THE Open GROUP

Business Scenario:

The Directory-Enabled Enterprise

Source:	The Open Group
Status:	Issue 1
Author(s):	The Open Group Directory Program Group
Last Revision Date:	June 2000

Business Scenario

The Directory-Enabled Enterprise

Contents

Executive Summary

Directory is a powerful tool. It can provide a standard repository for data shared by operating systems and applications. It can give external organizations controlled access to selected information. It can help simplify enterprise administration and achieve massive cost savings. This all adds up to a vision – the vision of The Directory-Enabled Enterprise.

The key to realizing that vision is interoperability. Increasingly, directory servers are bundled with other products such as databases and operating systems. This, coupled with the trend to Enterprise decentralization, makes a single-supplier policy for directory procurement completely impractical. The typical enterprise will have a hundred or more directory servers from perhaps ten different vendors. Customers and vendors want the servers to work with each other, and want the enterprise's applications to work with them all.

This Business Scenario:

- Explores the business and technical environment in which directories are deployed
- Analyzes the processes in which they are used
- Identifies the human and computing actors that participate in those processes
- Summarizes the requirements, and
- Looks at the resulting technology architecture model

This Business Scenario was first published in June 2000 as Part 1 of The Open Group White Paper: Assuring Interoperability for The Directory-Enabled Enterprise (W902).

Business Scenario:

The Directory-Enabled Enterprise

What a difference a few more bucks for first-rate architecture make to everyone and everything it impacts.

Malcolm Forbes

1 Business Scenario Problem Description

1.1 Background of Scenario

This business scenario describes an idealized enterprise that is based on a number of real organizations. It does so in order to present a generic picture of the requirements for and deployment of enterprise directories.

It was produced by combining and generalizing specific scenarios for The UK National Health Service and Shell International, adding input from Kaiser Permanente and Siemens, and incorporating input and comments from members of The Open Group Directory Program, who are drawn from a wide range of directory customer and vendor organizations.

The present version is a starting point, rather than a final product. It is based on the minimum range of input that is reasonable for a generic scenario. It is intended that the Program Group will add to it, using input from other organizations who are using directory in different ways.

The UK National Health Service is the largest single health-provider organization in the world, with one million employees. Recent implementations of high-profile networks and services — in particular, *NHSnet*, a computer intranet linking major NHS organizations; *GPnet,* a computer intranet linking together all English General Practitioners (GPs); and *NHSdirect*, a telephone inquiry service that allows the general public to obtain medical advice on minor ailments without the need to consult a General Practitioner — have created a pressing need for secured, accurate, and reliable internal directory services. In addition, a recent UK Government White Paper has called for an electronic patient record to be associated with each UK citizen throughout his or her lifetime. Internal directory services are seen as an essential underpinning for such a system.

Shell International is a worldwide family of companies, with a dynamic structure. It has constantly changing relationships with a host of other individuals and organizations that are intimately involved in its business operations and are connected via an "extranet". Its business operations are centered on oil and gas, and are diversified into other areas also. Many of its activities are characterized by high-value, high-risk transactions; for example, the value of a

supertanker cargo is enormous; the risk associated with a shipwreck is environmentally massive and may not even be quantifiable in business terms.

Kaiser Permanente is America's largest not-for-profit health maintenance organization, serving eight million members in 11 states and the District of Columbia.

Siemens is one of the largest electrical engineering and electronics companies in the world. Its product range includes directory servers, and it is developing a corporate PKI directory for internal use.

The main drivers for this business scenario are desires and needs to:

- Provide higher-quality service to customers
- Improve the efficiency and effectiveness of the business processes
- Control and manage risk
- Provide public access to information, and
- Maintain security and confidentiality of information

In the cases of public access to information, and security and confidentiality of information, there are often legal requirements (such as the confidentiality requirements imposed by US health insurance act regulations).

Directory can contribute directly to higher-quality service provision, to process efficiency and effectiveness, and to public information access. Its contribution to risk control and management and to information security is an indirect one, as a component of a Public Key Infrastructure (PKI) that provides improved security.

1.2 Purpose of Scenario

This Business Scenario was produced by The Open Group Directory Program Group. The Program Group aims to help customers and suppliers realize their vision of The Directory-Enabled Enterprise. It achieves this aim by delivering understanding of requirements and assurance of interoperability for directory services and applications.

The purposes of this business scenario are:

- To communicate the Group's understanding of The Directory-Enabled Enterprise, and
- To inform the work of the Group in developing testing and certification programs to provide assurance of directory interoperability

1.3 Objectives

This business scenario supports the following specific objectives.

1. Any authorized person should be able to access contact information for any person in the enterprise, or other information to which he or she is entitled, at any time, anywhere.
2. Authorized users should be able to access services and applications at any time, anywhere, including when they are away from their normal location.
3. Authorized computers should be able to access connection information to other computers for electronic data transfer of information any time, anywhere.
4. The integrity and privacy of information being accessed or being transmitted in messages should be protected.
5. Where desired, authorship and timing of messages should be incontrovertibly verifiable.
6. Directory services should rapidly reflect permanent or temporary changes to the organization's structure.

Not all organizations have all of these objectives, and the importance given to different objectives in different organizations varies. But every organization that is, or aims to be, "directory-enabled" will have some of these objectives, and they are listed here as the key objectives of The Directory-Enabled Enterprise.

2 Views of Environments and Processes

2.1 Business Environment

Enterprises range from small, unified companies to large, complex, distributed organizations. Directories are valuable to enterprises of all kinds, but the value increases with the organization's size and complexity. The organizations on whose experience this scenario is based are generally at the upper end of the complexity scale.

The UK NHS has a complex structure. A unit of NHS organization is called a Health Community. At its core is a Health Authority. A Health Authority typically has several Hospitals, of which some will work for other Health Authorities. An NHS Trust is a hospital that may have multiple functions, and be servicing more than one Health Authority. A Health Authority may have, say, 65 Practices, each practice having up to 15 General Practitioners (GPs). There are 90-100 Health Authorities in England, 400-450 trusts, about 1,000 Primary Care Groups, about 10,000 GP practices, and about 30,000 GPs. There are also other bodies, such as central government departments, teaching hospitals, laboratories, and mental health trusts. The relationships between these bodies are many-to-many. In principle, anyone in any of them can need to find people or information in any other. NHS bodies also need to co-ordinate with

many outside bodies, such as voluntary bodies (charities), local government social services departments, and the police.

Shell is 40% UK-owned, 60% Netherlands-owned. It is domiciled in both countries. Corporate leaders live in both countries; there is no single corporate headquarters. The corporation is organized as a set of global businesses; for example, the aviation fuel business which has 200 people in various locations who rarely meet. Its shape is constantly in flux. Acquisitions and deacquisitions happen frequently. Joint ventures come together and shut down quickly. Operating agreements are made and terminated. Cross-shareholdings are formed and dissolved. Locations, organizations, and employees — there are about 100,000 employees — fluctuate rapidly.

The key organizations and entities in the business environment — particularly as relevant to the processes discussed in this scenario — are illustrated in Figure 1.

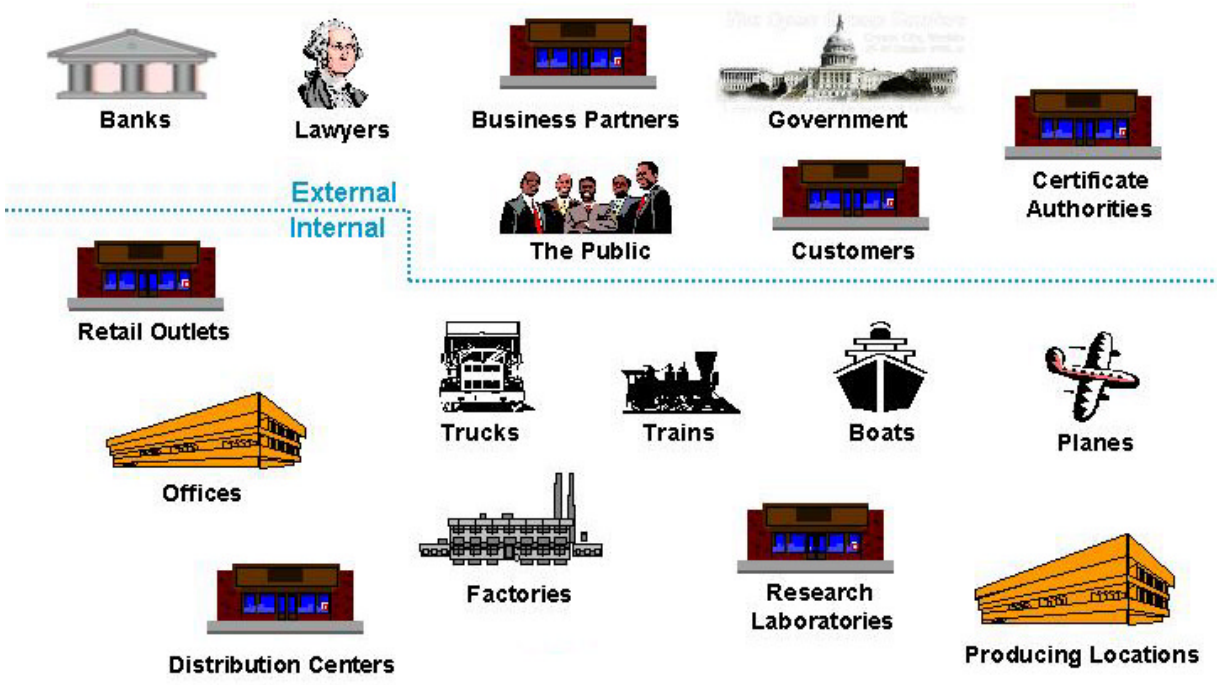

Figure 1: The Business Environment

Not all organizations will have all of these internal components and external relationships. But the figure illustrates a number of points typical of complex modern-day enterprises, each of which has particular implications for the provision of enterprise directory services.

