming, it may be difficult to find the right « key » to reach the right entry when synchronizing with a source of information. The couple « Surname-GivenName » may not be sufficient, and an unambiguous identifier may be necessary. This aspect is more organizational than technical. More details are given in subclause 6.5.

7.3 Solutions

- Synchronization products: most of the directory server products provide synchronization tools that allow to import flat files (CSV type);
- « dap » or « ldap » connections;
- APIs: these enable existing applications to sit directly on X.500.

7.4 Open Issues

A common identifier allowing synchronization of information between directories in different companies and with public directories is still to be defined and it has therefore been proposed that this issue be included in ETSI work programme.

8 Links with End-user

8.1 Introduction

End-users are interested in electronic directory systems because they expect to find there up-to-date information which might help them to locate the right person to communicate with.

To do that, they need to process the information delivered by the directory system, adding their own elements of information to make it relevant. Therefore, they need not only to get information from the system in the right shape but they require also that this information might be updated from the original database when there is a change, without losing the pieces of information they have added in their own database, each user having specific interests and needs. The latter may be stored either in the directory server or in the end-user's terminal.

8.2 Objectives, Requirements

Users often prefer looking for a person by using their own criteria even if this lowers system performance.

8.2.1 Search tools

When the name of the wanted person is not exactly known, nor his address, nor to which part of a structure they belong, the following features are required for quick identification:

- incomplete name search (namesake possibly non resolved) leading to a need for navigation means;
- phonetic search (homonyms with additional distortion), requiring a sophisticated resolution tool.

However, users want not only to get information on somebody where they know approximately the name but they want also to identify someone with specific skills, activity or responsibility and whom they probably do not know.

Therefore the directory application should enable searches using a selection of criteria taken from the list of preferred items for geographical localization or organizational localization:

postal address
site
building
room number

company
organizational unit
division
function
speciality, activity
hierarchical position
direct senior officer

To be more effective such search tools should include navigation means.

8.2.2 Editing facilities

Since paper directories remain very popular, the directory system should allow the printing of a selection of the information sorted according to the user's requirements.

8.2.3 Downloading and updating facilities

To fulfil the need for managing their personal customized electronic directory, users need not only to get information from the system in the right shape but they require also that this information be updated from the original database when there is a change, without losing the pieces of information they have added in their own database.

If end-users are expected to update some parts of the company directory, the facilities available for that should be user friendly enough to encourage the user to perform this task.

8.2.4 Interfaces

The interface between the directory system and the end-user terminal should be compatible with the most popular terminals and software.

8.3 Solutions

Most current directory systems provide advanced searching tools enabling the different kinds of searches described in subclause 8.2.1. Technical solutions for advanced updating as described in subclause 8.2.3 are available in most directory systems.

Taking into account the large flexibility needed for searches, downloading and editing facilities, the directory system has, in addition, to provide the same sorting and editing tools as those supplied with most current database systems. These tools could therefore be used by the end-user and by the people in charge of preparing the corporate directory on paper.

9 Management, updating

9.1 Introduction

The following aspects of management have to be considered:

- data management and update;
- management of the directory system;
- management of the directory service.

9.2 Objectives

Data management has to deal with the directory content for the lifetime of the directory:

- schema administration;
- who is responsible of which data;
- updating organization: regular synchronization as well as real time updating;
- access control: who can read, create, modify what?
- authentication needs;
- etc.

Management of the directory system is more or less complex depending on the chosen architecture (centralized, distributed).

It has to deal with the current operation of the components of the directory system:

- directory domains;
- DSAs and DUAs;
- replication strategy...

Management of the directory service has to deal with:

- quality of service monitoring and reporting: logs, statistics, optimization...;
- accounting aspects.

The directory designer should have all these issues in mind but the remainder of this clause deals with the management and update of data. Since it would be very difficult to provide a solution for every situation, a list of issues to consider is given hereafter.

9.3 Open issues

A corporate directory is a living thing - it is perpetually changing - as companies change and the people within a company change. People (or objects) whose names and addresses are contained within a directory change their names, change their jobs, change the location they work at. Companies expand or contract the number of locations they operate from, they expand or contract the number of employees at those locations, they take over new companies or divest companies: therefore the directory or directories change accordingly.

