

Directory Services Landscape

Services, Technologies, Protocols,
Products, and the Medium

Mohsen Banan

<public@mohsen.banan.1.byname.net>

Outline

- **Directory Concepts** 
- **X.500 & OSI Directory**
- **X.509 & PKI**
- **LDAP**
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)**
- **SQL & Oracle**
- **Misc.**
- **Predictions & the Future**

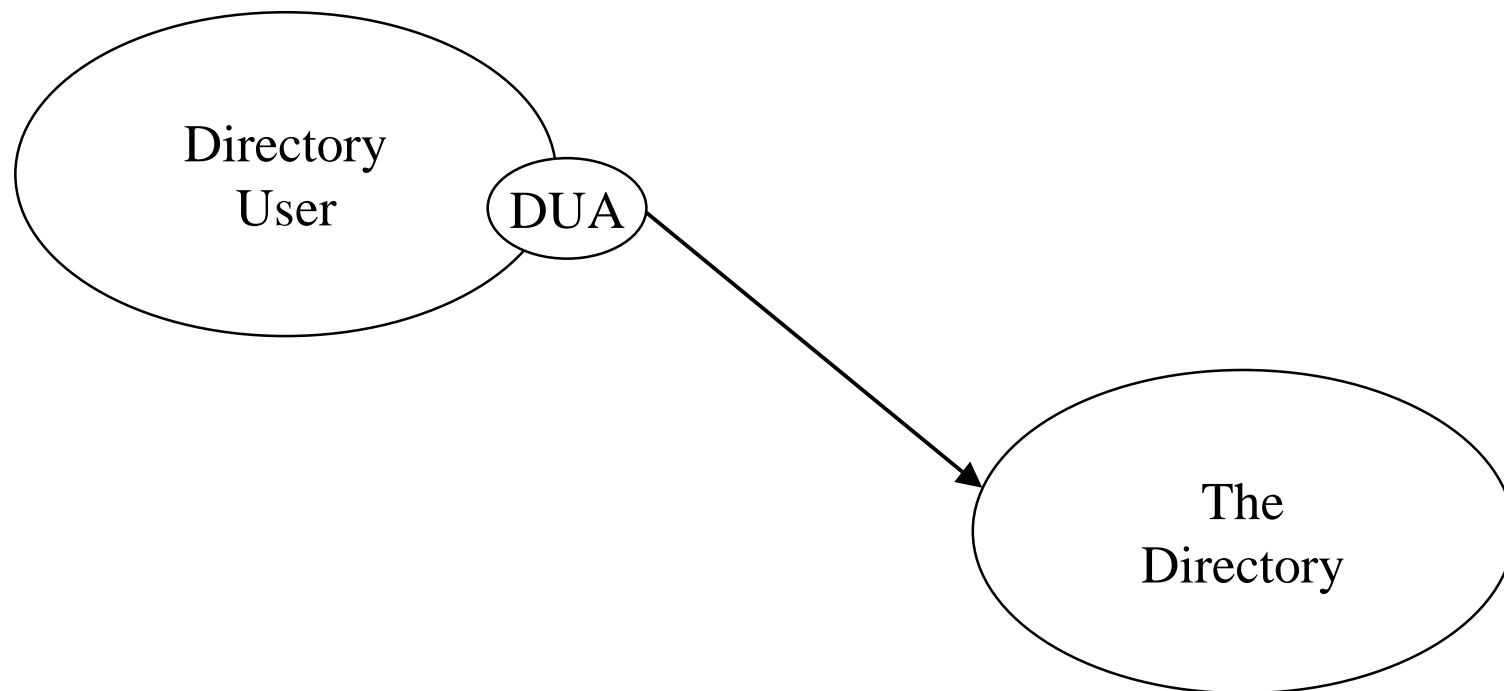
Basic Directory Concepts

- **Prior to the initiation of any communication, some addressing and other infrastructural information is needed for interconnection of information processing systems**
- **Directory services provide access to such information**
- **“The Directory” Is an integrated whole, consisting of a set of systems and the directory information they hold, that provide the addressing and other infrastructural information needed for communication**


Basic Directory Concepts

- **The Directory (singular) is an integrated whole one global name space**
- **The Directory is not intended to be a general-purpose database system**
- **A considerably higher frequency of 'queries' than of updates is assumed**
- **Transient conditions where both old and new versions of the same information are available, are quite acceptable**
- **Except for unpropagated updates and access rights, the results of directory queries will not be dependent on the identity or location of the inquirer**

Directory and Users



Outline

- **Directory Concepts**
- **X.500 & OSI Directory** ← 
- **X.509 & PKI**
- **LDAP**
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)**
- **SQL & Oracle**
- **Misc.**
- **Predictions & the Future**