- The organization has a number of facilities of different kinds and in different locations. These include shops, offices, warehouses, factories, and laboratories. They also include special-purpose facilities such as hospitals, oil rigs, construction sites, and police stations.
- In addition to fixed locations, an organization may have directory-users who are mobile — in trucks, trains, boats, planes, etc.
- Users can roam between different locations inside and outside the organization.
- Organizations have business relations with other organizations of various kinds, including business partners, banks, legal advisors, and government departments.
- As well as having established business relationships, an organization may interface to the general public, members of which may access its information and services, either anonymously or after establishing their identity.
- The shape of the organization and its business relationships can change dynamically.
- The distinction between those "inside" and those "outside" the organization may not be easy to draw.

2.2 Technical Environment

The key entities in the technical environment – particularly as relevant to the processes discussed in this scenario – are illustrated in Figure 2.

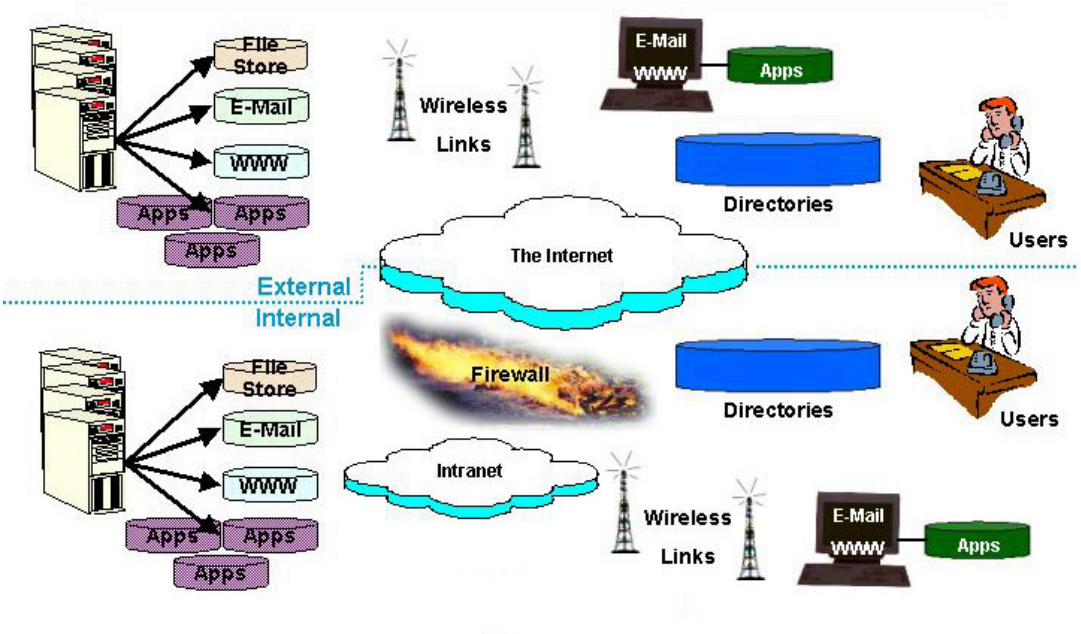

Figure 2: The Technical Environment

Host computers can be of various kinds: mainframes, minicomputers, server PCs. The operating systems that they run include:

- Proprietary mainframe and minicomputer O/Ss (MVS, VMS, AS/400, etc.)
- UNIX Operating Systems (see http://www.opengroup.org/regproducts/catalog.htm for complete lists of registered UNIX products)
- Linux
- PC Network operating systems (such as Netware), and
- MS-Windows operating systems

Some of these operating systems — notably Windows 2000, Netware, and some UNIX operating systems — incorporate Directories. These directories are a part of the operating systems' management infrastructure, but in many cases they can also be used for other purposes, including to store details of users and equipment within the organization.

Host computers are used as general-purpose filestores and databases, as mail servers, and as web servers. They also run specific applications to support activities such as:

- Personnel management

- Workflow management
- Finance
- Procurement
- Supply chain and catalog management, and
- Customer relationship management

Some of these applications make explicit use of directories, generally via the LDAP protocol.

Users access host information and applications from PCs, workstations, and terminals. They may work on the "fat client" (having major applications permanently installed) or the "thin client" (major applications are kept on the hosts and downloaded only as needed) principle.

Hosts and client computers are connected by networks. The Internet Protocol Suite is universally seen as the right choice of protocol for use both within the organization and for external communication. Proprietary protocols are still to be found but are being phased out.

It is estimated that the number of devices connected to the Internet via wireless will overtake the number with fixed connections within the next few years. Wireless connections are currently used for equipment in trucks, ships, etc. Increasingly, intelligent devices carried by the user (PDAs, WAP 'phones, etc.) will be a factor. Convenience may in time also lead to static devices being given wireless connections.

Network links vary in bandwidth. Present-day wireless links, in particular, often have low capacity. Availability of bandwidth often imposes practical limitations on communications.

Communication takes place between users, clients, and hosts both within and outside the organization. This often implies a need for enterprise directories to provide information about external users, and for external directories to provide information about users within the enterprise.

Many organizations use firewalls to filter traffic between their sites and the general Internet, and to control external access to their systems. The systems and networks running the Internet Protocol within the firewall are often called an *intranet*.

Directory systems are of various kinds. A number of organizations maintain corporate X.500 directories, which in general also have LDAP capabilities. There are specialist LDAP directory server products. There are other data storage products that support LDAP. As noted above, there are LDAP directories bundled with some operating systems. Finally, there are "metadirectory" products that provide a uniform (LDAP) directory interface to collections of directory and other data storage products.

2.3 Administrative Environment

Directory and other systems and services within an enterprise may be provided and managed by the enterprise itself, or may be outsourced.

The blurring of boundaries between organizations may lead to confusion among users about who has responsibility for administration of the systems that they are using. For example, a professor of medicine in a teaching hospital may access an NHS directory via the UK academic network, and will likely assume that his local university computing department has administrative responsibility for it.

In many organizations, systems are generally operated by people whose main job is not systems management. In some cases, they are not in an office environment with network engineers readily available to support them.

2.4 Process Descriptions

The processes that are analyzed in this scenario are:

- Information look-up
- Secure e-mail
- Access to information and applications
- Roaming
- Directory update, and
- Directory federation

2.4.1 Information Look-Up

Human users and also elements of the IT infrastructure use directories to obtain information that allows them to contact and access users and objects. In the case of a human user, this is carried out using a directory search engine, which may be part of another application (such as an e-mail client). The directory search engine accesses the directory across the network (typically via LDAP). An element of the IT infrastructure accesses the directory in the same way.

In distributed directories, the first directory that is accessed may not contain the requested information, but may obtain it from another directory. The X.500 DSP protocol is defined to support this kind of operation (known as *chaining*). Non-X.500 directories, and metadirectories, may use LDAP for this purpose.

Address look-up is typically the highest-volume application of directory in an enterprise. For example, in Shell there are tens of thousands of directory accesses per day. These are mostly

simple user look-ups, but the directory is also used increasingly by business applications to look up information. These are a mixture of off-the-shelf and house-written applications.

In a large and distributed organization, information about users may be fragmented, and ownership of it may be unclear. This makes creation and maintenance of the directory difficult, and favors a distributed rather than a centralized directory solution.

More information is needed in a typical enterprise directory than is found in conventional telephone directories; e.g., specialist skills relevant to the organization and other personal skills (such as languages spoken). The directory system will need to have some of the characteristics of an HR system.

The look-up service is often used from staff's homes as well as office locations, and by users outside as well as inside the organization.

Directories may be used to locate information, as well as people and physical objects. They can in effect play the role of index to large, distributed, and disorganized databases. For example, the UK NHS is considering their use to provide access to electronic patient records.

- Patients can turn up anywhere in the UK, and (by virtue of their medical condition) cannot necessarily communicate with medical staff. People can have medical emergencies that require fast access to patient records.
- Over 99% of the population of England is registered with some part of the NHS (this represents ~40million people).
- Each person may be registered with several different NHS locations in their place of domicile (General Practitioner, one of several hospitals, local authority).
- Existing practice is for a patient's General Practitioner to be told about every treatment applied to that patient. However, although GPs in theory have the means of keeping up-to-date records on all their patients, in practice the quality of information maintenance varies widely. Also there are no facilities in place to transfer records when a patient changes GPs.
- Patients can seek medical advice when visiting other parts of the country. There is thus a need for location and information transfer among GP computer systems.
- Smartcards are under discussion as a possible part of any solution; however:
    - Two different implementations are being considered: one where the card contains all the information, the other where it contains a pointer/URL to where the information is stored.
    - Smartcards are not necessarily acceptable politically.
- There needs to be an audit trail of who has seen, and who has changed, any patient record information.

- Only 2-3% of look-ups to patient records would be in a life-critical situation.
- Mobile access is needed also from paramedics and similar people who are mobile by the nature of their job. Also, people in transit will require access to the service. This implies access by public networks, and so validation and authorization are needed.
- Ownership of the different parts of a clinical record is a matter of debate between medical professionals.

2.4.2 Secure E-mail

The security of information being accessed or being transmitted in messages should be protected.

- *Integrity:* No messages should be altered.
- *Confidentiality:* As requested by the accessing person or machine, messages should be encrypted.
- *Digital Signature:* The parties involved should not be able to deny having received certain instructions.
- *Timestamping:* Some communications are time-critical, so need timestamping.

The requirements for integrity, digital signature, and timestamping most commonly apply to information sent in e-mail messages. The requirement for confidentiality often applies both to e-mail and to information held in filestores, databases, etc. Confidentiality of information held in filestores, databases, etc. is addressed under Access to Information and Applications.

Shell's shipping logistics management process provides a number of examples of requirements for integrity and digital signature:

- In a typical shipping movement, a trader – who buys and sells cargo – negotiates with an operator when and where a cargo will be loaded, when and where it will be discharged, and at what cost. The operator issues instructions to a ship's captain to pick up the cargo from one place and take it to another, on specified dates, sailing by a specified route, and using up a specified amount of fuel. The captain supervises loading with the ship's agent in the port, the local inspector, and the port authority.
- Negotiation and transmission of instructions is generally by e-mail. Some messages, such as inspection instructions and results, are safety-critical (it is important to know what has been inspected, where it is, and exactly what it is). Some messages involve high monetary value (for example, notifications to The Revenue that a refinery has paid duty). Integrity protection is needed for such messages.