All these directory changes have to be managed, if not the directory rapidly becomes out of date and because people cannot rely upon it the directory falls into disrepute. An inaccurate directory can often be worse than no directory at all. Therefore if a company is prepared to set up a corporate directory it needs also to be prepared to administer and manage that directory to ensure that it is as accurate as humanly possible.

A directory can be managed dictatorially (centralized and strongly controlled) or democratically (decentralized and lightly controlled).

The management of a corporate directory system depends upon a number of different factors.

1. Company culture:

   1a. Whether or not the company has a centralized or decentralized policy.

   1b. The number of changes made by the company (is it a stable company or always changing?).

   1c. Relationship of the company locations with each other.

2. The size of the company:

   2a. Number of different sites (i.e. factories, offices, depots etc.) which have directory systems.

   2b. The number of directory domains and the number of people within each directory domain.

3. The types of systems utilized by a company which require a directory:

   3a. Are all the systems requiring directories of the same type?

   3b. Does the company have separate directories for telephone, data and e-mail?

9.3.1 Managing the input

The input to the directory will depend upon whether it is centralized or decentralized.

In cases where the directory is decentralized the local system handles the connection between the directory and the end users.

In a centralized system the directory is usually maintained in one large database. The input can be downloaded to the central database location from each local site.

The personnel function should contribute with a large input into a directory. It is the only function within a company that knows the changes of personnel and when they occur. Far too often a directory becomes the responsibility of an Information Technology support centre and they only receive second hand information and very often late.

Another possibility is to rely on the accounting department for taking care of the directory database management since people in this department have a good view on the staff (wages) and financial flows with partners, customers and suppliers (invoices and bills).

9.3.2 Managing the output

The output from the directory will depend upon whether it is centralized or decentralized.

In cases where the directory is decentralized, the local system handles the connection between the directory and the end users.

In a centralized system the directory is usually maintained in one large database. The output for each location can be downloaded to each local site and distributed from there.

For a centralized system the input/output function can be automated allowing end-users to access the central database to update or output the data they require. These functions can be carried out by using the electronic mail system.

9.3.3 Directory Management Standards

The standards requirements and development for directory management represent a considerable problem. The major difficulties are the great diversity of management techniques which can be used for a given number of directory functions. The most appropriate method would be to provide a series of guidelines and recommendations which cover a set of different scenarios.

10 Security - privacy - misuse prevention

10.1 Introduction

This chapter deals with procedures intended to ensure that data cannot be altered by mistake or malevolence and that any unwanted use of the information be avoided. More precisely:

- security is related to how to avoid any unwanted change;
- privacy - how to restrict access to the authorized people only; and
- misuse prevention - to how to prevent too easy production of lists of people fitting sophisticated combinations of several criteria.

10.2 Objectives

10.2.1 Security

Regarding the database, security procedures should ensure that data remain in conformity with the data dictionary and that any piece of information is not entered twice.

Regarding the system, security procedures should ensure that people accessing the system can only have access to the information to which they have been given authorization and can change only the information they are allowed to change.

This procedure should be further reinforced by the management of information and controls.

10.2.2 Privacy

This issue is related to information with confidential aspects. In general this information is contained in the restricted use directory. In SME or in large companies, this is often a part of the private directory that may only be accessed by authorized people. In any case, this part is restricted to the company's employees but each employee should have access only to his allowed part.

No one other than the authorized persons should have access to any part of the database.

This means that strong authentication means are needed to prevent unwanted intrusion in this part.

10.2.3 Misuse prevention

Assuming that, in the near future, information is available on almost everybody in directory systems scattered all over the world, it could be possible, via sophisticated requests, to get a list of all people meeting specific criteria. Many misuses of such lists are easily conceivable and should be avoided.

It seems clear that the more meaningful the result of a search, the more confidentiality should be applied.

10.3 Open issues

Whatever the solution adopted, misuse of information should not be possible. In particular, obtaining lists of people meeting specific criteria should at least be very slow and/or difficult.