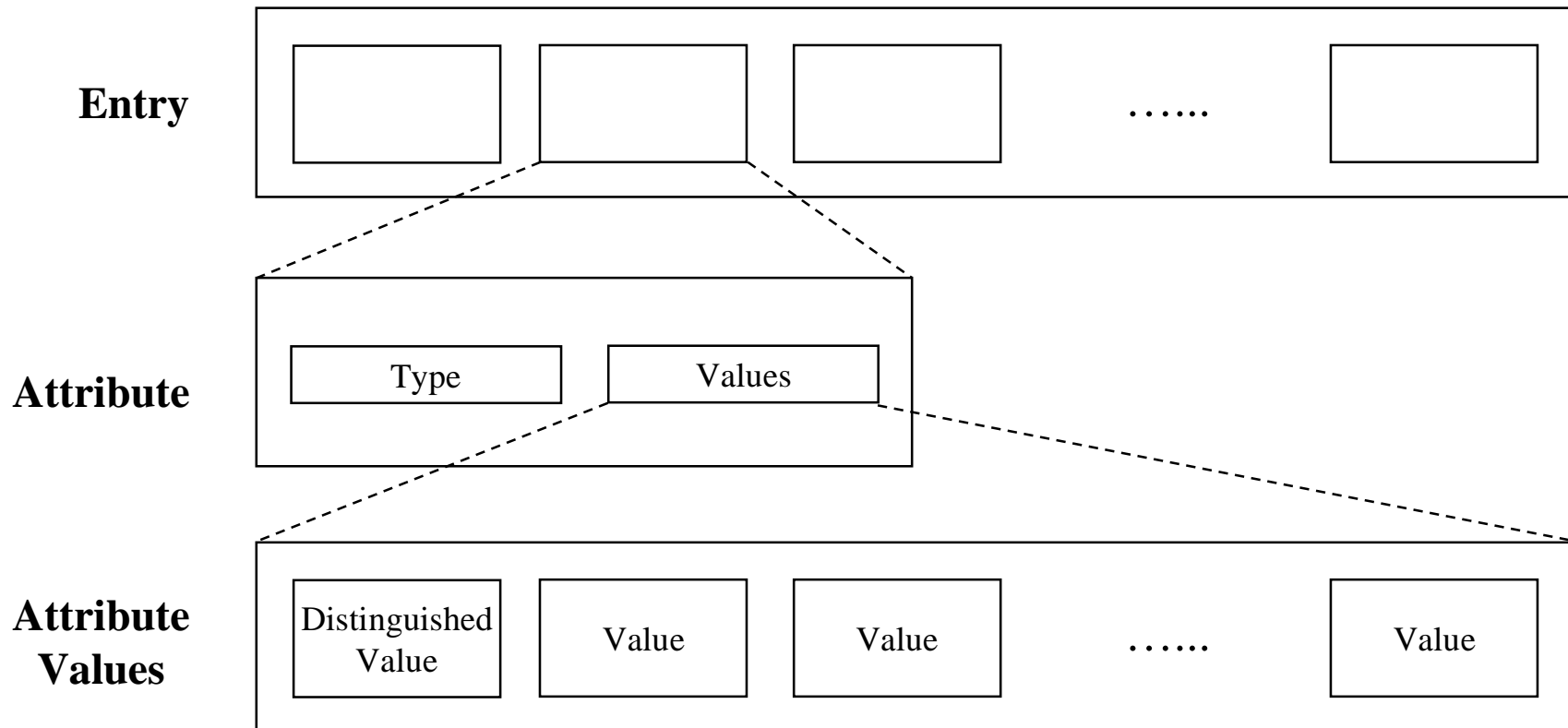
X.500 Topics

- **OSI Directory Services standards (The Dreams)**
 - Directory Model
 - Information Model
 - Security Model
- **Directory Services Implementations and Applications (Reality)**
 - Scope and field of application of OSI Directory Services
 - Expected Evolution of Directory Services
 - IBM, DEC and others
 - Internet White-Pages Pilot Project
- **Conclusions**

Information Model

- **Directory Information Base (DIB)**
 - All information to which the Directory provides access
 - Without regard to distributed or centralized architecture
 - Without regard to hierarchy

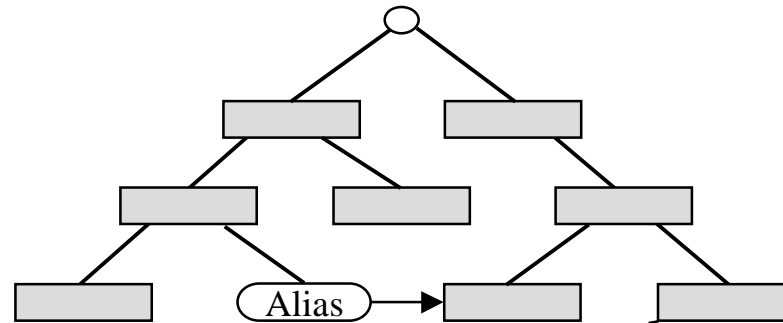
Informational Model Entries



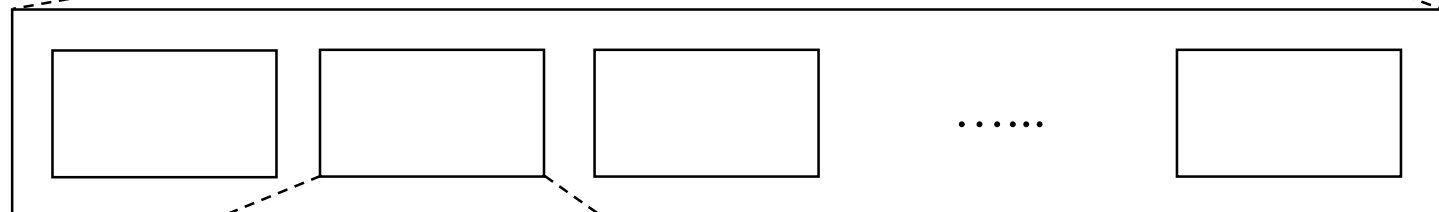
Information Model

Directory Information Tree (DIT)

