The Role of Directories in emerging network technologies

Carnet User Conference,

Zagreb, Croatia,

September 27, 2002

Peter Gietz

peter@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management

Agenda

- Introduction to LDAP
- LDAP based Directory Services
  - 1. Classical Services
  - 2. Indexbased services
  - 3. PKI Services
  - 4. Information Services (metadata, ontologies)
  - 5. Policy data service
  - 6. Services for Grid Computing
- Visions for the future

DAASI International

Directory Applications for Advanced Security and Information Management

Introduction to LDAP

What is a Directory?

- Information stored in a hierarchical System
- Examples:
  - File directory of an operating system (MS/DOS, Unix)
  - Domain Name Service (DNS)
  - Network Information System (NIS)
  - X.500 is *the* Directory
  - Lightweight Directory Access Protocol (LDAP) = The Internet (IETF) version of X.500
  - Novell Directory Service (NDS)
  - Microsoft Active Directory (AD)

DAASI International

Directory Applications for Advanced Security and Information Management

What is LDAP

- Lightweight Directory Acess Protocol
  - In Version 3 not only access protocol, but whole client-Server system
- It is a sort of a database
  - for storing and retrieving information
- It is a specialized database
  - designed for fast reading, writing is slower
  - static view on the data
  - simple updates without transactions

DAASI International

Directory Applications for Advanced Security and Information Management

What is LDAP (contd)

- It has a well defined and standardized network protocol for access
- It has inbuilt security features
- The technology allows for
  - distribution on the net
  - replication of the data
- Thus comparable to WWW, but:
  - It is well structured (as a database)
  - It can be accessed by humans *and* applications

DAASI International

Directory Applications for Advanced Security and Information Management

What kind of data can you store?

- Text data
  - names, addresses, descriptions, numbers, etc.
- Pointers
  - URLs, pointers to other data, etc.
- Public key certificates
- Graphics
  - photos, diagrams, etc.
- Other binary data
- Anything else you can think of

DAASI International

Directory Applications for Advanced Security and Information Management

Qualities of LDAP

- Any amount of data can be stored
- On any number of servers
- Data look the same everywhere
- Open model for any kind of data
- High scalability through distribution
- High accessability through replication
- High security through inbuilt authentication mechanisms

DAASI International

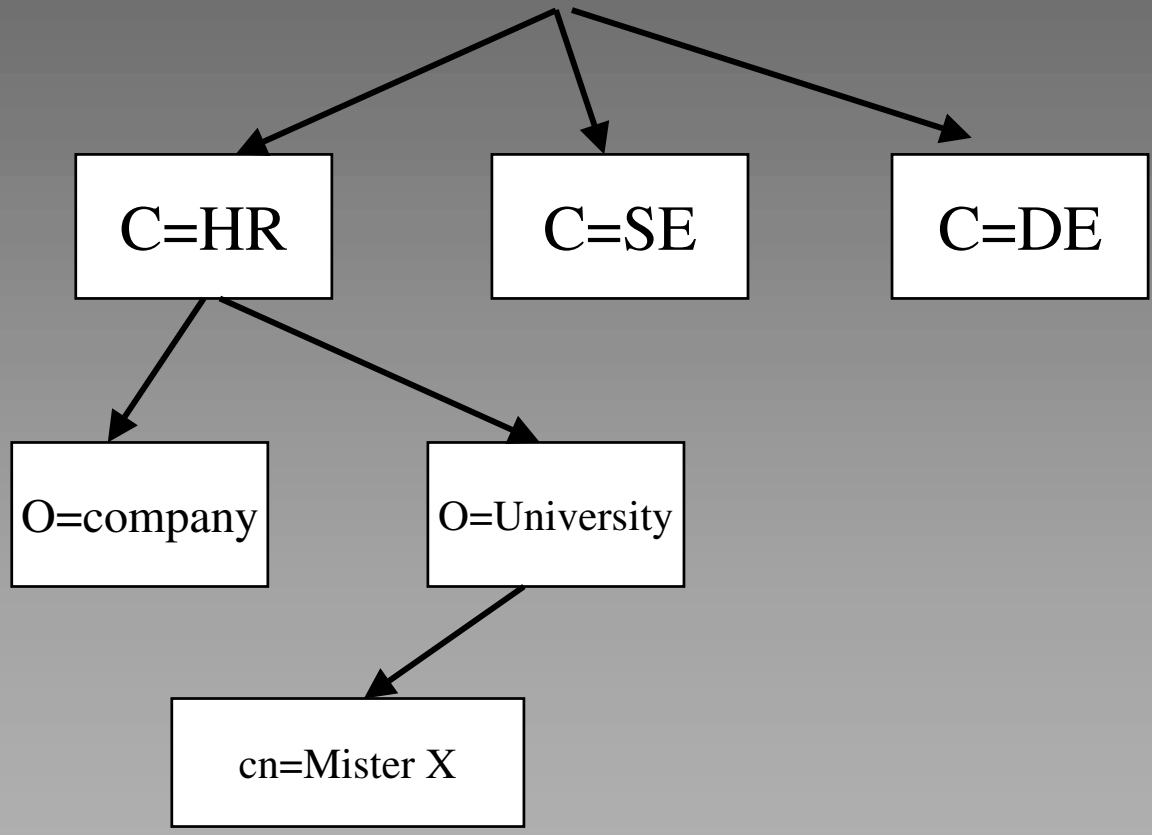
Directory Applications for Advanced Security and Information Management

Information Tree

- Data are stored in entries
- Entries are ordered as tree nodes
- In the Directory Information Tree (DIT)
  - Every node has 0 to n children nodes
  - Every node except root has 1 parent node

DAASI International
Directory Applications for Advanced Security and Information Management

Directory Information Tree (DIT)



DAASI International
Directory Applications for Advanced Security and Information Management