Annex A (informative): X.500 directory technology

A.1 What is a directory?

A directory is a repository of information about a number of types of objects organized in a particular way. A directory is typically established for some special purposes. There are many examples of directories for different purposes.

The most obvious examples are the white pages and the yellow pages of paper telephone directories. A white page directory is used for finding information about a particular person or organization using naming information as the search criterion, while yellow page directories are mostly used for searching for organizations that have some particular characteristics.

A price list is an example of directory in which the price can be found for a particular type of item. A department store catalogue is another example, where there can be several pieces of information about a particular type of item.

Electronic directories come in many different forms and for different purposes. All e-mail systems have some type of directory for proper handling of mail, e.g. routeing information. Some electronic directories are just configuration tables generated in computer memory during system initialization. A particular interesting directory is the Domain Name Server (DNS) used in the Internet environment to map names to addresses.

All types of directories have a common characteristic: they hold information about objects. Objects can be almost anything one would want to store and retrieve information about, such as persons, organizations, computer applications (on-line services), network components, etc..

A.2 The X.500 Directory

In 1984 ITU-T (then called CCITT) decided to develop a general purpose directory. The immediate requirement was to provide a directory for Message Handling (X.400). ISO/IEC JTC1 started a similar activity. It was decided quite early to merge the two activities into a single collaborative activity, so as not to produce two different standards for the same purpose. This collaboration on what is called the OSI Directory has worked very well and is still working.

The OSI Directory is an OSI application layer standard developed as part of the OSI standardization process. However, the OSI Directory standard has gained wide acceptance also outside the strict area of OSI. The term X.500 or the X.500 Directory is mostly used in preference to the more official title OSI Directory. Here we will often just refer to the Directory.

The Directory is specified in the ISO/IEC 9594 multi-part standard and in the ITU-T X.500 Series of Recommendations.

The texts in the two sets of documentation specifying the Directory are (with very few and insignificant exceptions) identical.

However, ITU-T calls its documents Recommendations, while ISO/IEC calls the same documents International Standards. The term "Specification" has been accepted as a common term. This term is used here.

The Directory Specifications are available in three editions:

1988 edition: This is the first edition and is issued as the multi-part standard ISO/IEC 9594: 1990 and as the CCITT X.500 (1988) Series of Recommendations. This edition specifies services, protocols and procedures necessary for basic directory operations. It specifies information models for how information is structured and some commonly usable information objects. In addition, it provides a common framework for general authentication techniques.

1993 edition: This second edition was issued as ISO/IEC9594: and as ITU-T X.500. This edition added some very useful functions, like shadowing of directory information, access control and significantly expanded the information model and administrative capabilities.

1997 edition: This is the third and so far the latest edition. It provides several minor and some extensive extensions. It adds a feature called contexts, which allow information to be distinguished according to the context in which it is being accessed. Another important addition is the provision of OSI Management of the Directory. It has also added and extended important security features.

ISO/IEC and ITU-T indicate different years for the same edition, due to different rules. The ITU-T indicates the year in which the work has been approved, and ISO/IEC indicates the year of official publication.

The Directory is not intended to be a general purpose database, but has mainly been developed for storing information about objects relevant to telecommunications, such as organizations, persons, distribution lists, OSI application-entities, etc. The information stored about an object is typically information relevant to communication with or about that object, e.g. its communication addresses.

The Directory specifications provide an information structure model, protocols for communicating directory information between open systems, and procedures that allow the directory information to be distributed among several independent systems, including procedures for navigation to the open system containing the information to be accessed.

An open system can locally maintain its part of the directory information using any suitable database technique.

A.3 Directory document structure

ISO/IEC 9594-1 | X.500:	Overview of Concepts, Models, and Services.
ISO/IEC 9594-2 | X.501:	Models.
ISO/IEC 9594-3 | X.511:	Abstract Service Definition.
ISO/IEC 9594-4 | X.518:	Procedures for Distributed Operation.
ISO/IEC 9594-5 | X.519:	Protocol Specifications.
ISO/IEC 9594-6 | X.520:	Selected Attribute Types.
ISO/IEC 9594-7 | X.521:	Selected Object Classes.
ISO/IEC 9594-8 | X.509:	Authentication Framework.
ISO/IEC 9594-9 | X.525:	Replication (not the 1988 edition).
ISO/IEC 9594-10 | X.530:	Use of Systems Management for Administration of the Directory (only the 1997 edition).