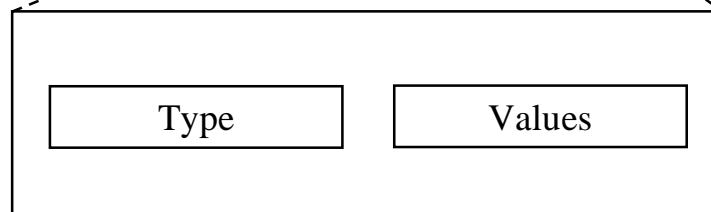
DIT



Entry



Attribute

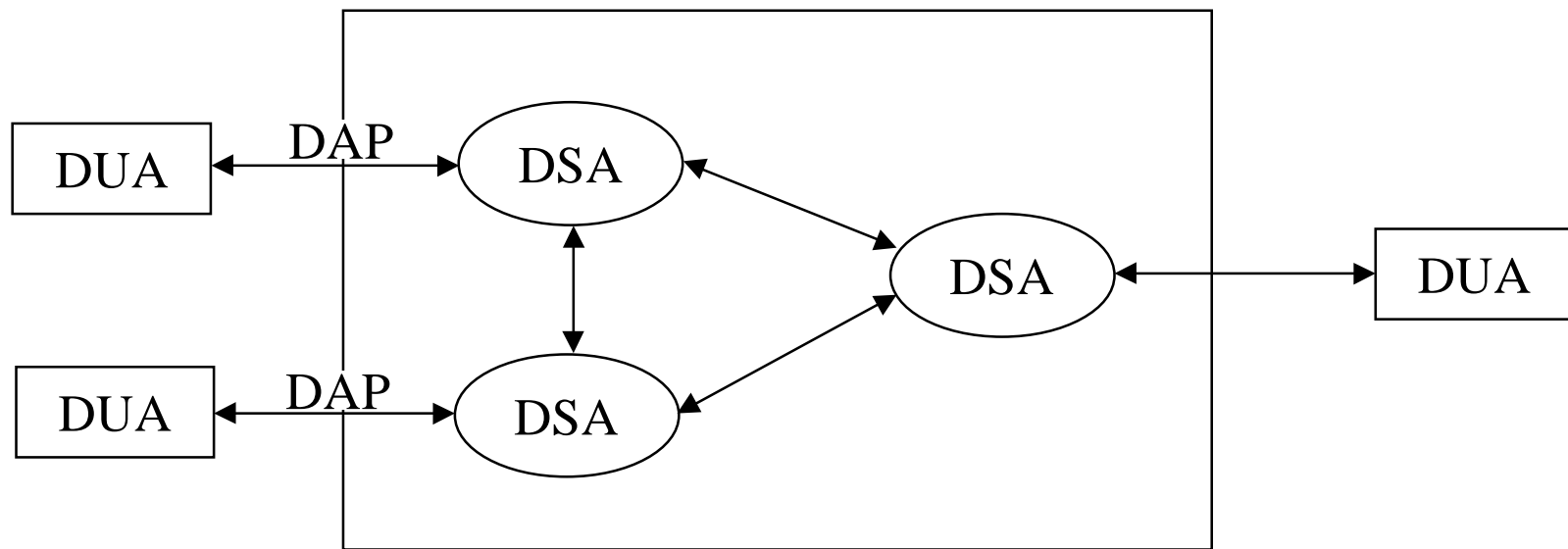


Information Model Schema

- **The Directory Schema comprises a set of:**
 - DIT structure definition
 - Object class
 - Attribute type
 - Attribute syntax

Functional Model

- Distributed Directory Service Model



DAP = Directory Access Protocol
DSP = Directory System Protocol

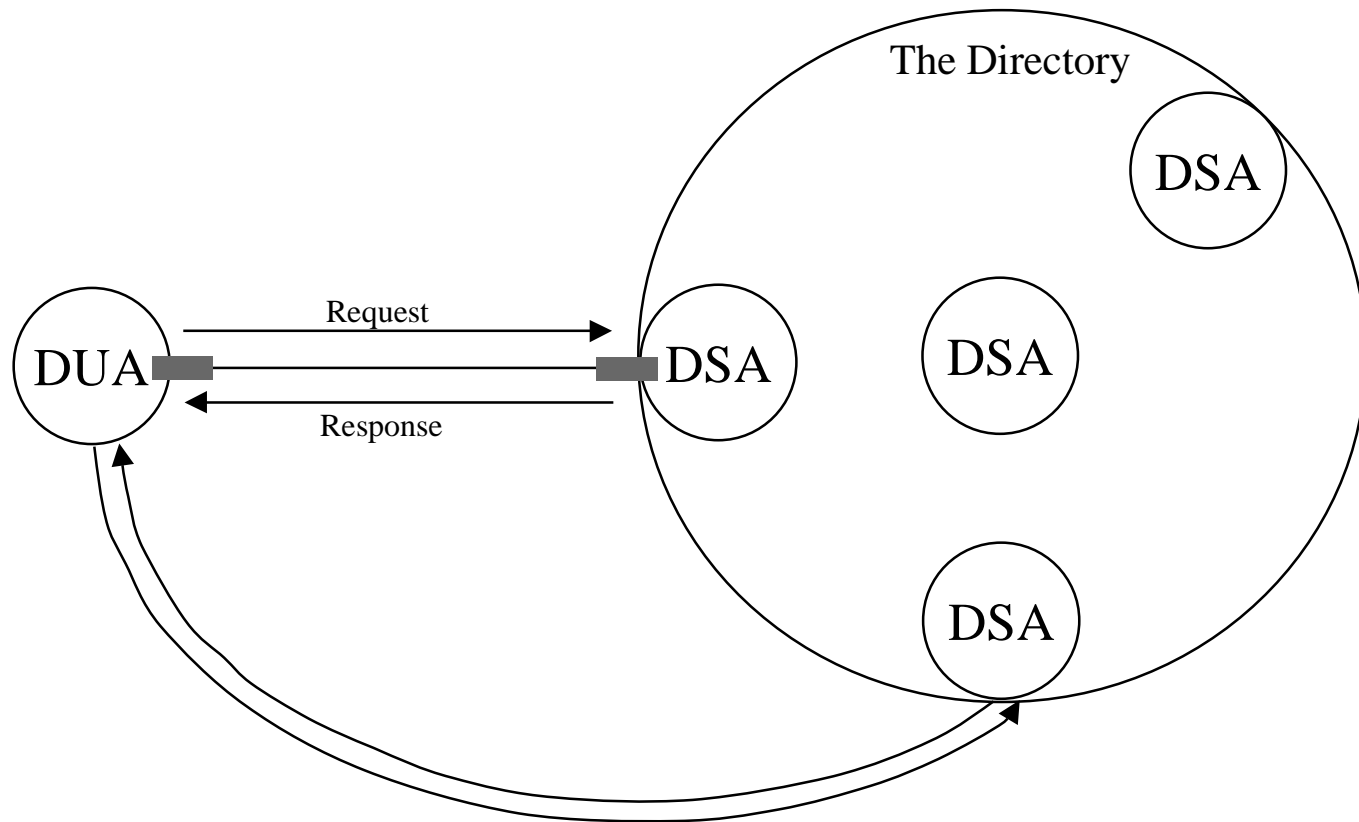
DUA = Directory User Agent
DSA = Directory System Agent