- Mistakes in instructions to tankers on where to go or how to load can be very expensive. Disasters aside, if a tanker misses its tide, there could typically be additional port fees of $30K.
- In addition, because of the value of the cargo, and the high cost of mistakes, some messages – such as instructions to the captain to discharge the cargo – must be digitally signed.

There is money lost or potentially lost from lack of integrity, but it is often impossible to quantify how much. There are manual procedures to ensure integrity; PKI should remove the need for these, but again the savings can be hard to estimate.

Confidentiality of information is required for various reasons. It may be a matter of employee relations, as with personnel records or salary negotiations. It may be required by law. For example, confidentiality of health records and other personal information is a legal requirement in some countries. It may also be required because of the commercial value of the information.

For example, when a proposal is made to form a consortium to explore and exploit oil and gas resources, there could be a huge investment cost involved: perhaps billions of dollars spread over 20-30 years.

- It will typically be necessary to find sources of funding, find exploitation partners, seek government approvals, and negotiate terms and conditions with lawyers, governments, bankers, etc.
- Typically, there will be competition with other companies to exploit the opportunity. There have been examples of information brokers selling information on negotiating positions.
- All aspects of the negotiation require privacy (and in many cases integrity and non-repudiation also)

Timestamping may be applied as part of non-repudiation or separately. It is a case of knowing you sent it by when or knowing you received it by when, as opposed to just knowing you sent it.

The overall requirements for directory-enabled security services in those of Shell's business processes that were analyzed in the preparation of this scenario (by no means all of their business processes) are illustrated in Figure 3.

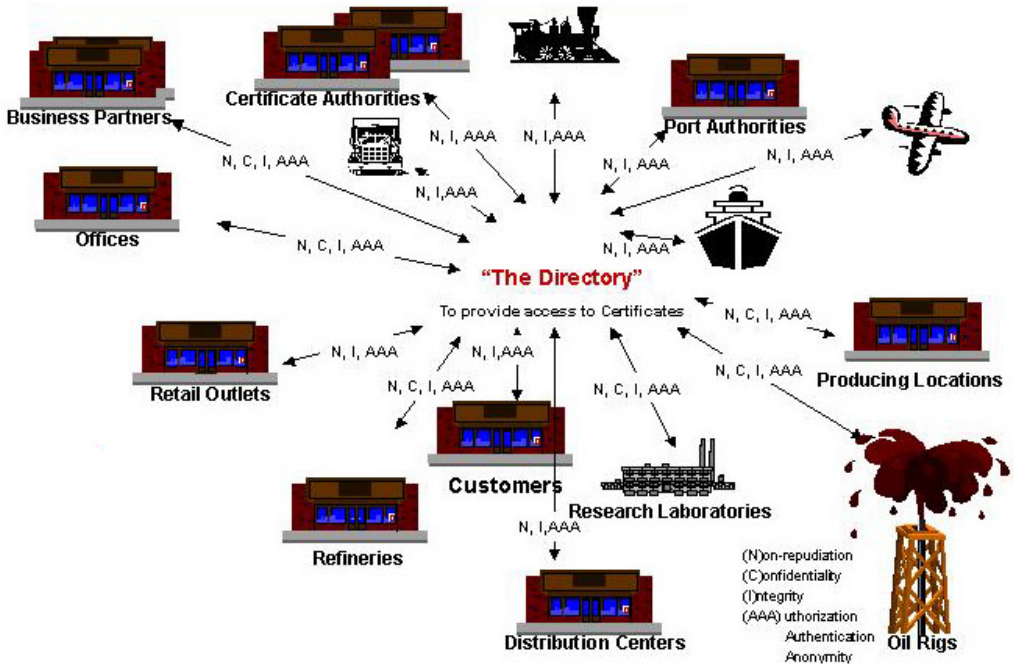

Figure 3: Shell's Requirements for Directory-Enabled Security

Integrity, confidentiality, and digital signature of e-mail can be provided by S/MIME in conjunction with a public-key encryption algorithm. With such an algorithm, a user has a pair of keys: one public, the other private. Information encoded using the public key cannot be decoded using that same public key but can be decoded using the private key. And information encoded using the private key cannot be decoded using that same private key but can be decoded using the public key.

For integrity checking and digital signature, the sender's e-mail client adds to the message information that has been encoded using the sender's private key. The recipient's e-mail client decodes this information using the sender's public key.

For confidentiality, the sender's e-mail client encodes the message using the recipient's public key. The recipient's e-mail client decodes it using the recipient's private key.

There are various ways in which the recipient can obtain the sender's public key and the sender can obtain the recipient's public key. Public keys need not be kept secret. They can be sent by e-mail. They can be stored in public databases. Often, they are stored in directories, together with other information about their owners.

Obtaining a public key is one thing, trusting it is another. So that their trustworthiness can be verified, public keys are generally made available in *certificates*. A certificate is issued by a *Certificate Authority* (CA) and certifies the ownership of a public key. It is digitally signed by the CA, using the CA's private key. The signature on the certificate can be checked using the CA's public key. If the verifying user does not have or trust the CA's public key, it can obtain another certificate containing the CA's public key, and signed by another CA. In fact, it can obtain a chain of certificates, each verifying the public key of the preceding one. If the chain ends with a CA that the user trusts, the user can also trust the public key at the start of the chain. The certificates that a user needs to build a chain verifying a public key are often stored in directories – in particular, in directories maintained by the CAs concerned.

A CA can revoke a certificate that it has issued. One way in which CAs publish the fact that they have revoked a certificate is to put it in a *Certificate Revocation List* (CRL) stored in a directory. A user verifying a certificate needs to verify not only that it was validly issued, but also that it has not been revoked.

The process of sending and receiving secure e-mail may thus involve searching directories for certificates and CRLs. In theory, such searches should be performed by the e-mail clients. In practice, the user may have to perform much of the verification process manually.

The use of directories to store certificates and CRLs for PKI is described in more detail in Appendix A.

2.4.3 Access to Information and Applications

When users access information and applications across a network – especially when that network is the public Internet – there are often requirements to:

- Authenticate those requesting access
- Ensure that only authorized users can have access, and
- Preserve the integrity and confidentiality of the information as it crosses the network

For example, Shell publishes specifications of all their products. Some are commodity products, some are speciality products. Associated with each product is a set of materials safety data sheets covering what to do, what not to do, what to do if you do something wrong, etc. Some products have unique characteristics, and Shell may therefore need to implement controlled access to certain parts of the information. The community that has access may or may not be known in advance. For example, they may let ICI see some information but not Exxon, BP but not Elf, etc. Granularity can be important.

Shell Cards provide another example. There are four million Shell Cards. Most belong to road transport fleets. The client businesses give them to their drivers. The drivers can go anywhere in Europe, fill up with fuel, and the client gets a bill at the end of each month. Some fleets have sophisticated control systems, some have none. All clients want to know how to administer the

cards, and how to find out what the bills will be. Shell has built a web-based system that gives the clients the information relating to their cards and the use made of them. There is a need to authenticate access to particular records.

Health records provide a further example of information to which access must be carefully restricted to a few authorized people. Here, confidentiality can be a legal requirement, and information accessed across a network must often be protected from snooping.

When the user authenticates (via smartcard, or whatever), his environment should be enabled for him, and he should be denied access to everything else. It is necessary to manage the user as a person and also as the filler of a number of roles. A person may fill several roles at the same time.

Specific authentication needs are:

- Single sign-on – no-one likes to have to enter multiple passwords, especially when they are different
- Platform-independence
- Rights management and dynamic resource management — basically ACLs and *good* ACLs, and
- International operation of CAs and RAs

Increasingly, the web is the method of choice for providing access to information. The principles are, however, the same when information is accessed in other ways, such as by client parts of client-server applications, by file transfer, or by "dumb" terminals (or PCs acting as such).

The most common way of authenticating users is probably still by use of passwords. However, transmitting these "in clear" across the Internet is insecure.

The most common way of providing confidentiality is use of the Secure Sockets Layer (SSL) protocol over TCP. With the web, this is generally invoked by the client requesting a URL with the https (rather than http) protocol.

Usually, this leads to a connection that is secured by the server's public/private key pair, and the public key is sent to the client in a certificate. The client can verify this certificate by establishing a trust chain. In practice, such verification generally requires all certificates in the chain to be already stored in the client, and revocation of them is not checked, although in theory a client could search directories for certificates and CRLs needed to establish the chain.

SSL contains provision for the client to provide a certificate to the server. In practice, this is rarely implemented. However, establishment of a connection secured by the server's public/private key pair does make it safe for the client to transmit a password for authentication.

The use of directories to store certificates and CRLs for PKI is described in outline in Secure E-mail, and is described in more detail in Appendix A.

2.4.4 Roaming

When a user is away from his or her normal location, and the resources are available in the location where the user is, he or she should be able to use them there, without connecting back to the normal location.