The 1988 edition of the Directory Specifications consists of 8 documents, which are the ISO/IEC 9594-1 to ISO/IEC 9594-8 or the corresponding CCITT documents.

The 1993 edition includes substantial extension to those parts, although the extensions to Part 8 are minor.

Part 9 on Replication is new for the 1993 edition.

The 1997 edition adds extensions to most parts. Part 10 on the Use of System Management is new for the 1993 edition.

A.4 Directory Information Tree (DIT)

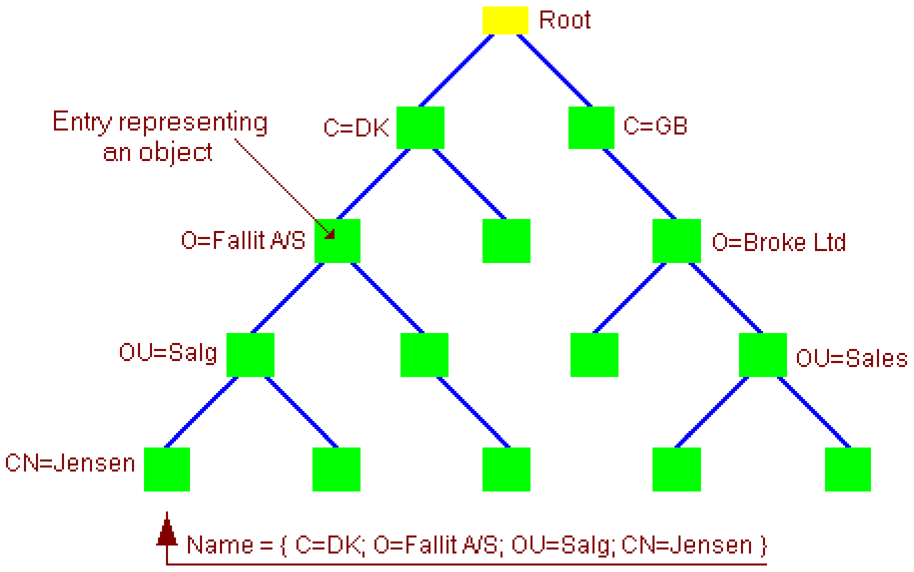
Root
C=DK
C=GB
Entry representing an object
O=Fallit A/S
O=Broke Ltd
OU=Salg
OU=Sales
CN=Jensen
Name = { C=DK; O=Fallit A/S; OU=Salg; CN=Jensen }

Figure A.1: Directory Information Tree

An object for which information is to be stored is represented by an entry in the directory. To store and retrieve information about objects, those objects have to be named. Each object and its corresponding entry have one or more names. A name has to be unambiguous - referring to just one object. However, an object may have more than one name.

Directory names are hierarchical in nature and form a naming tree, i.e. in the general case, a name consists of several components reflecting this hierarchy. This naming tree is called the Directory Information Tree (DIT), as a directory entry is associated with each vertex of this tree holding information about the object having the corresponding name.

The first level of names below the root is assumed to be names of countries and international organizations. (A country's name is its code taken from ISO 3166 - "Codes for the representation of names of countries").

In the example shown in figure A.1, the next level is the organization, like a company or governmental institution. The full name of an organization is then the country name concatenated with the organization name component, e.g. {C=DK, O=Fallit A/S}.

The next two levels in the example are the organizational unit and person. The corresponding names could be {C=DK, O=Fallit A/S, OU=Sales} and {C=DK, O=Fallit A/S, OU=Sales, CN=Jensen}, respectively.

The name component added as we move one step down the naming tree is called the Relative Distinguished Name (RDN) for the corresponding entry (and object). The name of an entry is therefore the concatenation of the RDNs from the root down to and including the entry in question. The root does not add any name component.