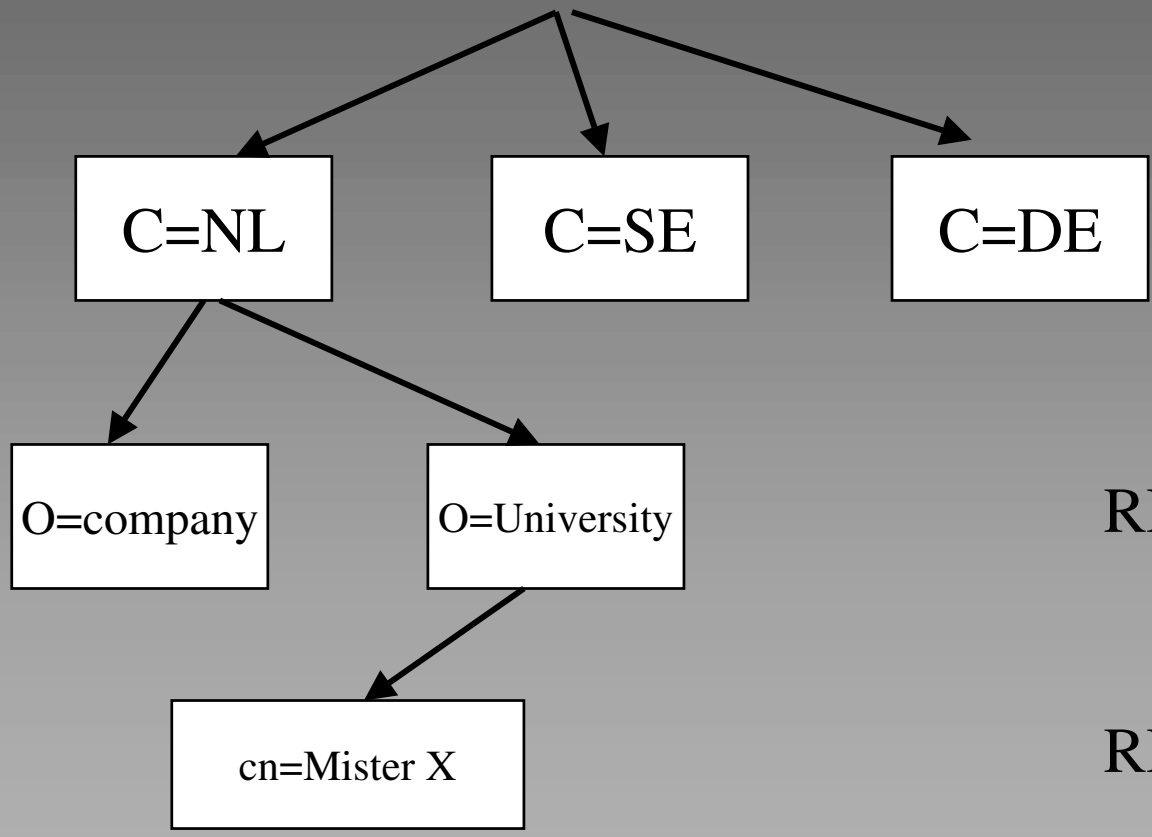
DN Distinguished Name

- An entry has a distinguished name
  - in its hierarchy level: Relative Distinguished Name (RDN)
  - all RDNs on the path from root form the Distinguished Name (DN)
- No two siblings, i.e. entries with a common parent can have the same RDN
- Thus no two entries in the whole Directory can have the same DN

DAASI International

Directory Applications for Advanced Security and Information Management

Relative Distinguished Name (RDN) and Distinguished Name (DN)



RDN: C=NL

RDN: o=University

RDN: cn=Mister X

DN: c=NL;o=University;cn=Mister X

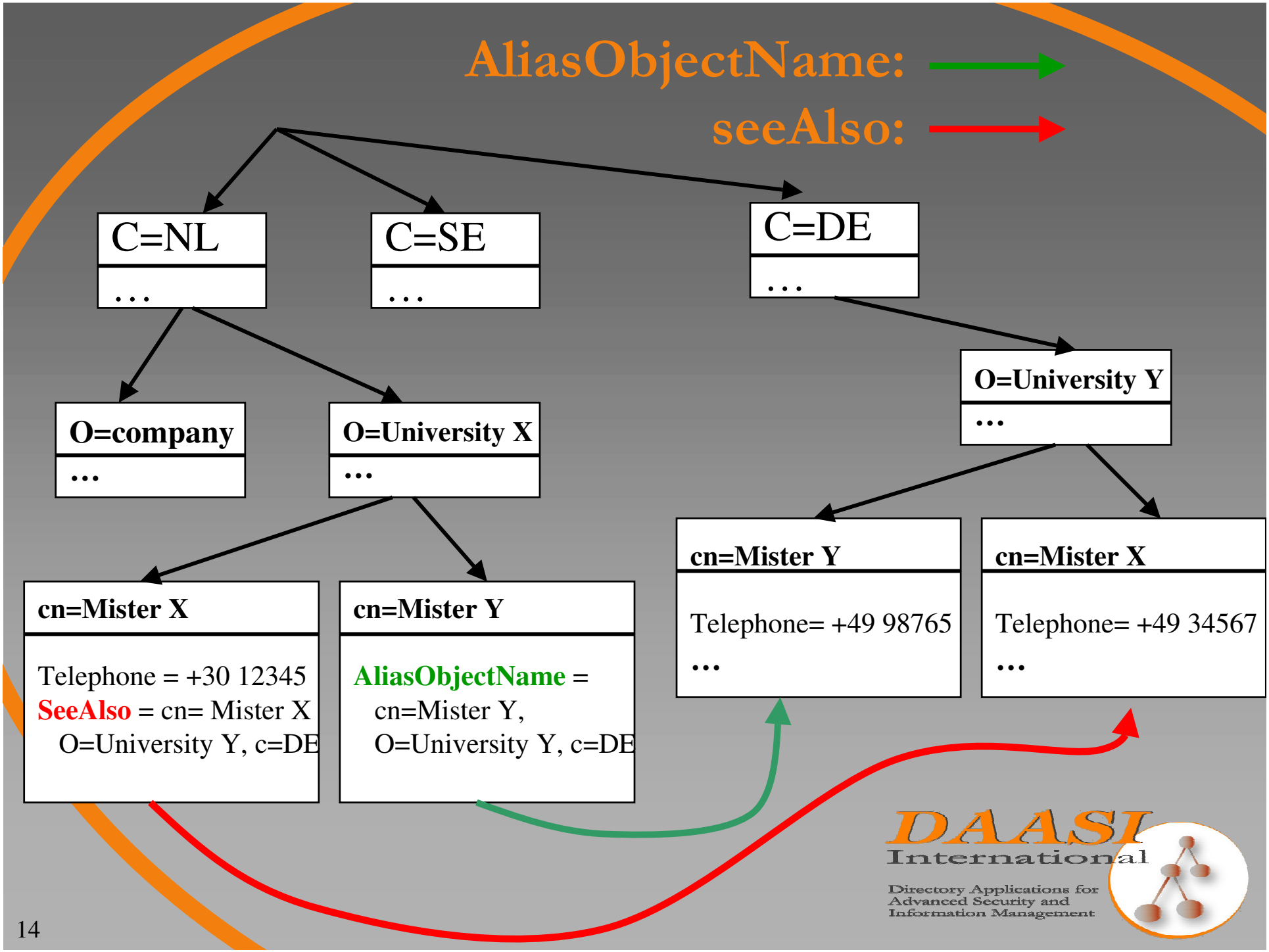
DAASI International
Directory Applications for Advanced Security and Information Management

DN Pointer

- Alias Entries have a DN and point to another DN via aliasObjectName Attribute
- seeAlso Attribute: Entry contains data and a seeAlso pointer to another DN

DAASI International

Directory Applications for Advanced Security and Information Management


AliasObjectName:
seeAlso:
C=NL
…
C=SE
…
C=DE
…
O=company
…
O=University X
…
O=University Y
…
cn=Mister X
Telephone = +30 12345
SeeAlso = cn= Mister X
O=University Y, c=DE
cn=Mister Y
AliasObjectName =
cn=Mister Y,
O=University Y, c=DE
cn=Mister Y
Telephone= +49 98765
…
cn=Mister X
Telephone= +49 34567
…
DAASI International
Directory Applications for Advanced Security and Information Management

Information Model

- An Entry contains a number of Attributes
- An Attribute consists of:
  - Attribute Type
  - Attribute Value(s)
- An Attribute Type has an associated Attribute Syntax
- The Attribute Value has to conform to that syntax
- Matching Rules to compare Attribute values for
  - equality
  - substring
  - ordering
  - extensible (selfdefined) matching

DAASI International
Directory Applications for Advanced Security and Information Management