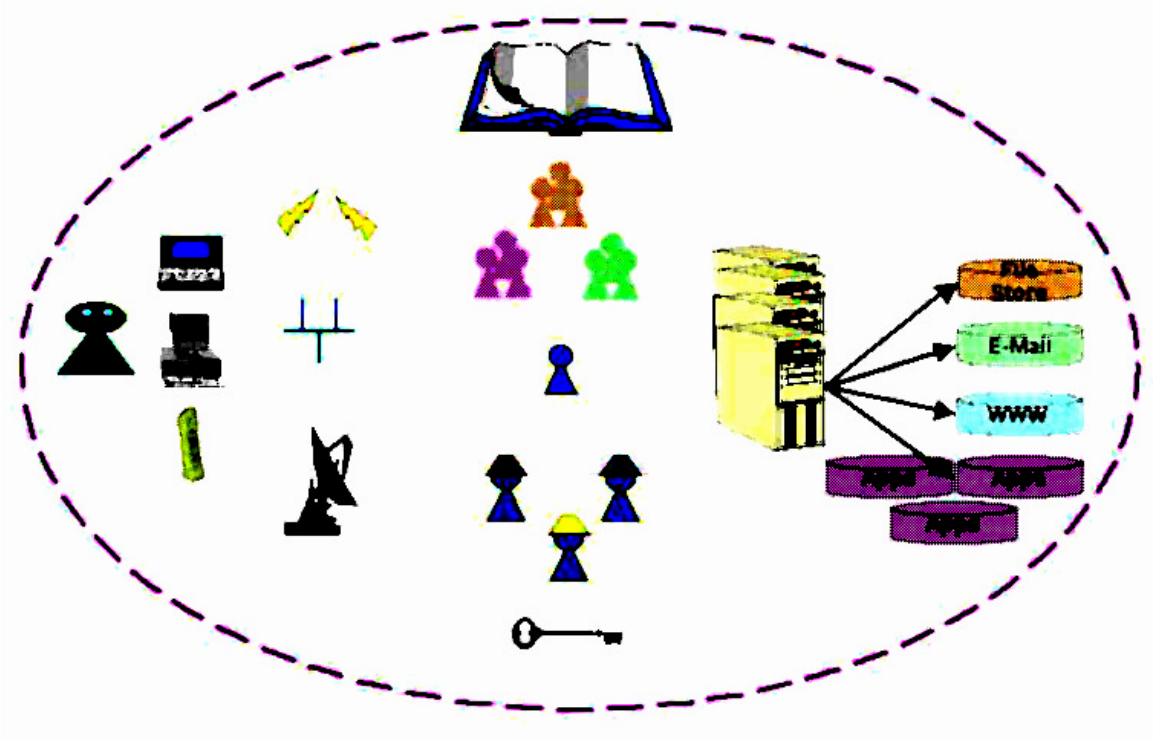

Figure 4: A Local Environment

What services he can use, and how he can use them, may depend on:

- Whether he is using a laptop, workstation, PDA, or other kind of terminal device
- What kind of link he is connected by: it could, for example, be wireless, 10 MBps LAN, or satellite; it could be symmetric or asymmetric
- What roles he is filling
- What his personal attributes are, and
- What groups he is a member of, and what they allow and enable him to do

Figure 5 illustrates the information that may be required for correct service provision.

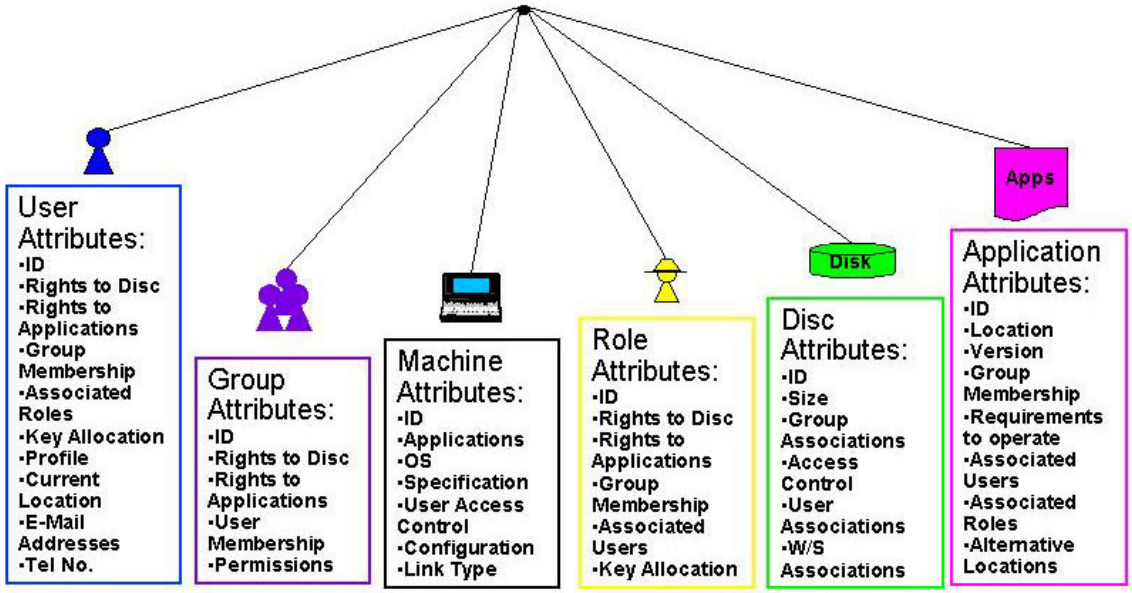

Figure 5: Environment Information

Providing services involves:

- Giving the user access to his filestore (wherever it is)
- Identifying the nearest mail service, web server, and other applications that can support him and that he can use, and
- Determining whether his workstation has the capability of running those applications on his data and, if not, finding alternative means of delivering the capability.

In addition to providing the user with service, it may be desirable to inform other users of his location.

Having established the user within the environment he is visiting, he must be enabled to communicate with other users and access services in other environments. He has authenticated himself within one island; that must be propagated to others.

2.4.5 Directory Update

The volume of changes to a corporate directory may be substantial. For example, currently there are about 5,000 changes per week to Shell's central directory. These could be to a person name, company name, departmental name, location, and so on. Central administration of this information can be expensive. An alternative (which Shell have adopted) is to put as much of

the maintenance as possible in the hands of the users. This implies assigning ownership of particular entries to particular users, and giving them update capabilities.

However, assigning ownership is not always easy. For example, in the NHS, each Health Authority is typically supported by a single HR function, but that function might be supporting several Health Authorities. Such an HR function would own the information about the staff in the Health Authority offices only (i.e., not the staff in hospitals and trusts in the same Health Community), but it would also have information on all the GPs/Primary Care Groups for which it was responsible. Trusts (hospitals, community trusts, and mental health trusts) have their own HR departments. Trusts mostly own staff information for ordinary Laboratories, while the Department of Health owns it for the Public Health Laboratory Service.

Updates are typically carried out using LDAP (operations add, delete, modify, and modify DN). Bulk updates may be carried out by loading files in LDIF format.

In a distributed directory, updates must often be propagated from one server to another. The X.500 DISP protocol and the (currently being defined) IETF LDUP protocol provide for this.

2.4.6 Directory Federation

Groups from different organizations have a need to work together. Their infrastructures are joined by a WAN and are federated – data-live and sharing basic services.

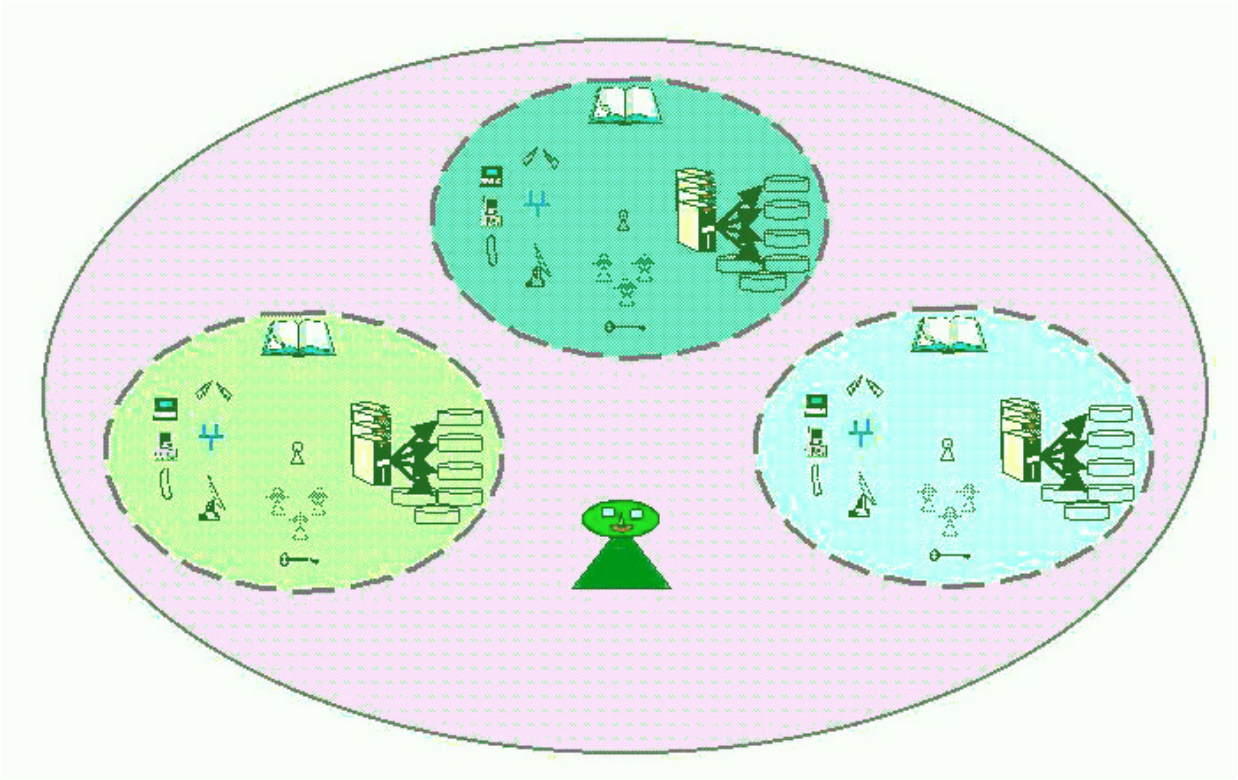

Figure 6: Federation

An example is provided by the formation of a consortium to explore and exploit oil and gas resources, mentioned above. The links between the directories concerned may need to be established quickly. The process of linking the directories should be reversible and non-destructive.