Functional Model

- **Referrals**
- **Chaining**
- **Multi-casting**

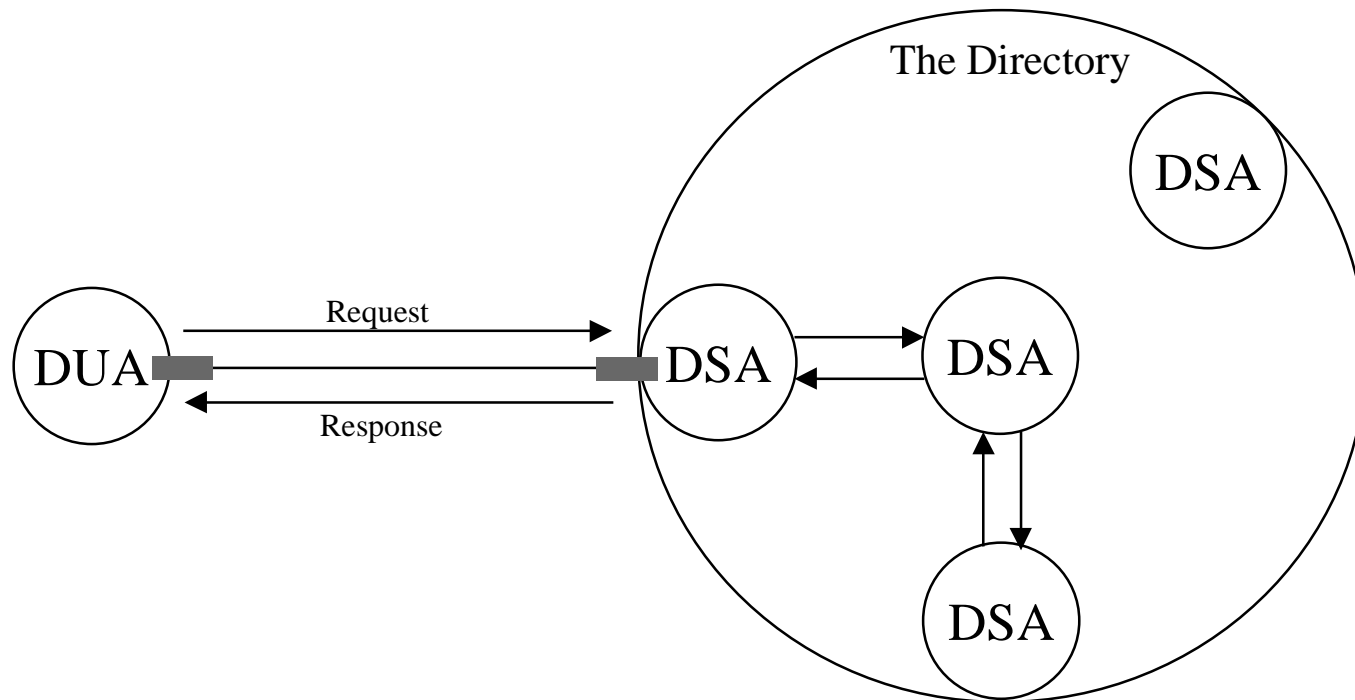
Functional Model

- Referrals



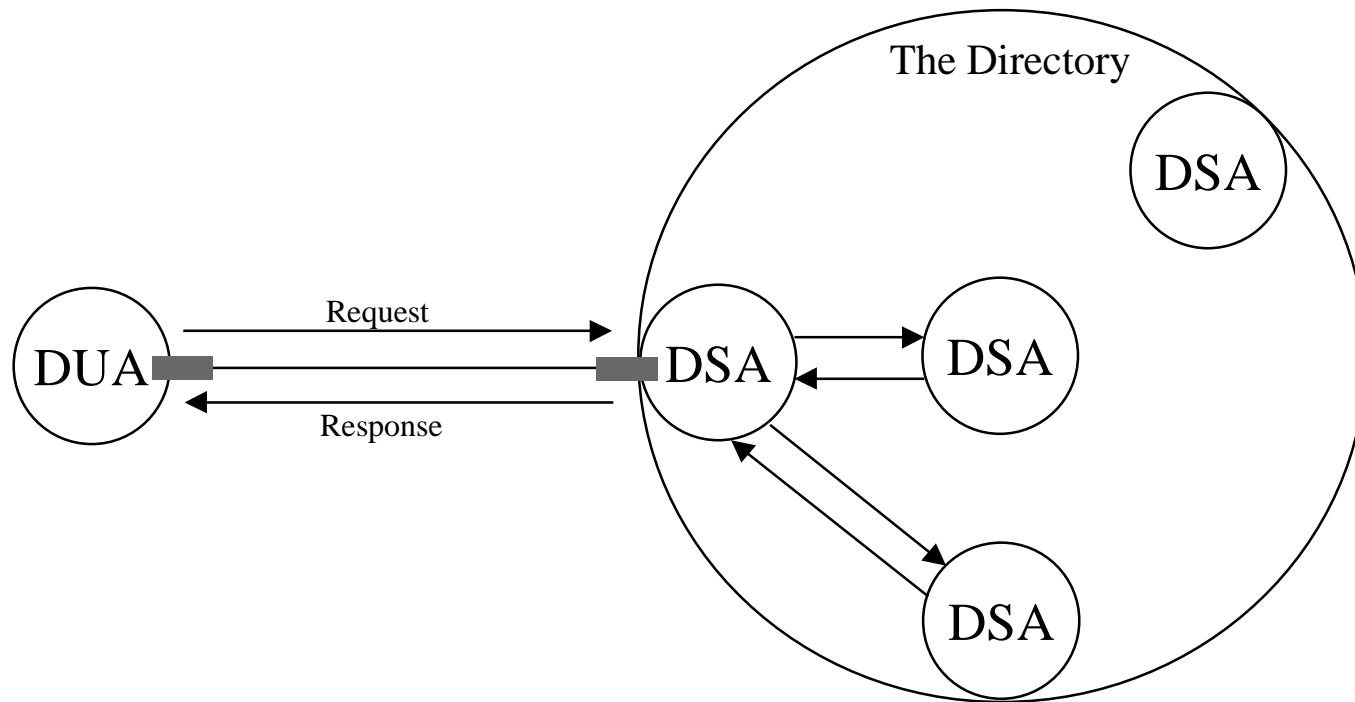
Functional Model

- Chaining



Functional Model

- Multi-Casting



The X.500 Recommendation (ISO-9594)

- **X.500 Overview**
- **X.501 Models**
- **X.509 Authentication Framework**
- **X.511 Abstract Service Definition**
- **X.518 Procedures for Distributed Operations**
- **X.519 Protocol Specifications**
- **X.520 Selected Attribute Types**
- **X.521 Selected Object Classes**


Field of Applications of OSI Directory Services

- **Inter-personal Communication**
 - Provide humans or their agents with information on how to communicate with other humans, or groups thereof
- **Inter-system Communication**
 - Map application-titles onto presentation addresses