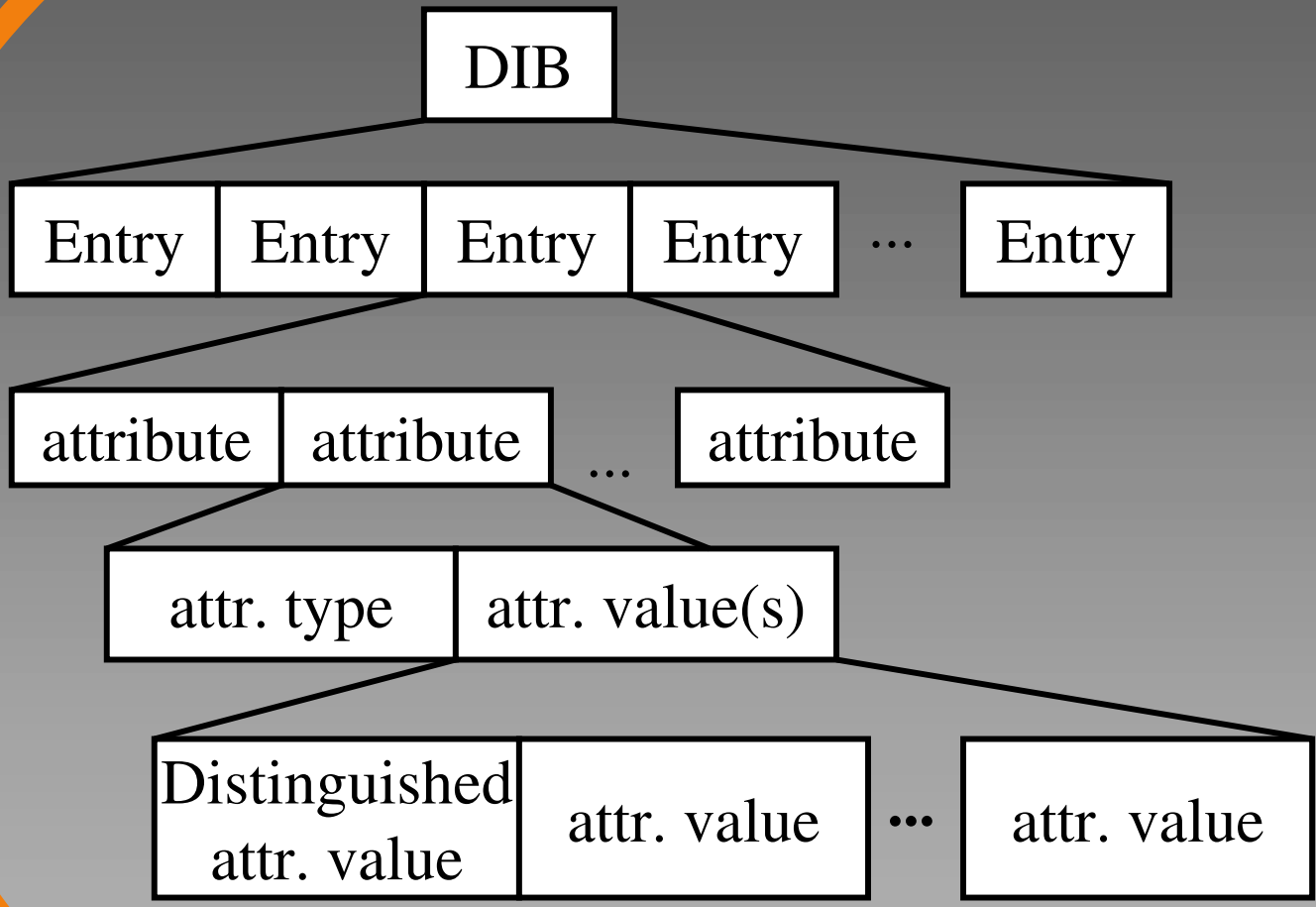
Special Attributes

- One or more Attribute type/value pairs form the RDN
  - The Naming Attributes or
  - The Distinguished Attributes
- An Entry must have one or more **Objectclass Attributes** which:
  - Characterizes the Entry, e.g. Person
  - Defines a set of usable Attributes the entry may contain and must contain
- Objectclasses can inherit Attributes from other Objectclasses
- A set of Objectclasses, Attributes and Syntaxes for a special purpose is called schema

DAASI International

Directory Applications for Advanced Security and Information Management

Directory Information Base



DAASI International

Directory Applications for Advanced Security and Information Management

Example:

DN: cn=Mister X, o=University, c=NL

Objectclass=top
Objectclass=person
Objectclass=organizationalPerson
cn=Mister X
cn=Xavier Xerxes
mail=X@dot.com
mail=Mister.X@dot.com
telephoneNumber=1234567

DAASI International
Directory Applications for Advanced Security and Information Management

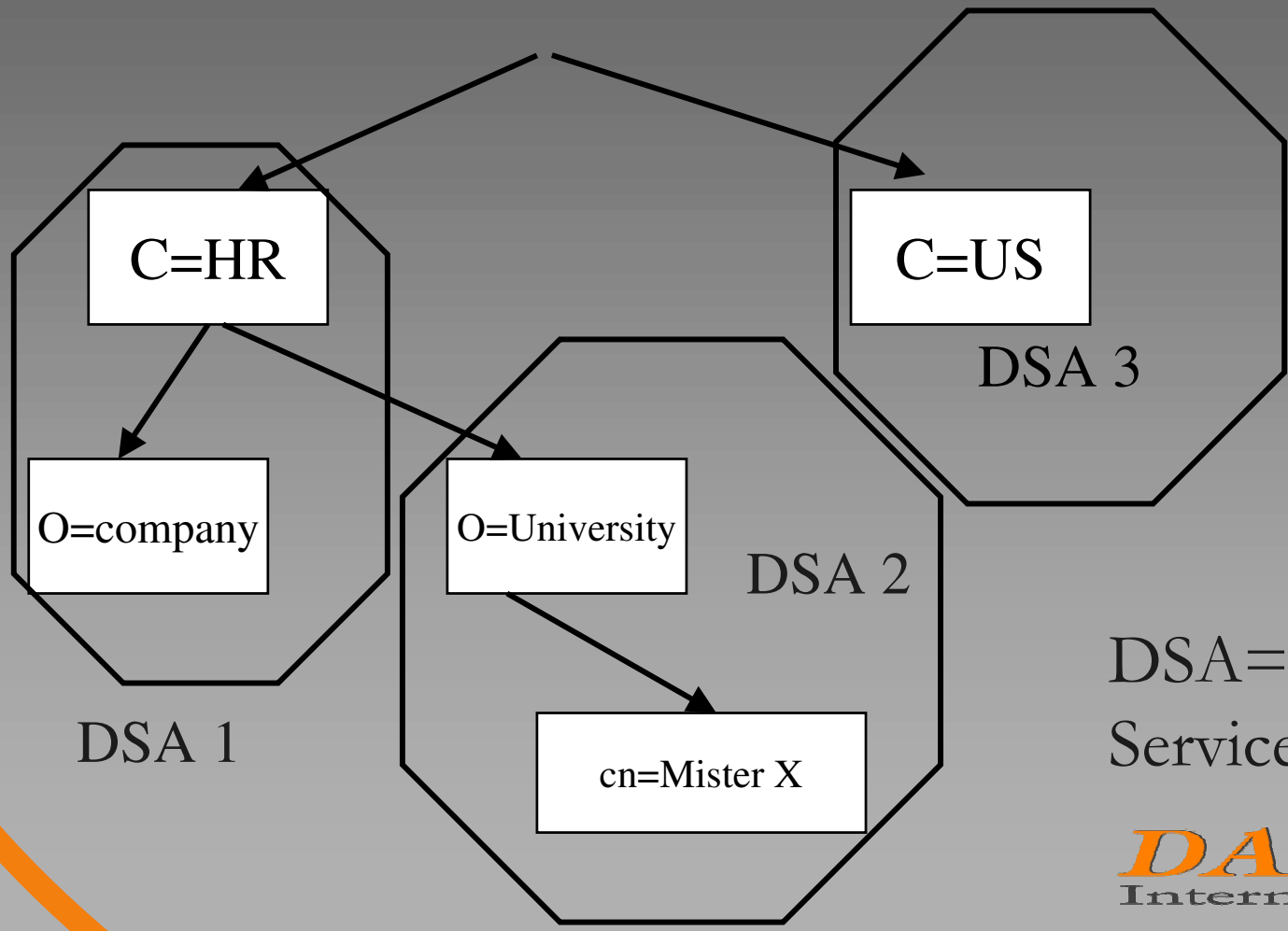
Open structure

- You can define your own:
  - Object Classes
  - Attribute Types
  - Attribute Syntaxes
  - Matching Rules
- You can locally use self defined schemas
- If you want them to be used globally you have to
  - standardize them (IETF)
  - or at least register them