For names to be unambiguous the RDNs for entries just below a particular entry all have to be different. This requires some naming authority or possibly a hierarchy of naming authorities to be in place.

An object represented by the Directory always has a so-called distinguished name structured as described above, which is the principal name for the object. An object may also have one or more alias names, which are structured in a similar way.

The DIT concept is the very basic directory concept on which most other concepts are built.

Several independent directories, i.e. several independent DITs, may be created. However, if the names of the objects represented by these directories are all drawn from the same name space, such directories can be merged into a single directory (provided that they have compatible implementations, information structures, etc.). It is a generally held vision that eventually, with a very few exceptions, all directory information will be part of one "global directory", global in the sense that it is world wide, and global in the sense that it will be common for all directory uses, such as for Message Handling (X.400), EDI, general Internet, etc. The Directory Specifications have been developed with that view in mind and talk in general about the Directory.

A.5 The distributed DIT

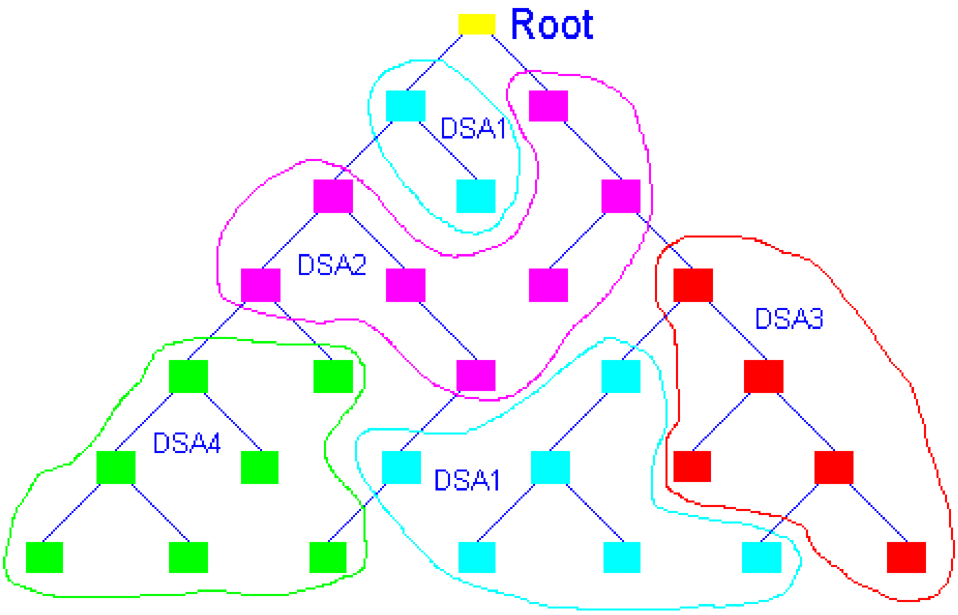

Figure A.2: The distributed DIT

A system that maintains and communicates directory information is called a Directory System Agent (DSA). A directory can be composed of any number of DSAs. Figure A.2 shows a rather simple DIT distributed among four DSAs. The figure also illustrates that the way a DIT can be distributed is very flexible. The entries can be distributed in any way among the DSAs and a DSA does not need to hold a contiguous set of entries.

Note, that the root is not an actual entry, it contains no information, and it is not held by any DSA.