- **Authentication**

X.500 Conclusions

- **X.500 provides a valuable model and terminology for directory**
- **Implementations of OSI Directory Services that address the local and enterprise-wide directory requirements will soon be available from a number of vendors**
- **“Global OSI Directory” requires completion of the specification**
- **We need to understand our directory requirements and properly apply OSI Directory Services to those requirements**
- **Policies and procedures for administration of an enterprise-wide directory must be very carefully planned**

Outline

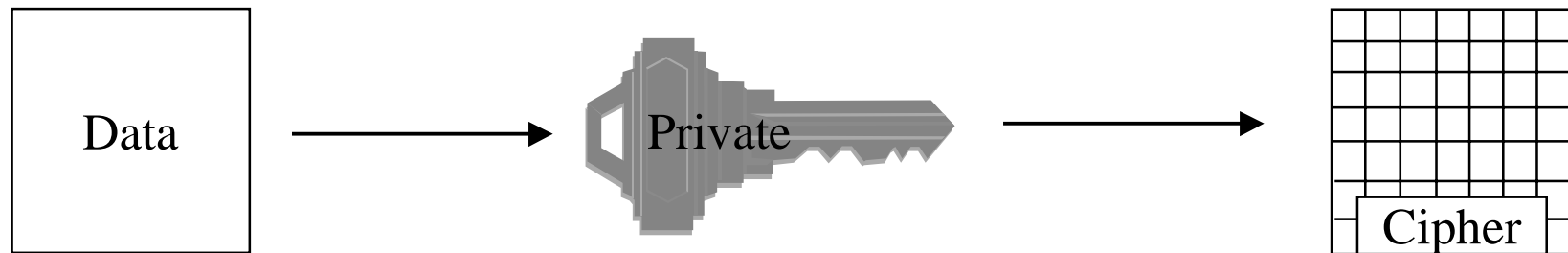
- **Directory Concepts**
- **X.500 & OSI Directory**
- **X.509 & PKI** 
- **LDAP**
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)**
- **SQL & Oracle**
- **Misc.**
- **Predictions & the Future**