DAASI International

Directory Applications for Advanced Security and Information Management

Distribution of the data among Servers



DSA=Directory Service Agent

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP Features

- The LDAP standard defines...
  - a network protocol for accessing information in the directory
  - an information model defining the form and character of the information
  - a namespace defining how information is referenced and organized
  - secure authentication mechanisms
  - an emerging distributed operation model defining how data may be distributed and referenced (v3)
  - Both the protocol itself and the information model are extensible
  - A C API and a Java API

DAASI International

Directory Applications for Advanced Security and Information Management

LDAP Functional Model

- Authentication and control operations:
  - bind
  - unbind
  - abandon
- Interrogation operations:
  - search
  - compare
- Update operations:
  - add
  - delete
  - modify
  - modifyDN

DAASI International
Directory Applications for Advanced Security and Information Management

LDAPv3 Extension mechanisms

- LDAP controls
  - All 9 LDAP operation (bind, search, add, ...) can be extended
  - controls modify behavior of operation
  - client and server must support the control

DAASI International

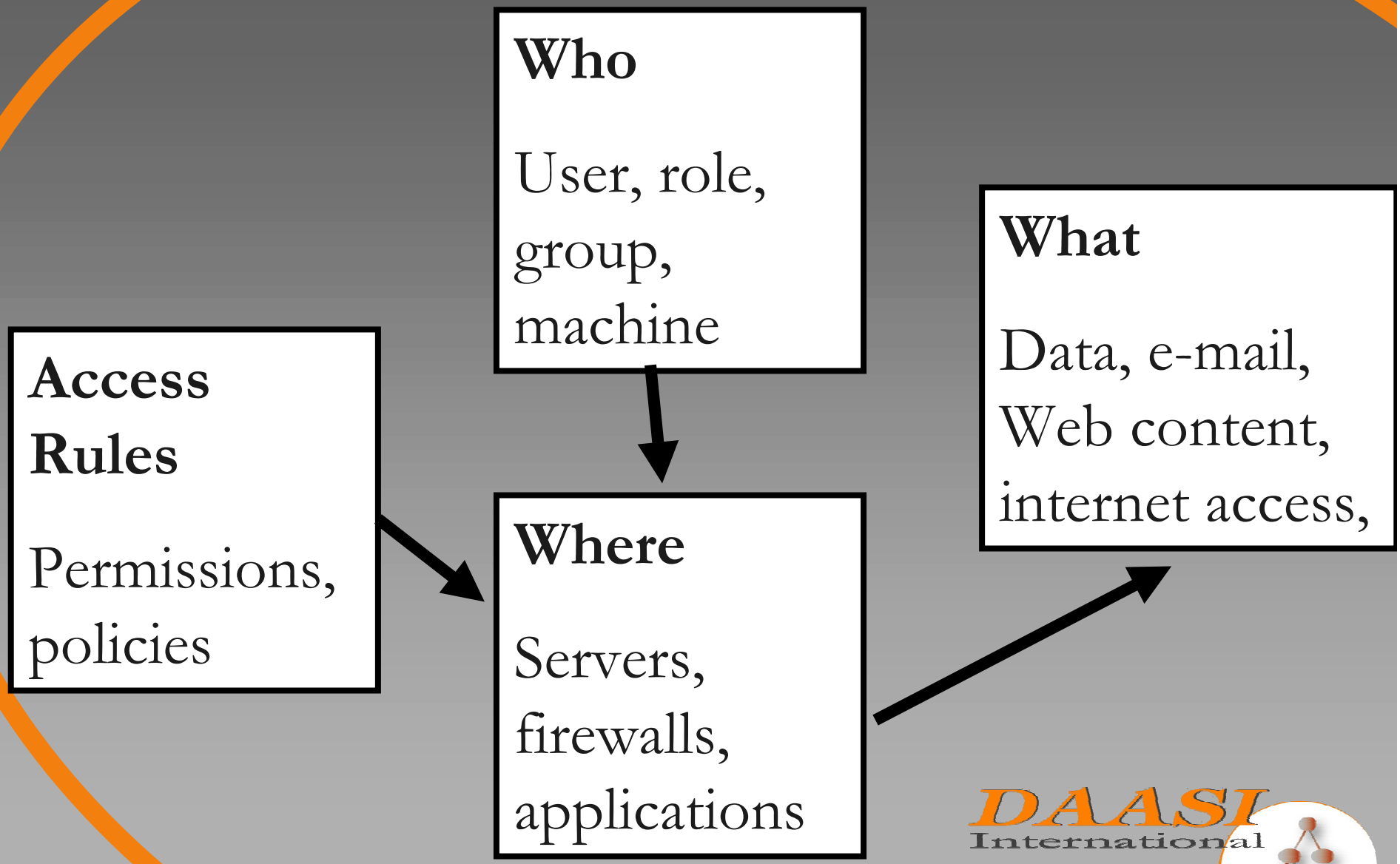
Directory Applications for Advanced Security and Information Management

LDAPv3 Extension mechanisms contd.

- LDAP extended operations
  - New defined protocol operation in addition to the nine
- SASL mechanisms
  - Simple Authentication and Security Layer
  - Framing for support of different authentication mechanisms

DAASI International
Directory Applications for Advanced Security and Information Management

Access Control



DAASI International
Directory Applications for Advanced Security and Information Management

From RL Morgan, PKI Standards Overview

LDAP Data Interchange Format LDIF

- RFC 2849:
- Format for exchanging data
- Example:

```
dn: cn=Mister X, o=University, c=NL
objectclass=top
objectclass=person
objectclass=organizationalPerson
cn=Mister X
cn=Xavier Xerxes
mail=X@dot.com
mail=Mister.X@dot.com
telephoneNumber=1234567

dn: cn=next entry, ...
```