A.6 The distributed directory

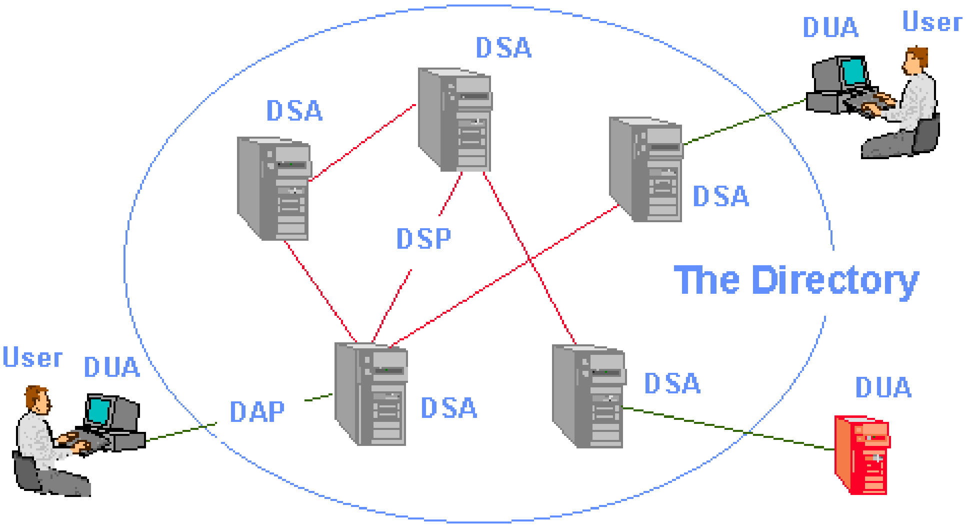

Figure A.3: The distributed directory

Figure A.3 illustrates the distribution of directory information among DSAs in another way. A user can access directory information by connecting to one of the DSAs. The function supporting the user in this access is called a Directory User Agent (DUA). The DSAs interact in such a way that the user can access information in the directory without needing to know the exact whereabouts of the particular piece of information accessed. The DSAs co-operate by use of distributed operations to provide this service to the users. The protocol used between two DSAs is called the Directory System Protocol (DSP). The protocol used between a DUA and a DSA is called Directory Access Protocol (DAP). There is an alternative access protocol called Lightweight Directory Access Protocol (LDAP), developed within the Internet Society.

LDAP is supported by several Web browsers. In addition, there are also several implementations of Web server/DUA gateways.

A.7 Directory Management Domains

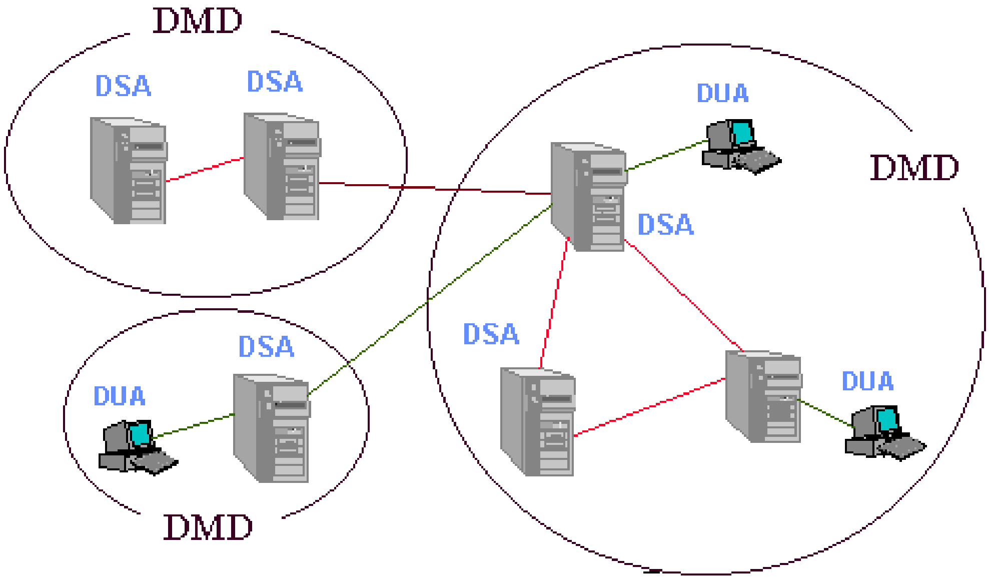

Figure A.4: Directory Management Domains

One or more DSAs and possibly some DUAs may be managed by a single organization. Such a set of systems is called a Directory Management Domain (DMD). A directory is therefore composed of one or more DMDs. Eventually, in a large directory infrastructure there may be thousands of DMDs.

The concept of DMDs is only to a limited degree reflected in the X.500 Directory standard. It is more related to how a directory is established with respect to interconnection and with respect to the scope of operation and management. The concept of DMD does not in itself impose restriction on how DSAs are interconnected, but a DMD may for security and management reasons be restricted to only have external communication with other DMDs through a dedicated DSA.