Security Model

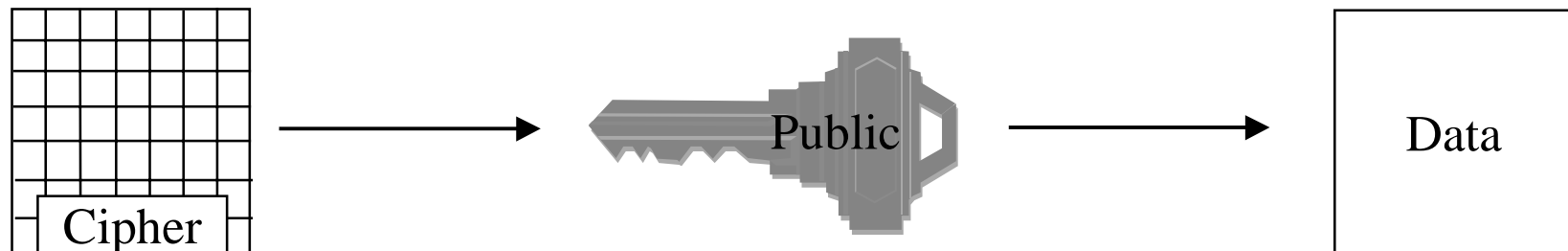
- **Authentication**
- **Public Key Cryptographic Systems (PKCS)**
- **Digital Signatures**

Security Model

- Public Key Cryptographic Systems (PKCS)
 - Data encrypted by one key half:

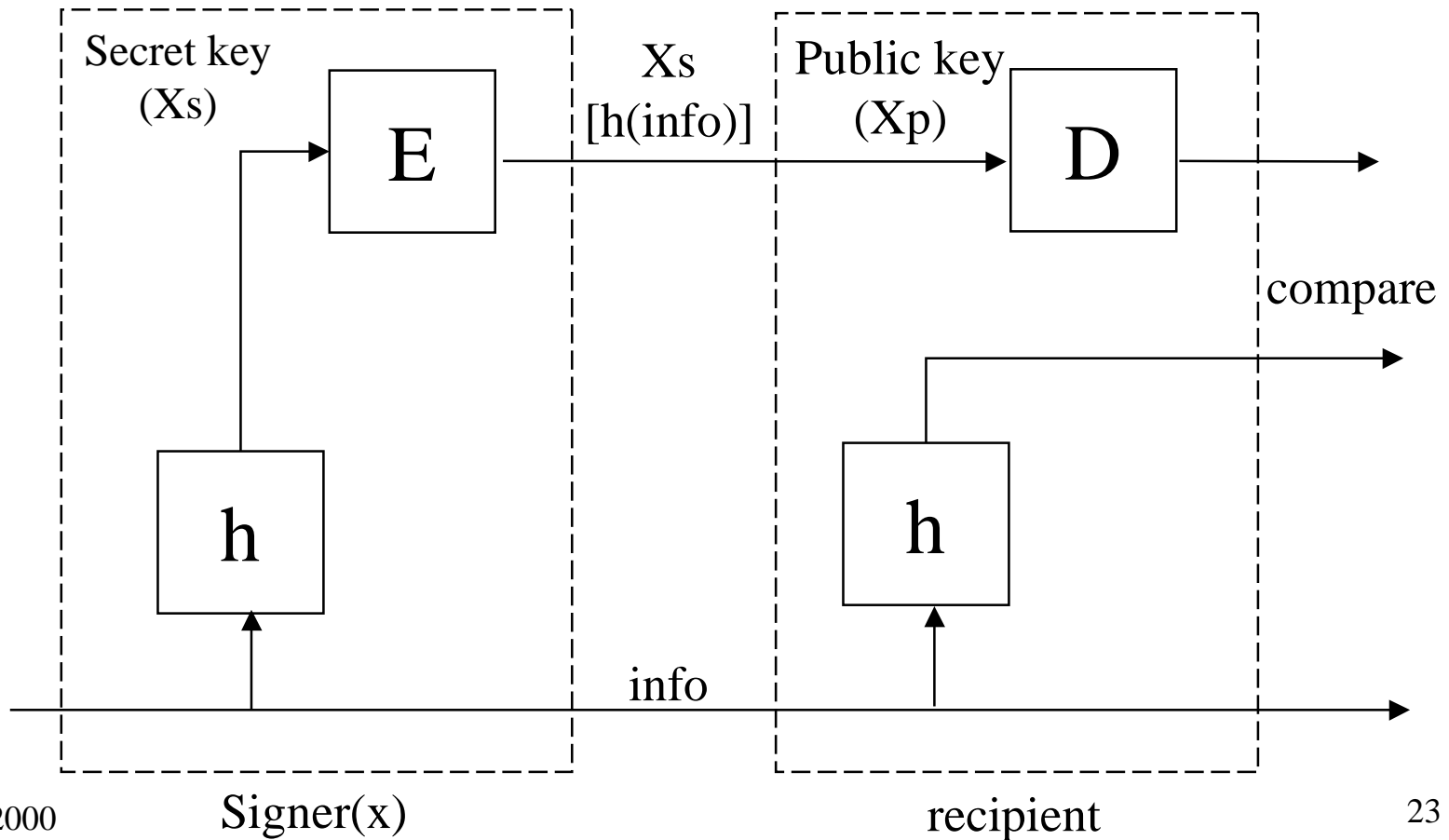


- Can only be decrypted by matching key half




Security Model

-Digital Signatures



Outline

- **Directory Concepts**
- **X.500 & OSI Directory**
- **X.509 & PKI**
- **LDAP** 
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)**
- **SQL & Oracle**
- **Misc.**
- **Predictions & the Future**

LDAP- related RFCs

- **RFC-1777 Lightweight Directory Access Protocol.**
- **RFC-1558 A String Representation of LDAP Search Filters**
- **RFC-1778 The String Representation of Standard Attribute Syntaxes**
- **RFC-1779 A String Representation of Distinguished Names**
- **RFC-1798 Connectionless LDAP**
- **RFC-1823 The LDAP Application Program Interface**
- **RFC-1959 An LDAP URL Format**

What is LDAP?