Federation requirements are:

- Plug and play – seven days is too long to get people talking to each other; 72 hours is pushing it
- Information available when systems federated should be improved
- Common standards-based interfaces, and
- Reversibility (most important) — federation must be reversible and non-destructive — if legacy systems are pulled in, it must be possible to pull them back out

3 Actors and Their Roles and Responsibilities

3.1 Human Actors and Roles

Human Actors	Roles
User	• Looks up addresses and other information about people and other entities, either using a directory search engine or using an application (such as an e-mail client) that interrogates the directory • Creates, secures, and sends e-mail messages • Receives e-mail messages • Obtains other users' certificates from the directory for secure messaging • Looks up certificates and CRLs in order to verify other users' certificates for secure messaging • Accesses information • Uses services and applications • Looks up certificates and CRLs in order to verify server's certificate • Roams to different local environments • Adds, modifies, and deletes "own" directory entries
Administrator	• Configures directory schema, etc. • Adds, modifies, and deletes entries • Defines directory access control • Configures replication between directories • Configures referrals, chaining, replication, and other server-server communication mechanisms to federate directories

3.2 Computer Actors and Roles

Computer Actors	Roles
Mainframe	• Scientific and business computing
Internet/Intranet/ Extranet	• Connects computing elements
Wireless Links	• Connects mobile (and some fixed) computing elements to Internet/intranet/extranet
Workstation/Desktop/ Portable Computer	• Hosts client applications • Provides user access
Thin Client	• Provides user access

Computer Actors	Roles
Firewall	• Filters traffic between Internet and intranet • Accesses directory for PKI
E-mail Client	• User access to messaging • Looks up certificates and CRLs for secure messaging
Web Client	• User access to information • Looks up certificates and CRLs for secure access
Client/Server Applications	• User access to information • Looks up certificates and CRLs for secure access • Looks up information about people and other entities in the directory • Publishes certificates
Directory (Internal and/or External)	• Contains information about users and other entities • Contains certificates and certificate revocation lists (CRLs) used by the PKI
CA (Internal and/or External)	• Creates certificates (both for users and for CAs) • Creates CRLs • Stores certificates and CRLs in the directory • Updates and manages certificates and CRLs in the directory
Tools	• Information and systems management

4 Requirements

4.1 Directory Requirements

Capacity

The following parameters are important:

- *Volume:* Currently, the highest-volume application of directory is probably White Pages — simple address look-up. There is currently little use of PKI information in the directory — but there will be very high-volume use when PKI is used for log-on authentication to services.
- *Growth Rates:* Some organizations require scalability to support tens or even hundreds of millions of records at a reasonable cost.
- *Headroom:* What will be the next barrier to prevent growth? In general it is not possible to control the rate at which traffic will grow (for example, if an organization changes its name

overnight, there will be thousands of extra look-ups). So there is a need for burst capability, and capacity to cope with the unexpected.

Response Time

For human users, using the directory must be quicker than picking up the 'phone and asking the operator. This places an absolute limit of about five seconds, regardless of load. Sub-second response is desirable for most operations; longer is tolerable where encryption is involved. Some time-of-day differences may be tolerable.

For some uses by the IT infrastructure and applications, response times should be measured in milliseconds.

Accuracy

100% accuracy of information returned is required.

In a distributed directory, it may take time for an update entered at one point to be propagated throughout the directory. Time of update propagation should be no more than overnight.

Availability

Any authorized person should be able to access addresses, or other information that they are entitled to access, at any time, anywhere. Authorized computers should be able to access connection information to other computers for electronic data transfer of information any time, anywhere.

Many organizations require their directories to be available 24 hours a day, seven days a week, 365 days a year.

Some organizations require business continuity "even if the San Andreas fault opens".

Prioritization

Prioritization of applications and of requests may be required.

Cost

Should be low; less than five cents per access as a maximum for White Pages look-up.

There may sometimes be an internal or external charge, and a need for accounting capabilities.

Ease-of-Use

Directories and directory-enabled applications are generally used by non-technical people, and must be easy-to-use.

For example, the Shell Card system had to be designed for use by administrative personnel without technical backgrounds. Such people were in fact able successfully to order cards, change cards, calculate vehicle fuel consumption, etc. for the fleets they administered. The ease-of-use principle is now enshrined by Shell for all extranet applications.

Schema

Co-ordination between different organizations implies a need for common schema and policy object definitions.

Most organizations use off-the-shelf products. Some of these can use directory – but with special schema. A common set of schema attributes is needed at the leaf level if they are to be integrated with other directory applications.

External Communications

Many of the needs for directory are for internal communications, but more and more are for communications with outside bodies. For example, in Shell, tanker instructions may need to be delivered to shipping agents. The trend is for more change and for more interaction with third parties.

Internationalization

The standards are written by westerners, and have specific ways of expressing names, etc. They do not fit the Dutch, and a number of near and far eastern cultures. For example, far eastern staff have two names: a real Chinese name, and a westernized Chinese name.

There is a need for schemas that can be used across the organization, by Cas, and by business partners.

Manageability

The following aspects are important.

- *Fault-Tolerance:* Systems should be fault-tolerant.
- *Self-Diagnostics:* Should be built-in.
- *System Messages:* Must be understandable by the recipient.
- *Changes:* There must be ability to cope with changes and preserve integrity.
- *Test System:* It must be possible to have one.

4.2 PKI Requirements

This section describes some general requirements relating to and issues with PKI. A detailed description of how directories are used to store certificate information for PKI, and of some of the problems that can arise, may be found in Appendix A.

What now seems the likely development of PKI is different from what seemed likely two or three years ago. CA services will be adopted, but there are three sets of problems:

1. There is a wide variety of potential legislation surrounding digital signatures – governmental and "super-governmental".
2. There are problems with interoperability at a policy and at a technical level.
3. Working with multiple partners will present problems.

An example of legislative problems is that Malaysian legislation requires use of a Malaysian CA when using digital signatures in Malaysia.

A large organization may operate across many different legal systems. For example, Shell has particular preferences for laws under which contracts are made – UK, Netherlands, US – but that causes problems in other countries.

Industry initiatives may imply particular methods of working. An organization is likely to be a customer of and supplier to partners who participate in different initiatives.

Relationships, for example with banks, cannot be avoided. And there will be a need to deal with multiple certificate authorities. But no organization is big enough to determine the form of the relationships with all its partners. As soon as there is more than one partner, there are interoperability conflicts and policy conflicts.

For example, many different smartcards are needed to interoperate with different banks. A treasury clerk will have great problems with this.

These considerations lead to the following requirements.

Liability

Public services should carry some liability for certificate misuse.

There are concerns with CA organizations because they have different policies in different countries. Who do you sue when things go wrong? With Globalsign, for example, sometimes it is Globalsign that has liability, but in some countries it is their partners.

Policy Manageability

Each user organization needs to manage, control, and execute a policy relating to the issue of the liability that a certificate carries. Applications could then allow events, access, etc., in the

light of current information and a particular policy. It would help if the directory contained information that would enable applications to understand when a certificate can and cannot be used.

For example, how will BT authenticate someone in Venezuela? It does not have a big presence there. Will it just carry that as a business risk? How should an application behave when presented with a BT certificate for a Venezuelan resident?

Some CA policies say "Our certificate is only valid in country X". An international organization cannot use such certificates. And what if two companies want to do business but there are policy conflicts between their CAs? Is there a "Super-CA", and if so can it resolve these conflicts? Because of these problems, a user or entity may need several certificates – which must be stored in the directory.

Consistency Across CA Consortia

Two customers may have relationships with different members of a consortium — but those members' policies may vary. Who manages the conflict?

For example, there is no single CA that matches Shell's presence across the globe. One user or thing may need to have multiple certificates associated with it. These issues are going to complicate the lives of all multi-country organizations.

5 Technology Architecture Model

5.1 Constraints

There are generally constraints on the definition of any technology architecture. Those applying to enterprise eirectory include:

- *Quality*
- *Cost*; for example, the NHS directory could be funded by the government Treasury department, which has limited funding and strict rules
- *Legislation*; for example, data privacy legislation
- *Interworking*; the need to work with particular existing or planned elements of the enterprise's IT infrastructure
- *Corporate IT Rules and Policies*; for example, Shell has a group communication policy, and has other rules that relate to the directory, including that:
  - There will be a single e-mail system.
  - Everyone will appear in the directory.
  - Everyone will have access to the web.

- Individuals are responsible for protecting company assets — physical and information assets, etc.
- Individuals are accountable for maintenance of their own information.

5.2 IT Principles

Solutions must be based on standards — which can be international, imposed, or market-driven.

5.3 Technology Architecture Supporting the Process

This section does not attempt to define a standard technology architecture for the enterprise directory. In the first place, the requirements are only partially understood. There are several aspects – such as use of the directory to store information about the enterprise IT infrastructure – that this version of the scenario does not address. In the second place, even if the requirements were understood completely, circumstances differ so widely between different enterprises that it is unlikely that a single architecture could suit them all.

What this section does attempt to do is to outline the concept of the distributed directory, and to describe some of the implementation considerations that arose in the discussions with the organizations that have contributed to this scenario.

5.3.1 The Distributed Directory Concept

Most large organizations have many directory servers. (An oft-quoted statistic is that the average Fortune-100 corporation has 181.) Ideally, these servers act collectively as a single, distributed information store. This store is part of a larger store that includes information held on servers belonging to external organizations also.

The original concept of the X.500 Directory was that there is just one, global directory, which all the world's directory servers co-operate to provide. This concept is still preserved to some extent in present-day directories.