DAASI International

Directory Applications for Advanced Security and Information Management

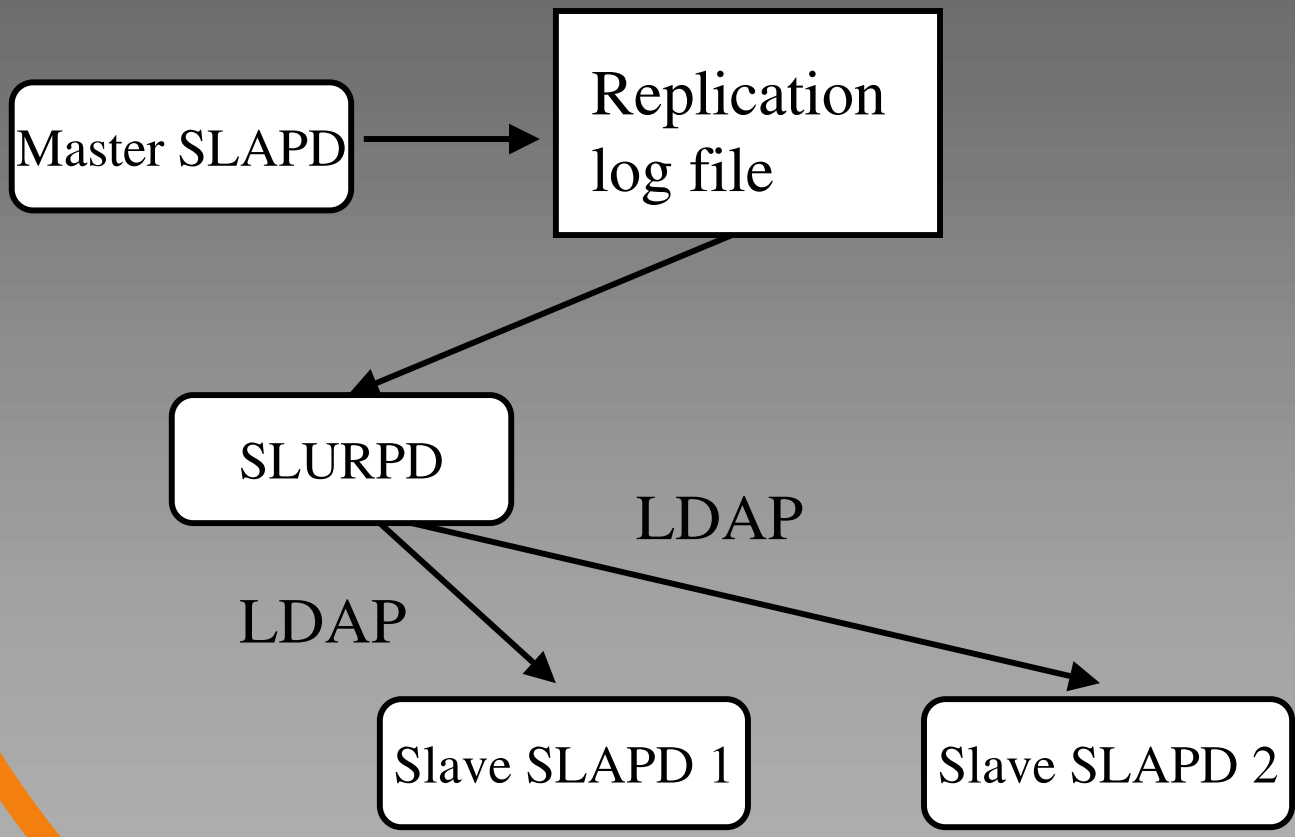
Replication

- Vital missing part in LDAP standardization
- Needed to really replace X.500
- Current LDAP implementations have
  - Either proprietary replication mechanisms
  - Or stick to the pseudo standard of University of Michigan implementation (SlurpD)
  - Or just use plain LDIF
  - New possibility: XML (DSML)

DAASI International

Directory Applications for Advanced Security and Information Management

Non Standard LDAP Replication



DAASI International
Directory Applications for Advanced Security and Information Management

Replication log file format

```
replica: host1.hu:9999
replica: host2.hu:8888
time: 960373276
dn: cn=Mister X, o=University, c=HU
changetype: delete

replica: host1.hu:9999
replica: host2.hu:8888
time: 960373277
dn: cn=Mister X, o=University, c=HU
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Xavier Xerxes
mail=X@dot.com
mail=Mister.X@dot.com
telephoneNumber=1234567
```

DAASI International

Directory Applications for Advanced Security and Information Management

Who talks LDAP?

- All directory implementations have an LDAP interface:
  - all X.500(93) implementations
  - Novell Directory Service (NDS)
  - Microsoft Active Directory (AD)
- Many client applications have an LDAP interface:
  - mailagents
  - browsers
  - PGP clients

DAASI International
Directory Applications for Advanced Security and Information Management

Who talks LDAP? (contd.)

- Many Programs use LDAP for user authentication
  - SMTP auth for outgoing emails
  - IMAP Servers for managing emails
  - Apache Webserver
  - …

DAASI International

Directory Applications for Advanced Security and Information Management

More Information on LDAP ?

- Go to the the Workshop ! ;-)
  - Today 15:00-17:00
  - *Room: TCR*
  - Beware: you will see some slides again that you have seen here

DAASI International

Directory Applications for Advanced Security and Information Management

LDAP based Directory Services 1

Classical Services

DAASI International

Directory Applications for Advanced Security and Information Management

Classical Services 1

- Contact information of people
  - Name, address, telephone number, email address, ...
  - White Pages Directory Service
- Contact information of Organisations
  - Organisational structure, addresses, telephone numbers, email address, ...
  - Yellow Pages Directory Service

DAASI International
Directory Applications for Advanced Security and Information Management

Classical Services 2

- User management
  - Network Information Service
    - replacement of Unix /etc/passwd, groups, services, etc.
  - Authentication service
    - Unified login
    - Web authentication etc.

DAASI International
Directory Applications for Advanced Security and Information Management

BTW: Good News!

- You can build up different Services with the same data
  - E.g. combine White Pages, Yellow Pages and User management in one Directory Information Tree on one or several Servers
  - Just add appropriate Objectclasses and data to your entries and set up a new user interface to the new data
  - This sincerly reduces management costs!

DAASI International

Directory Applications for Advanced Security and Information Management

LDAP based Directory Services 2

Indexing for providing central services on distributed data

DAASI International

Directory Applications for Advanced Security and Information Management

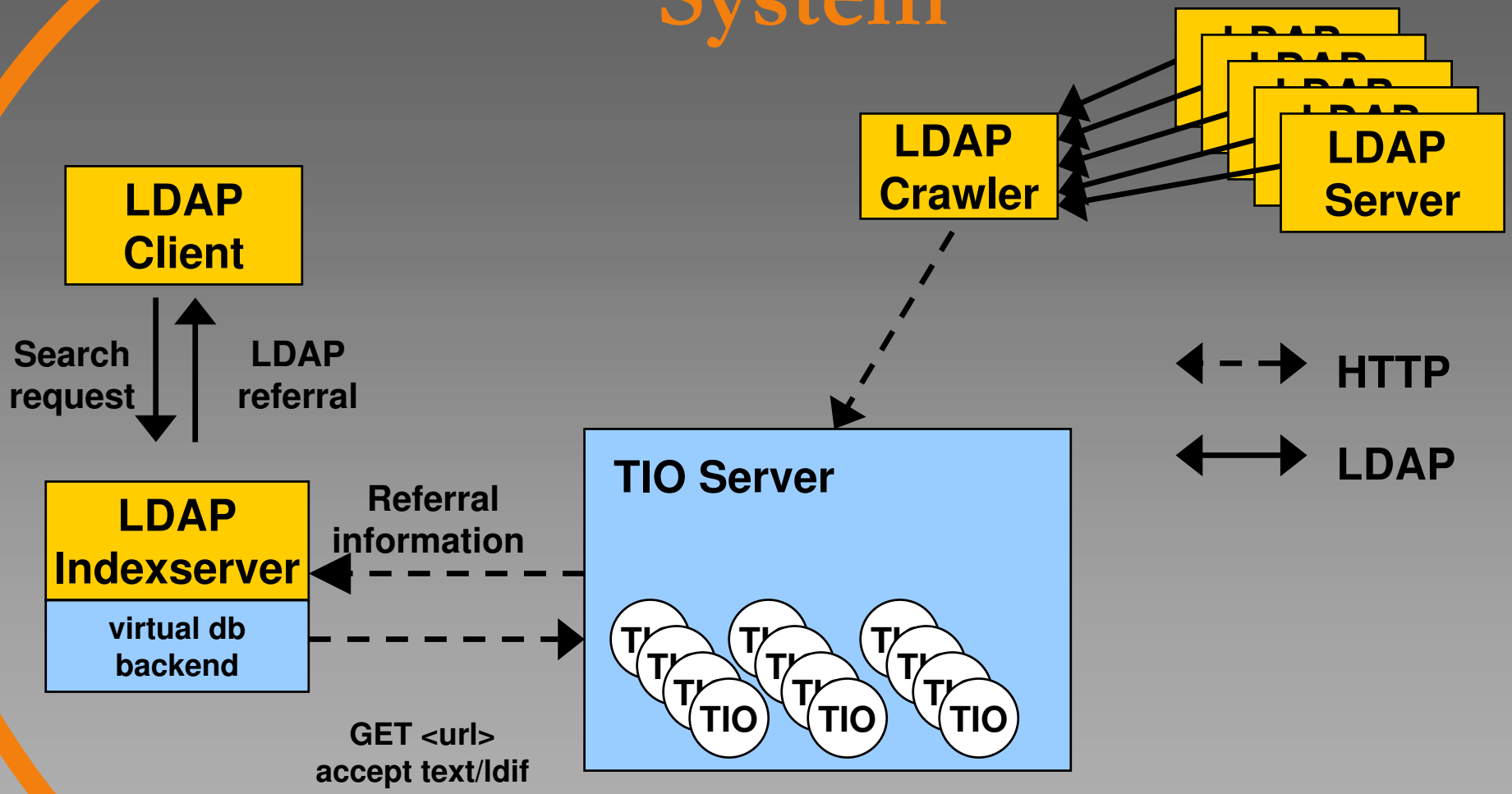
Common Indexing Protocol CIP (RFC 2651 – 2655)