For mainly historical reasons, two different types of DMDs have been identified. A Private Directory Management Domain (PRDMD) is a DMD that serves the internal needs of a corporation, organization, or an institution. An Administrative Directory Management Domain (ADDMD) is a DMD run by a public service provider to serve the needs of a public service, like telephony, e-mail, etc. In addition, ADDMDs provide services to PRDMDs by providing the backbone of a directory infrastructure.

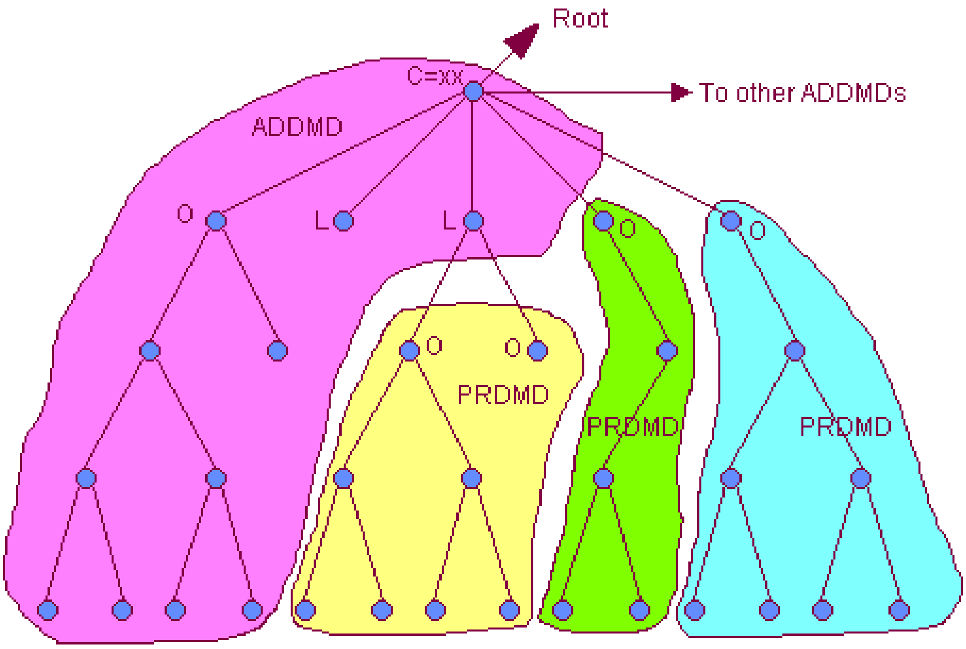

Figure A.5: ADDMDs and PRDMDs

It should be understood that the distinction between an ADDMD and a PRDMD is not always clear. However, it is useful first to consider the "pure" cases of ADDMDs and PRDMDs. Such a simple view is illustrated in figure A.5.

In the simple case there is exactly one ADDMD in a country co-operating with ADDMDs in other countries to provide a directory backbone infrastructure. This ADDMD holds the country entry, and if the country is subdivided, it also holds entries representing smaller locations, like counties. It may hold entries to support particular services, such as an e-mail service. In addition, it may provide a regular service for organizations not wanting to establish their own directory services.

A PRDMD has typically an organization entry as its top entry, and its entries form a subtree that is subordinate to the part of the DIT held by the ADDMD. An organization entry can either be subordinate to the country entry, if it is a large national organization, or it can be subordinate to an entry representing a smaller area.

It should be noted that even within this somewhat simplified view of a PRDMD, users served by a PRDMD can access information in other PRDMDs without necessarily going through any ADDMD.

A PRDMD can hold more than one subtree if it is shared among several organizations.

This view of DMDs can be extended to cover the case where there are several ADDMDs in a country, where an ADDMD serves more than one country, where a PRDMD serves an international organization, where a PRDMD also performs some public services, and so on.

History

Document history		
V1.1.1	January 1998	Publication

ISBN 2-7437-1920-6
Dépôt légal : Janvier 1998