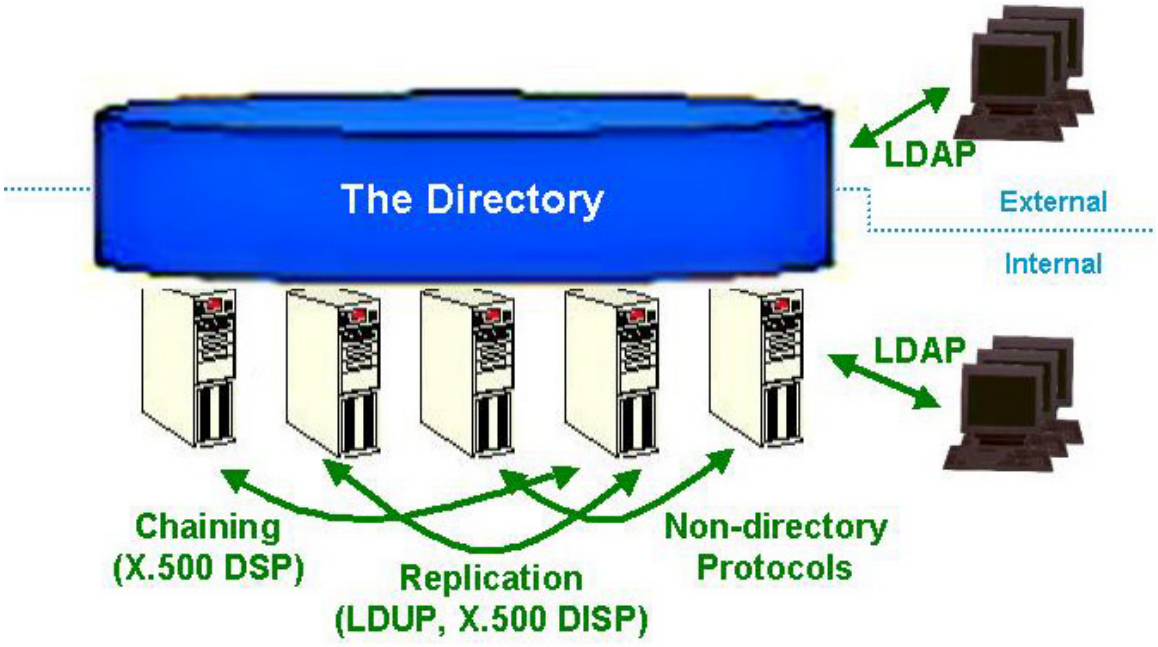

Figure 7: The Distributed Directory Concept

The servers co-operate by:

- *Referrals and Continuation References:* When a server to which a request is made does not have all of the requested information, it may return a *referral* to another server to which the entire request should be directed, or return part of the information together with a *continuation reference* to another server that can provide the rest.
- *Chaining:* When a server to which a request is made does not have all of the requested information, it may obtain some of it from another server.
- *Replication:* Information on one server can be copied to others. A particular case of this is *synchronization* of a smaller directory (for example, on a PDA) with a larger one.

The ITU X.500 Recommendations define a Directory Access Protocol (the DAP). This has largely been displaced by LDAP for client access to directories over the Internet. The X.500 Recommendations also define protocols for chaining and replication. The IETF has defined the LDAP protocol for directory access, and is working on protocols for replication and synchronization. LDAP can also be used for a form of chaining. Enterprise directories include X.500 Directory products (most of which also support LDAP), non-X.500 Directory products supporting LDAP, directories bundled with operating systems and other products, data stores

supporting a variety of non-directory protocols, and metadirectories that provide an integrated directory view of disparate storage components.

5.3.2 NHS Implementation Considerations

The following figure depicts a possible technology view of the architecture of the directory service for the NHS.

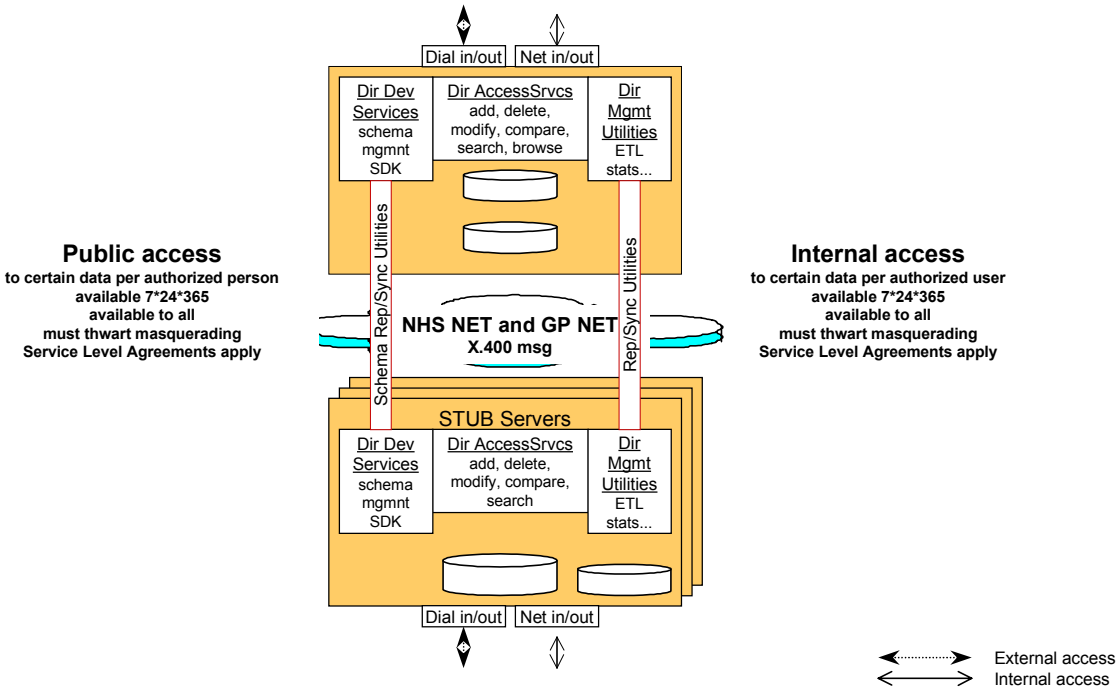

Figure 8: Possible Technology View of NHS Directory Service

Central Server Side

The central server is the record of reference for directory information. It is primarily comprised of the following components:

- Directory Access Services
- Directory Store
- Directory Audit Log
- Directory Management Utilities
- Directory Development Services and Tools

The central service is likely to be implemented by X.500 directories. It may be outsourced to a service provider.

Stub Servers Side

Stub servers surround the central store and are the first place people will look for information. Though the directory entries are not the record of reference, they do serve the business by providing local directory information that is in synchronization with the record of reference. The synchronization can be set up to support the business needs. For example, if it is critical that directory information be accurate in a real-time sense, one may either always go to the record of reference or set up the local directory with a very sensitive synchronization time.

Stub servers are optional. However, if they are used they are primarily comprised of the following components:

- Directory Access Services
- Directory Store
- Directory Audit Log
- Directory Management Utilities
- Directory Development Services and Tools (optional)

Client/Requester Side

The client or requester side has the input and output interfaces. These are assumed to be APIs and/or applications with human interfaces that use the APIs to fulfill a human-generated request.

5.3.3 Shell Implementation Considerations

The role of directory in Shell's planned technical architecture is illustrated in Figure 9.

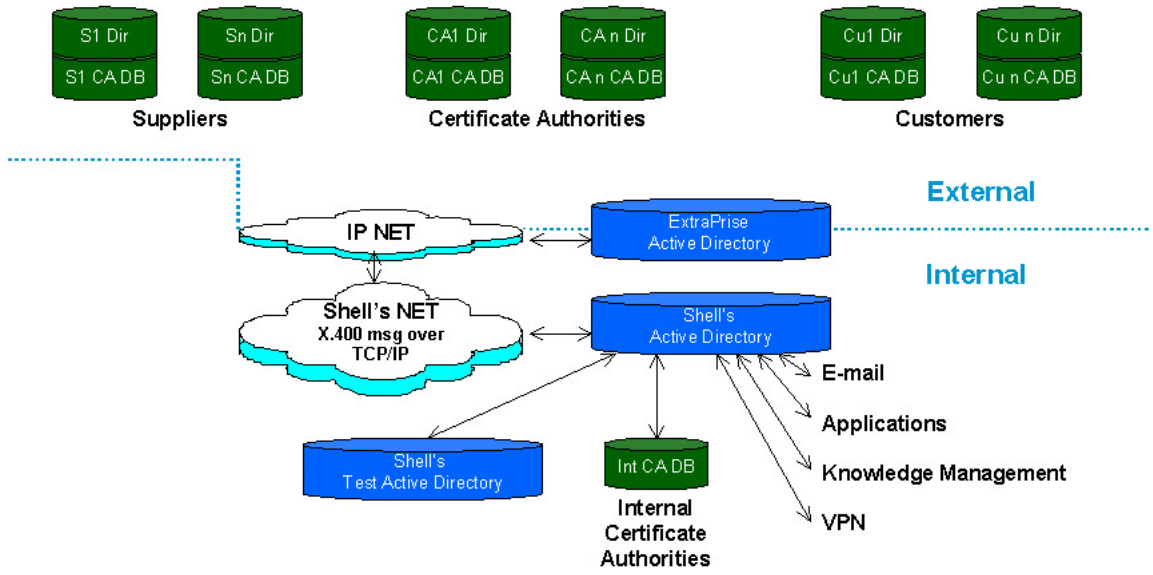

Figure 9: Shell's Planned Directory Architecture

Shell has moved from closed networks to using open networks that they will selectively close. This will be implemented using PKI supported by directory. Shell wants to move away from user IDs and ACLs to Certificate Services to authenticate individuals and generate rights to access the systems.

Some of the directory information will be shared with external organizations. This information will be conceptually – and probably physically – stored in an "Extraprise" directory separate from the main corporate directory. But at present this is not done for certificate information, which is retrieved directly from certificate providers' directories.

It is not yet entirely clear how to implement the directory services. Perhaps an independent global metadirectory service provider could play a role. Shell would have to tell them the maximum number of accesses, retrievals, etc. Customer and supplier administrators will need to maintain parts of the directory information. Shell has an existing corporate X.500 Directory, but has now taken an implementation decision to use Active Directory for their directory systems.

Shell will be storing X.509 certificates associated with user records. These will certify things — including mailboxes, function or role-based, that may represent a process — as well as people.

There will be an internal CA for issuing logon authentications and certificates for business partners. Shell is producing policies and procedures for smartcards and certificates.

The Extranet directory will be populated partly with Shell information for external dissemination, and partly external information for Shell dissemination. In particular, external CAs will access the Extranet Active Directory. One concern is replication: at this moment, if you change the value of a field in a schema, that complete record is input to the replication process. Customer and suppliers might well be asked to maintain their own entries in the Extranet directory.