- **What is LDAP?**

LDAP is a client-server protocol for accessing a directory service. It was initially used as a front-end to X.500, but can also be used with stand-alone and other kinds of directory servers.

- **Why do we need LDAP? Why don't we just use X.500?**

LDAP does not require the upper layers OSI stack, it is a simpler protocol to implement(especially in clients), and LDAP is under IETF change control and so can more easily evolve to meet Internet requirements.

LDAP Info Model

- **What can I store in an LDAP directory?**

The LDAP information model is based on the entry, which contains information about some object (e.g., a person). Entries are composed of attributes, which have a type and one or more values.

Each attribute has a syntax that determines what kind of values are allowed in the attribute and how those values behave during directory operations.


Examples of attribute syntaxes are for IA5 (ASCII) strings, JPEG photographs, u-law encoded sounds, URLs and PGP keys.

LDAP & X.500

- **Can I connect a stand-alone LDAP directory server into an X.500 directory?**

Yes! See for example the X.500 Enabler.

Outline

- **Directory Concepts**
- **X.500 & OSI Directory**
- **X.509 & PKI**
- **LDAP**
- **Domain Name System (DNS)** ← 
- **Novel Directory Services (NDS)**
- **SQL & Oracle**
- **Misc.**
- **Predictions & the Future**

Domain Name System (DNS)

- **What is DNS?**

DNS is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses, and to control Internet email delivery.

Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

Structure of DNS Name

- **Each name consists of a sequence of alphanumeric components separated by periods**
- **Examples:**
 - www.eg.bucknell.edu
 - www.netbook.cs.purdue.edu
 - charcoal.eg.bucknell.edu
- **Names are hierarchical, with most-significant component on the right**
- **Left-most component is computer name**

DNS naming structure

- **Top level domains (right-most components; also known as TLDs) defined by global authority**
- **Organizations apply for names in a top-level domain:**
 - bucknell.edu
 - macdonalds.com
- **Organizations determine own internal structure**
 - eg.bucknell.edu
 - cs.purdue.edu

Top Level Domains

Domain Name	Assign To
Com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military group
net	Major network support center
org	Organization other than those above
arpa	Temporary ARPA domain (still used)
int	International organization
<i>country code</i>	A country

Name Server Concept

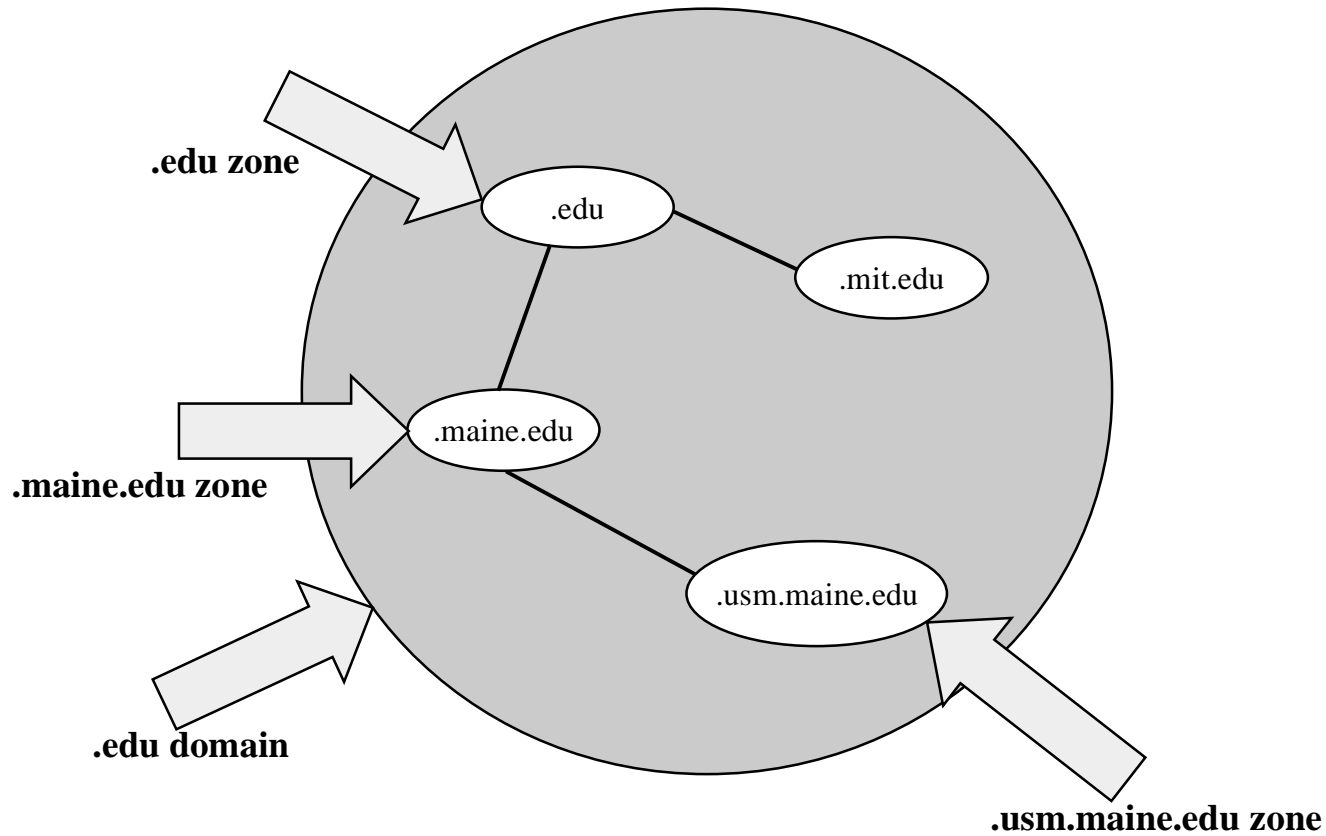
- **Zone**

- A zone is part of the name space (such as ee.usm.maine.edu or bbn.com) delegated to a single server. If a nameserver is listed at the internic (or a higher level nameserver as authoritative for part of the name space, and it has full data on that part of the name space then it is authoritative for that zone.