- Index definitions for any directory technology
- Index meshs
- MIME wrapper
- Several Transport protocols (email, FTP, HTTP)
- Several Index Object Formats
  - E.g.: Tagged Index Object (TIO)

DAASI International

Directory Applications for Advanced Security and Information Management

The LDAP Indexing System



DAASI International
Directory Applications for Advanced Security and Information Management

What can the index system be used for?

- White Pages Service
- Metadata Service
- Certificate Service
- Every wide scale service on distributed data

DAASI International

Directory Applications for Advanced Security and Information Management

LDAP based Directory Services 3

Public Key Infrastructure

PKI and Directory

The Burton Group: Network Strategy Report, PKI Architecture, July 1997: (Quoted after: S. Zeber, X.500 Directory Services and PKI issues, http://nra.nacosa.nato.int/pki/hdocs/pkiahwg30/index.htm)

" ... Customers should always consider PKI a directory-enabled set of services and infrastructure. Without directory services, PKI will be exponentially harder to implement and manage. Consequently, customers should't deploy PKI widely without an accompanying directory plan"

DAASI International

Directory Applications for Advanced Security and Information Management

Directory as Key Server Requirements

- Publishing medium for public keys and certificates
- Gets public keys from user
- Gets certificates from CA
- Documents revocation of keys/certificates (CRL)
- Documents status of a certificate at a specific time

DAASI International

Directory Applications for Advanced Security and Information Management

Motivation

- Address problem of multiple certificates for one entity
  - How can the client find the right certificate?
- Find a simple and easy to implement solution
- Solution should be usable in the frame of a large scale distributed LDAP / Common Indexing Protocol (CIP) based certificate repository

DAASI International

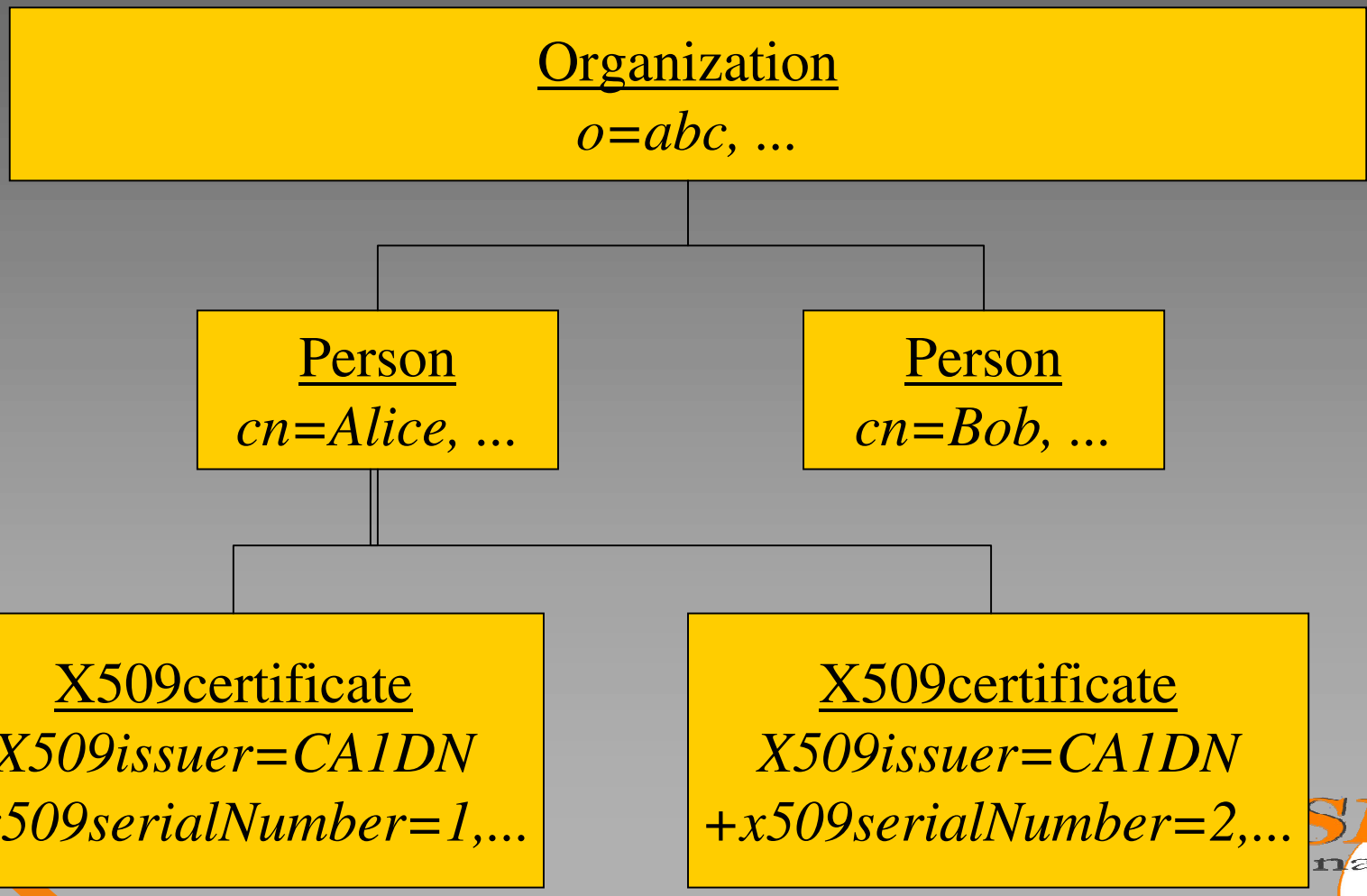
Directory Applications for Advanced Security and Information Management

Schema as a simple solution

- Find a set of certificate fields and extensions that one might want to search upon
  - Meta-data approach
- Parse the certificate and store this set as LDAP attributes
- Advantages:
  - no new server features needed
  - easy to implement in clients
  - usable in a CIP environment