Figure 10 shows the directory components in more detail.

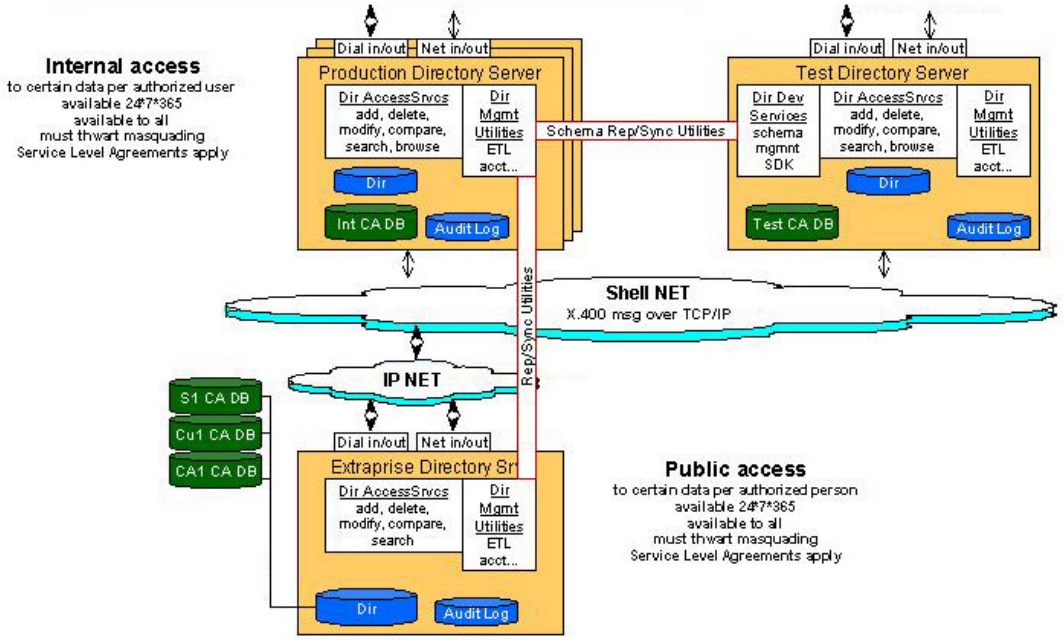

Figure 10: Shell's Planned Directory Architecture – Detail

5.3.4 Kaiser Permanente Implementation Considerations

The directory employs a "Hub and Spoke" model. There is a corporate metadirectory with distributed repositories and DBMSs. The hub may need to interface to any kind of repository, including (for example) repositories that support the HL7 messaging protocol, and flat files.

Appendix A: Certificates and the Corporate PKI Directory

Introduction

This Appendix describes how certificate information is held in a directory for a corporate PKI, and identifies some of the problems that can occur.

A PKI Directory

Definition of the Repository

PKIX definition in IETF RFC 2459: A system or collection of distributed systems that stores certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities.

(Note that the official wording is *repository* and not *directory*; a repository can be a directory, but can also use other technologies.)

- *CRL:* Certificate Revocation List (a list of revoked certificates).
- *End Entity:* User of PKI certificates or end-user/system that is the subject of a certificate.

Information Stored in the Repository

Two kinds of information will be stored in the repository:

1. Certificates
2. Information about revocation of certificates, which means a list or certificates which are no longer valid for several reasons.

It is very important to see clearly:

- Who/which instance creates/updates this information
- With whom/which instance this information is associated or to whom/which instance this information "belongs", and
- Who/which instance reads and uses this information

Instances and Roles

In order to understand this better, we will extract the three important instances of a PKI which are relevant for the simplest scenario:

1. The CA, certificate authority

2. One end entity — who we will call Bob, for whom the CA creates a certificate, and
3. Another end entity — Alice, who wants to use Bob's certificate for her secure communication with Bob

Note : The simplest scenario involves only one CA. A complete scenario should involve several CAs which work together (cross-certification).

Basically the roles are:

- Bob wants to have a certificate and expresses this request.
- Only the CA creates the certificate.
- Only the CA also updates the certificate, if necessary.
- Only the CA creates and updates CRLs.
- Alice only retrieves the certificate and revocation information in order to validate the certificate when she wants to communicate securely with Bob. She will need some means in order to find the right certificate and the complete revocation information which is necessary for validation.

Ownership of Information

How is the information associated with the PKI instances and stored in the repository? Basically, several objects are defined in the repository and the information to store is considered as a property of the object:

- Bob's certificate is associated with the object Bob.
- Revocation information is associated with the object CA.
- The CA itself needs to have its own certificate; this *CA certificate* is also associated with the object CA.

The Directory Schema

If the repository is a directory, the directory concepts of *Entry* and *Attributes* can be used. The following entries will be used in the directory:

- The CA´s entry, and
- Bob´s entry

The information associated with these objects will be mapped to attributes of these entries:

- Bob´s entry will have the attribute "Certificate".

- The CA´s entry will need the attributes "Certificate Revocation List" and "Certificate".

Now the directory has additionally the concept of *object class.* An object class allows control over which attributes can be placed in which entries.

All objects belonging to the same object class have the same characteristics. The definition of an object class prescribes which attributes are allowed for an entry if this entry has just that object class:

- Some attributes are *mandatory*, which means that they have to be present if an entry has this object class.
- Other attributes are *optional*, which means that they are allowed for the entry, but need not always be present.
- Attributes that are not contained in the definition of the object class are not allowed in the entry.

Every entry has one or more object classes.

All these means of controlling the information in the directory, including additional aspects such as syntax of attributes, are collectively called *directory schema*.

This is not only a characteristic of directories. All good databases have schema: this is the set of rules that control all aspects of what can be put into the database.

When an entry has to be created or modified, the server will check if the request for creating/modifying the entry is compliant with the rules of the schema in force.

And all good databases will reject requests that are not compliant with the defined schema.

Schema Problems

Problems arise because:

- The directory server is not administered correctly and does not support the necessary schema elements.
- Some PKI implementations do not understand the X.500 schema concept.
- Some LDAP servers have too few or no schema control at all.
- The schema defined for PKI in the second (1993) and third edition (1997) of X.500 was too inflexible and made too much use of mandatory attributes.

Handling of Certificates

Schema Elements for Certificates

Note: The schema information contained in this illustration is not complete; it is limited to the needs of the scenario and its comprehension.

Schema Elements in Second and Third Edition of X.500 (X.520, X.521)

For Bob's entry:

```
Object class Strong Authentication User
    Mandatory attribute: User Certificate
Attribute: User Certificate with Syntax Certificate, attribute is
           multi-valued
```

For the CA's entry:

```
Object class Certification Authority
    Mandatory attributes: CA certificate
                          Certificate Revocation List
    Optional attribute:   Cross certificate pair (not discussed here)
Attribute: CA Certificate with Syntax Certificate, attribute is
           multi-valued
```

Schema Elements in Fourth Edition 2000 of X.500

For Bob's entry:

```
Object class Strong Authentication User is obsolete
Object class PKI User
    Optional attribute : User Certificate
Attribute: User Certificate with Syntax Certificate, attribute is
           multi-valued
```

For the CA's entry:

```
Object class Certification Authority is obsolete
Object class PKI CA
    Optional attributes: CA certificate
                         Certificate Revocation List
                         Cross certificate pair (not discussed here)
Attribute: CA Certificate with Syntax Certificate, attribute is
           multi-valued
```

Schema Elements in PKIX Documents

In IETF RFC 2587: Internet X.509 Public Key Infrastructure - LDAP V2 Schema, only the object classes defined in the fourth edition, PKI User and PKI CA, are used.

Schema Elements Actually Used in PKI Implementations

The latest integration tests with several PKI implementations showed that the schema elements defined in the second and third edition of X.500 are still used. This caused several problems. Using the new object classes PKI User and PKI CA, which only have optional attributes, will considerably reduce these problems.

What the Directory Administrator Has To Do

The schema elements used by the PKI implementation have to be supported and administered in the directory server that is used.

Normally a directory product is delivered such that every DSA already supports a number of standard schema elements and such that the directory administrator disposes of tools allowing him to extend the schema.

Before running the PKI application, the administrator has to make sure that the necessary schema elements are available in the directory server.

If it is not the case, the server will normally not allow him to add the certificate attribute to an entry.

What the CA Does

After having created a certificate for a user or for the CA itself, the CA will want to publish this certificate. This means that the CA will try to add the attribute "user certificate" or "CA certificate" to the corresponding entry. It will first try to find if this entry exists, and then behave differently if the entry exists or not.

The operational protocol recommended by PKIX with a directory is LDAP. Nevertheless it is possible to use the X.500 DAP, and some PKI implementers support both protocols. In both cases the strategy is the same.

Searching an Existing Entry

The CA will use the directory operation "search" to see if the entry exists.

The search request normally contains a base object, often the root of the tree where the entry should be, and a filter containing characteristics of this entry. This is normally the value of one or more existing attributes of this entry; for instance, the e-mail address.

Note: The behavior of the CA could be different for a user or for its own CA entry.

Entry Exists

If the entry exists, then the CA will use the directory operation "modify entry" to add the attribute "certificate" to the entry, or add a value to this attribute if it already exists.

If the attribute already exists, the steps are the same for the old and the new object classes.

If the attribute does not exist, adding this attribute has to be done in different ways, due to the fact that the old object classes have mandatory attributes.

Use of object classes "Strong Authentication User" and "Certification Authority" with their mandatory attributes.

If it is Bob's entry, a user entry, and the entry has no attribute "User certificate", then this operation must simultaneously:

- Add the object class "strong authentication user", and
- Add the attribute "user certificate" with a valid value

It is *not* possible to use two separate operations to perform these steps.

If it is the CA's entry, and the entry has no attribute "CA certificate", then this operation must simultaneously:

- Add the object class "strong authentication user", and
- Add the attributes "CA certificate" and "Certificate Revocation List", each with a valid value. (The value for the Certificate Revocation List can be empty.)