- **Domain**

- A domain is also part of the name space, but it may covers several zones. (maine.edu is a domain that covers both the usm.maine.edu and the caps.maine.edu zones)

Zone Example



Name Servers

- **The DNS Server**

- Answers DNS Queries sent by resolvers
- Listens at UDP and TCP port 53
 - UDP for routine queries
 - TCP used for zone transfers

- **Configurations**

- Caching-only: relies on other name servers for authoritative answers
- Primary: Contains the writable authoritative copy for the zones that it is primary for
- Secondary: Contains mirror copy of the data from a primary nameserver. No updates take place here, used to provide redundancy

Client-server computing

- **Clients and servers communicate in distributed computing**
 - Client initiates contact to request some remote computation
 - Server waits for clients and answers requests as received
- **Clients are usually invoked by users as part of an end-user application**
- **Servers are usually run on central, shared computers**



Primary vs. Secondary Servers

- **Primary**
 - Data loaded from a file.
 - One primary server per zone.

- **Secondary**
 - Data transferred from a primary server.
 - Data may be stored in a file.
 - Checks every refresh period with the primary, looking for changes.
 - Might have many secondaries per zone

Outline

- **Directory Concepts**
- **X.500 & OSI Directory**
- **X.509 & PKI**
- **LDAP**
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)** ←
- **SQL & Oracle**
- **Misc.**
- **Predictions & the Future**

NDS

According to Novell

- **Directory-enabled applications are the future of e-business -- the directory will soon be to the network what the operating system is to the PC.**
- **eDirectory supports more open standards and protocols than all other directory services combined.**
- **It is well on its way to becoming the de facto standard for directory services.**
- **Companies like Alta Vista, BroadVision, Cisco, CNN, Lucent Technologies, Nortel, Oracle, Sun Microsystems, Xircom, and many others support NDS and offer NDS-enabled services.**
- **This NDS momentum is driving computing into a new era based on the directory.**

NDS Security

According to Novell

- **With NDS eDirectory you can also be sure your resources are secure.**
- **eDirectory's superior security features include:**
 - Novell International Cryptographic Infrastructure
 - passwords encrypted over Secure Sockets Layer
 - RSA private key/public key encryption
 - Secure Authentication Services, smart cards, and X.509v3 certificates.
- **You will be able to designate exactly who is allowed access to which information; granting rights to one directory will not provide rights to your entire network or even to all the information in that directory.**

NDS Comparison According to Novell

- **Why is NDS eDirectory better for e-business than Netscape Directory Server, Oracle Internet Directory or other existing LDAP directories?**

Besides a technical argument, we can boil our answer down to three reasons:

- **Maturity--we've been around for 8 years.**
- **Performance--Key Labs testing shows that we beat Netscape in head to head benchmarking**
- **Scalability--We demonstrated at Brainshare SLC 99 a billion user tree**

Check out www.novell.com/advantage/nds for competitive briefs.

NDS vs. X.500


According to Novell

- **X.500 directories are being pulled along as part of PKI deployments, how do you expect NDS to penetrate this market?**

NDS eDirectory provides the foundation for e business.

Security and PKI are becoming an increasingly important component in thee-business e-costructure.

Outline

- **Directory Concepts**
- **X.500 & OSI Directory**
- **X.509 & PKI**
- **LDAP**
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)**
- **SQL & Oracle** 
- **Misc.**
- **Predictions & the Future**


What About SQL?

- **Structured Query Language (SQL) is a language that provides an interface to relational database systems. SQL was developed by IBM in the 1970s for use in System R.**
- **SQL is a de facto standard, as well as an ISO and ANSI standard. SQL is often pronounced SEQUEL.**
- **In common usage SQL also encompasses DML (Data Manipulation Language), for INSERTs, UPDATEs, DELETEs and DDL (Data Definition Language), used for creating and modifying tables and other database structures.**
- **The development of SQL is governed by standards. A major revision to the SQL standard was completed in 1992, called SQL2. SQL3 support object extensions and will be (partially?) implemented in Oracle8.**

SQL Features

- **SQL allows users to access data in relational database management systems, such as Oracle, Sybase, Informix, Microsoft SQL Server, Access, and others, by allowing users to describe the data the user wishes to see.**
- **SQL also allows users to define the data in a database, and manipulate that data.**


Outline

- **Directory Concepts**
- **X.500 & OSI Directory**
- **X.509 & PKI**
- **LDAP**
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)**
- **SQL & Oracle**
- **Misc.** 
- **Predictions & the Future**

Others & Misc

- Oracle
- Netscape Directory
- The Web itself
-

Outline

- **Directory Concepts**
- **X.500 & OSI Directory**
- **X.509 & PKI**
- **LDAP**
- **Domain Name System (DNS)**
- **Novel Directory Services (NDS)**
- **SQL & Oracle**
- **Misc.**
- **Predictions & the Future** 

True Of All

- **Technology is not all that relevant**
- **What information & why?**
- **Who owns the information**
- **Trust -- Show stopper -- Unless dealt with**
- **Privacy -- Show stopper -- Unless dealt with**
- **Not a big brother problem -- Lots of small brothers**