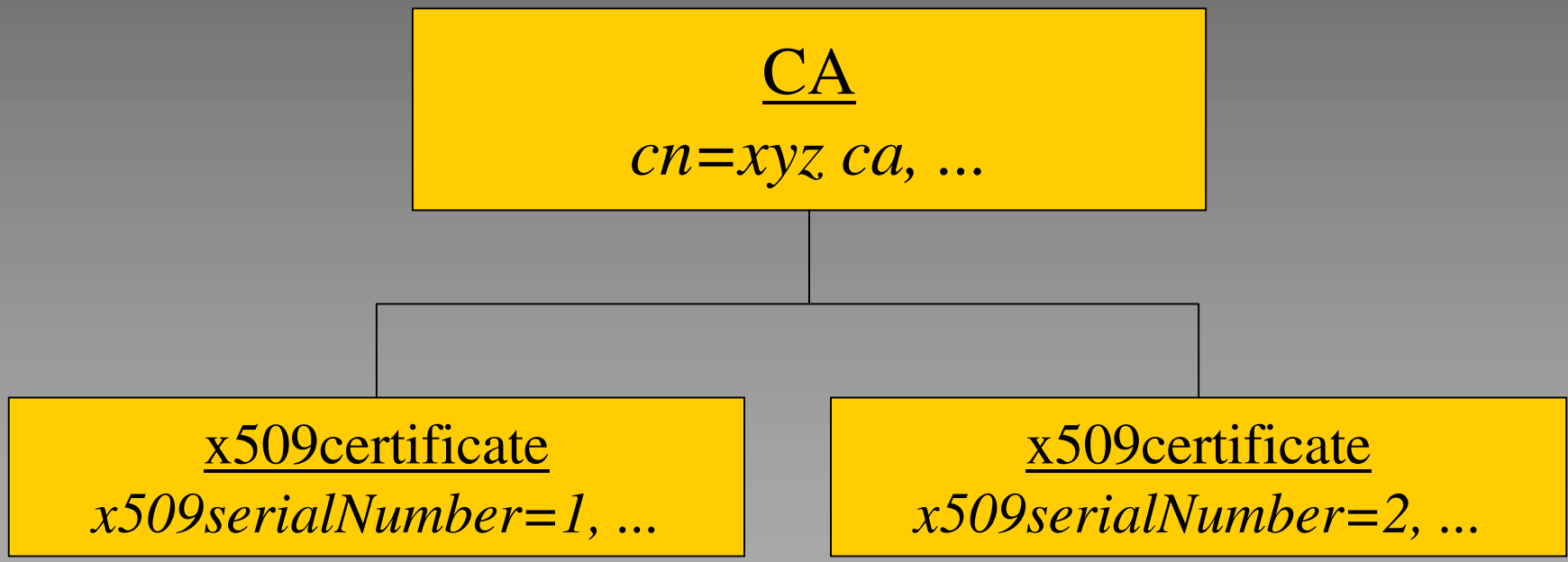
DAASI International
Directory Applications for Advanced Security and Information Management

DIT Structure in white-pages services



Directory Applications for Advanced Security and Information Management

DIT Structure in certificate repositories



DAASI International
Directory Applications for Advanced Security and Information Management

LDAP based Directory Services 4

Metadata Service and the Semantic Web

DAASI International

Directory Applications for Advanced Security and Information Management

Metadata

- Easiest definition: Data about data, e.g.:
  - Data: Texts, i.e. anything that tells us some kind of story (books, articles, webpages, films, etc.)
  - Metadata: Information about the texts (author, title, date of creation, etc.)
- There is one kind of Metadata that is really complicated: Keywords
  - How can we be sure that we use the same keywords for describing the same topics?
  - Controlled vocabularies!

DAASI International
Directory Applications for Advanced Security and Information Management

Controlled Vocabulary

- Classification System
  - E.g. Dewey Decimal Classification
  - Classes, subclasses, subsubclasses, ...
  - One kind of relation between concepts
- Thesaurus
  - Assembly of homonyms
  - Could include antinyms and some more relations
  - A limited set of relations between concepts

DAASI International

Directory Applications for Advanced Security and Information Management

Ontologies

- Again: Concepts and relations between them
- No limitation as to the number of different relations
  - Including sub/superclass
  - Including relationships of thesauri
  - ...
- Thus a perfect knowledge store

DAASI International

Directory Applications for Advanced Security and Information Management

Current WWW

- Mere publishing medium
- Huge amount of information
- Designed for human access only
- Lack of structure and organization
- Insufficiant access methods
- Ambiguous:
  - bank (finance institute) the same as
  - Bank (river bank)

DAASI International

Directory Applications for Advanced Security and Information Management

Visions for the future

- „Semantic Web“ (Tim Berners-Lee)
- Web Services (see below)
- Accessed by humans *and* programs
- Quality content better structured
- Knowlegde enhanced through Ontologies
- Disambigued:
  - Bank (finance institute) is not the same as
  - Bank (river bank)

DAASI International

Directory Applications for Advanced Security and Information Management

How can Ontologies help?

- Remember: Concepts and relations between them
- Computer knows more than inputed

```
Input: Parents have children
Input: Mother = female parent
Output: Mothers have children
```

DAASI International
Directory Applications for Advanced Security and Information Management

Ontologie Storage Proposal

- Combined repository for metadata and ontologies
  - based on LDAP technology
  - thus accessible with the same protocol
- Large scalability
  - by setting up an Indexing system
  - based on Common Indexing Protocol (CIP)

DAASI International

Directory Applications for Advanced Security and Information Management

Ontologie Storage Proposal

- Ontologie data model based on Common Information Model (CIM)
  - provides a model for associations that can be used for mapping the relations between objects
  - CIM is commonly used in Resource management and for Policy data
  - Technology independant modelling language (sort of UML)
  - Mappings to e.g. LDAP and XML