It is *not* possible to use separate operations to perform these steps.

Use of object classes "PKI User" and "PKI CA" with their optional attributes.

In this case, due to the absence of mandatory attributes, there are several possibilities for performing the necessary steps.

If it is Bob's entry, a user entry, and the entry has no attribute "User certificate", then this operation can simultaneously:

- Add the object class "strong authentication user", and
- Add the attribute "User certificate" with a valid value

It is also possible to use two separate operations to perform both steps.

If it is the CA's entry, and the entry has no attribute "CA certificate", then this operation can simultaneously:

- Add the object class "strong authentication user", and
- Add the attributes "CA certificate" and "Certificate Revocation List", each with a valid value. (The value for the Certificate Revocation List can be empty.)

It is also possible to use separate operations to perform these steps.

Entry Does Not Exist

If the entry does not exist, then the CA has to use the directory operation "add entry" to create this new entry.

In this case the handling of mandatory attributes has to be done the same way as for the "modify entry" operation: object class and mandatory attributes have to be contained in the "add entry" operation.

In addition, the name of the entry has to be clear to the CA, and the form of the name has to be allowed by the server.

Problems that Can Occur

Schema Elements are Not Available in Server

In this case, the server will reject every "add" or "modify entry" operation.

Adding an Attribute Without Having Added the Object Class

When the new object classes are used, it is possible to add the object class and the attributes in several steps. But the object class has to be added before the attributes. If it is not the case, the attribute is not allowed for this entry and the server will reject the request.

Note: The X.500 "content rules" mechanism allows another way of administration here, but is not recommended.

Handling of Mandatory Attributes

If the steps described under *Use of object classes "Strong Authentication User" and "Certification Authority" with their mandatory attributes* are not done exactly as defined, the server will reject the request with an error such as "object class violation".

Name Form Not Allowed

The directory administrator has always to define the structure of the tree. One part of this is which components may be used in order to build the name of an entry. If the CA does not use a correct name in the "add entry" operation, the server will reject the operation with an error such as "naming violation".

CA has Insufficient Access Rights

All directory servers have ways to administer access control rights to the information contained in the database. X.500 has its own complete access control concept.

In order to be able to perform "add" or "modify entry" operations, the administrator must give the CA the corresponding rights. The CA has then to bind to the server with the corresponding credentials to make sure that it gets the necessary rights.

If the CA does not have the rights, an "add" or a "modify" operation will be rejected with an error such as "insufficient access rights".

Adding Several Certificates to an Entry

If the entry has already one certificate attribute, the CA should have the possibility to add a new value to this attribute. Two problems could then arise:

1. *Administration Error*: The attribute is administered as a single-valued attribute and not as a multi-valued attribute.
   In this case the server will reject the request with an error such as "constraint violation".
2. *Application Error*: The CA uses with the "modify entry" operation the functionality "add attribute" and not the functionality "add value".
   In this case the server will reject the request with an error such as "attribute already exists".

Appendix B: Glossary

ACL	Access Control List
API	Application Program Interface
BLITS	Basic LDAP Interoperability Test Suite
CA	Certificate Authority (in a *PKI*)
Chaining	A mode of interaction that may be used by a directory server that cannot perform an operation itself. The server chains by invoking an operation of another server and relaying the outcome to the original requestor.
Continuation Reference	A continuation reference describes how the performance of all or part of an operation requested of a server can be continued at different servers. See also *Referral*.
CRL	Certificate Revocation List
DAP	The X.500 Directory Access Protocol
DBMS	DataBase Management System
DEN	Directory-Enabled Networks
DHCP	Dynamic Host Configuration Protocol (of the Internet). See IETF RFC 2131.
DIF	Directory Interoperability Forum
DIT	Directory Information Tree. The set of entries in a directory form a tree. Each entry (except the root entry) has a single superior entry and may have one or more subordinate entries. See also *RDN*, *Leaf Entry*.
DN	Distinguished Name. In a directory, the unique name of an entry formed by the concatenation of the *RDN*s of the entry and each of its superior entries.
DNS	Domain Name Service (of the Internet). See IETF RFC 1035.
End Entity	User of PKI certificates, or end-user/system that is the subject of a certificate.
Extranet	Extension of an organization's *intranet* that includes its business partners and other correspondents.
Firewall	Device or set of devices that protects an organization's network by filtering traffic between it and the global Internet.
GP	General (medical) Practitioner, in the UK
HR	Human Resources
HTTP	The HyperText Transfer Protocol. See IETF RFC 1945.
HTTPS	Secure HTTP — obtained by running *HTTP* over *SSL*.
IESG	The Internet Engineering Steering Group
IETF	The Internet Engineering Task Force
IMAP	Internet Mail Access Protocol. See IETF RFC 2060.
Intranet	The systems and networks that operate the Internet Protocol and belong to a single organization. They are often separated from the global Internet by a *firewall*.
IP	The Internet Protocol defined in IETF RFC 791.
IT	Information Technology
ITU-T	Telecommunications Standardization Section of the International

	Telecommunications Union
LAN	Local-Area Network
LDAP	Lightweight Directory Access Protocol. See IETF RFC 2251.
LDIF	The LDAP Data Interchange Format. A data format specification for directory contents, currently at draft status within the IETF.
LDUP	LDAP Duplication/Replication/Update Protocols
Leaf Entry	A directory entry that has no subordinate entries in the *DIT*.
Metadirectory	Product that provides a uniform (LDAP) directory interface to collections of directory and other data storage products.
NHS	(UK) National Health Service
ODBC	Open DataBase Connectivity
PC	Personal Computer
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure (X.509) working group of the *IETF*
RA	Registration Authority (of certificates, in a *PKI*)
RDN	Relative Distinguished Name. In a directory, a name that uniquely distinguishes an entry from other entries with the same superior entry in the *DIT*.
Referral	An outcome which can be returned by a server which cannot perform an operation itself, and which identifies one or more other servers more able to perform the operation.
Replication	The process by which copies of entries are made and maintained between servers.
RFC	Request For Comment – generic name given to standards and other publications of the *IETF*.
SASL	Simple Authentication and Security Layer. See IETF RFC 2222.
SDK	Software Development Kit – especially one that includes a client implementation of LDAP and provides LDAP functionality to applications via an API.
S/MIME	Secure/Multipurpose Internet Mail Extensions. See IETF RFC 2633.
SQL	Structured Query Language
SRV	*DNS* Service Location Record. See IETF RFC 2782.
SSL	Secure Sockets Layer protocol
T.61	A recommendation of the *ITU-T* that includes the definition of a particular character set used in telematic services.
TCP	Transmission Control Protocol of the Internet, defined in IETF RFC 793.
TLS	Transport Layer Security. An IETF-defined protocol based on *SSL*. See IETF RFC 2246.
UDP	User Datagram Protocol of the Internet, defined in IETF RFC 768.
UNICODE	The Universal Character-Set Encoding defined by the UNICODE consortium, and a subset of the encoding defined in ISO 10646.
URL	Uniform Resource Locator — colloquially, a *WWW* address. See IETF RFC 1738.
USERID	User Identity
UTF-8	The File System Safe Universal Character Set Transformation Format

	defined in The Open Group Technical Standard C501. A representation of the *UNICODE* character set.
VPN	Virtual Private Network. See also *Intranet*.
VSLDAP	*LDAP* Verification Test Suite produced by The Open Group.
WAN	Wide-Area Network
WAP	The Wireless Applications Protocol
WWW	The World-Wide Web (of *HTTP* servers on the Internet)
X.500	Series of recommendations for directory services defined by the *ITU-T*. Different versions of these recommendations have been produced in different years.
X.509	One of the X.500 recommendations – "X.509: The Directory: Authentication Framework". Includes a data format specification for certificates.

Appendix C: Bibliography

Practical Guide to the Open Brand, January 1998, The Open Group (X981).

The Open Brand Trademark License Agreement (TMLA), January 1998, The Open Group (X982).

LDAP 2000 Product Standard, December 1999, The Open Group (X99DI).

IETF RFC 2251, Lightweight Directory Access Protocol (Version 3), December 1997.

IETF RFC 2252, Lightweight Directory Access Protocol (Version 3): Attribute Syntax Definitions, December 1997.

IETF RFC 2253, Lightweight Directory Access Protocol (Version 3): UTF-8 String Representation of Distinguished Names, December 1997.

IETF RFC 2254, The String Representation of LDAP Search Filters, December 1997.

IETF RFC 2255, The LDAP URL Format, December 1997.

IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.

The SSL Protocol, Version 3.0, Netscape Communications Corporation, March 1996.

ITU-T Recommendation X.500, Information Technology — Open Systems Interconnection — The Directory: Overview of Concepts, Models, and Services, August 1997.

Understanding and Deploying LDAP Directory Services, T. Howes, M. Smith, and G. Good, MacMillan, December 1998.

Directory-Enabled Networking, J. Strassner, MacMillan, October 1999.

Directory-Enabled Computing: The Directory's Expanding Role, Network Strategy Overview, The Burton Group, December 1999.

The Enterprise Directory Value Proposition, Network Strategy Overview, The Burton Group, February 1999.

Appendix D: Acknowledgements

The scenario in its current state incorporates the work of a number of people, both within and outside the Directory Program Group. Particular thanks are due to the following:

- Globalsign — Wim Hendrickx for his input.
- Kaiser Permanente — Doug Shelton for his input.
- Shell —Nick Mansfield for his support, Pauwl Lunow for his input, and especially Peter Harris for his patience in explaining Shell's business processes and their use of directory to support PKI.
- Siemens — Patrick Fantou, for his input and for the contents of Appendix A, which is his work.
- The UK NHS — Hugh Fisher for his input and support, and Ron Bissell and Andy Garcarz for their patience in explaining NHS requirements and thinking.

Finally, a special acknowledgement is due to Terry Blevins, formerly of NCR, who introduced the concept of the Business Scenario, led the workshops with the NHS and Shell, and developed specific scenarios from them. Without his help, this Business Scenario for The Directory-Enabled Enterprise would not have been possible.