DAASI International

Directory Applications for Advanced Security and Information Management

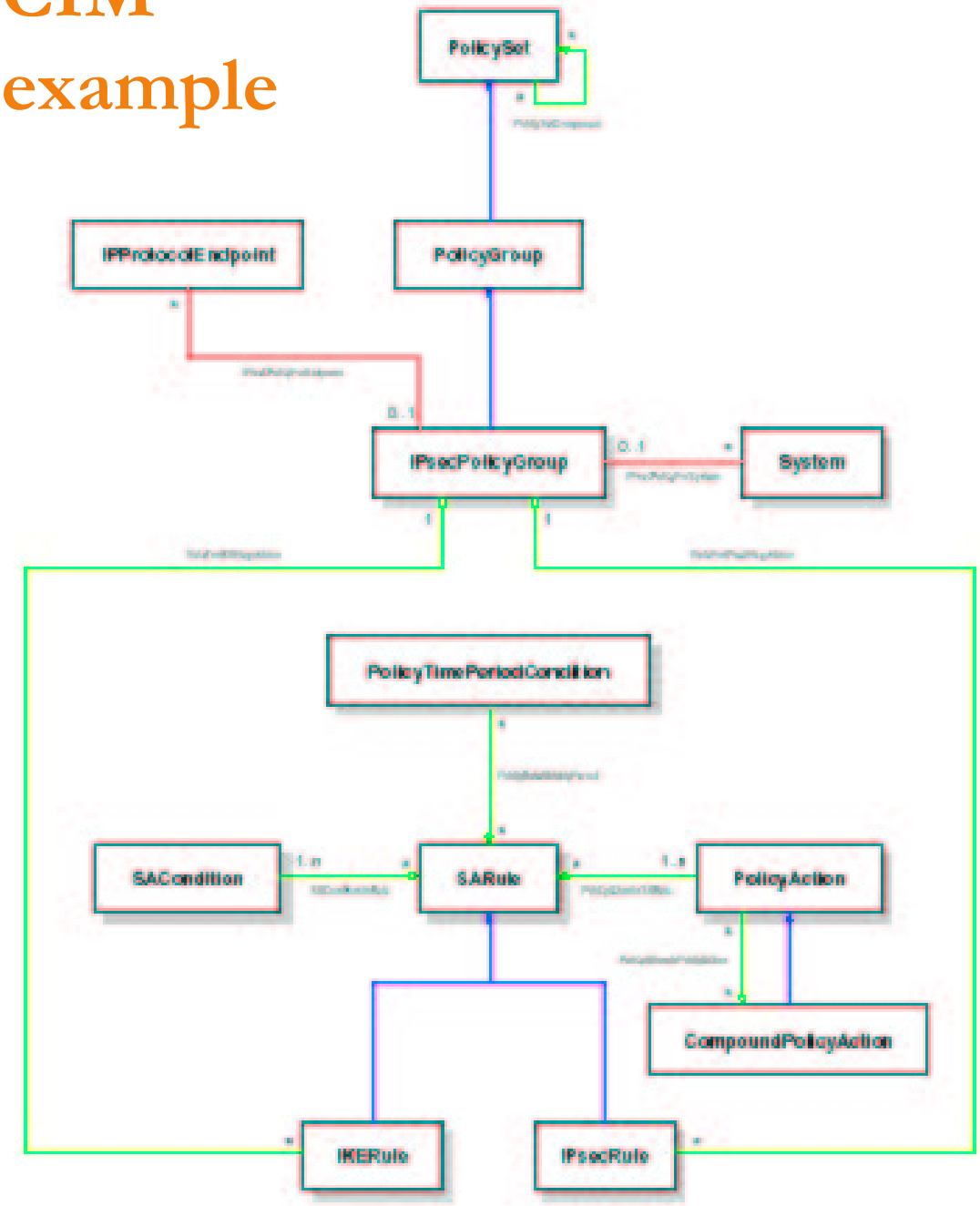
Common Information Model

- Object oriented meta model for structuring information technology independantly
- Capable of describing the whole computer world
- Basically an Ontology
- Three layers
  - Core: the basic lego bricks
  - Common: standardized descriptions
  - Extesion: vendor‘s extras

DAASI International

Directory Applications for Advanced Security and Information Management

CIM example



objects

inheritance

aggregation

association

DAASI International

Directory Applications for Advanced Security and Information Management

CIM, LDAP and Ontologies

- Any kind of relations can be defined with CIM and mapped to LDAP
- LDAP provides:
  - Object Class inheritance
  - Attribute inheritance
- Associations and aggregations can be mapped by object classes

DAASI International

Directory Applications for Advanced Security and Information Management

Apropos Web Services

- SOAP
  - Simple Object Access Protocol
  - XML based Remote Procedure Calls
- WSDL
  - Web Services Description Language
  - XML based Interface description
- UDDI
  - Universal Description, Discovery and Integration
  - Repository for WSDL descriptions
  - Can be well replaced by LDAP

DAASI International

Directory Applications for Advanced Security and Information Management

LDAP based Directory Services 5

Policy repository

DAASI International

Directory Applications for Advanced Security and Information Management

Policy repository

- Policy for Routers defining which packets to priortise, if and how to check authenticity, etc.
- Based Common Information Model (CIM)
- Directory Enabled Networks (DEN)
  - Quality of Service (QoS)
- IPSec policy
  - IETF WG IPSecpol
- Any other policies

DAASI International

Directory Applications for Advanced Security and Information Management

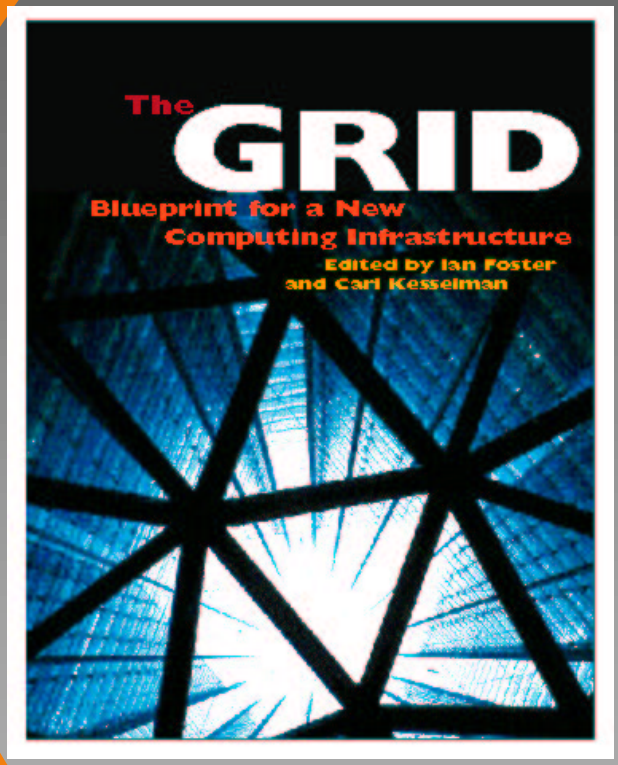
LDAP based Directory Services 6

- Information for Grid Computing

DAASI International

Directory Applications for Advanced Security and Information Management

The book



- Ian Foster, Carl Kesselmann (Ed)
  The Grid: Blueprint for a new Computing Infrastructure
  Morgan Kaufman Publishers, 1998
  - a summary of the state of the art of super computing,
  - now seen as the beginning of a new vision

DAASI International
Directory Applications for Advanced Security and Information Management

The metapher

- Power Grid is a complex infrastructure that has a very simple user interface: the power outlet. Everything else is hidden from the user
- Grid Computing wants to provide an equally simple interface to computing power (CPUs, data storage, etc.) from the network.

DAASI International

Directory Applications for Advanced Security and Information Management

Definitions

„The Grid is a consistent and standardized environment for collaborative, distributed problem solving that requires high performance computing on massive amounts of data that are stored, and/or generated at high data rates using widely distributed, heterogeneous resources „

„The Grid is an inherently layered architecture that provides for common services and a diversity of middleware that supports building distributed, large-scale, and high performance applications and problem solving systems. „

(W.E. Johnston as quoted by Ian Foster)

DAASI International

Directory Applications for Advanced Security and Information Management

The tasks

- Distribution of data and computing ressources in broadbandwith networks to be able to provide petabyte storage and petaflops computing power
- Promotion of international collaboration
- Optimal utilization of resources (storage, CPUs, measuring devices, experimental devices

DAASI International

Directory Applications for Advanced Security and Information Management

What is new?

- Metacomputing is in existance for quite a while
- New is the concept of standardized interface to meta computing, the so called Middleware
- The Global Grid Forum (GGF) took up the task to create such standards in an IETFish way
- Complicated requirements: “Run program X at site Y subject to community policy P, providing access to data at Z according to policy Q”

DAASI International

Directory Applications for Advanced Security and Information Management

Requirements

- High bandwidth between powerfull systems
  - To specify simulations, initiate and steer computation
- Security
  - Use Encryption, Certificates, Single sign on
  - To Authenticate, negotiate and delegate authorization
- Data management
  - Use Distribution, Replication, Metadata
  - To locate and acquire resources, access remote datasets, collaborate on results

DAASI International

Directory Applications for Advanced Security and Information Management

Grid Resource Information Service

- (Dynamic) Information about specific resources:
  - Load, process information, storage information, etc.
- Supports multiple information providers
- Answers questions like:
  - How much memory does machine have?
  - Which queues on machine allows large jobs?
- LDAP is an ideal technology

DAASI International

Directory Applications for Advanced Security and Information Management

Replica management

- Maintain a mapping between logical names for files and collections and one or more physical locations
- replica cataloging and reliable replication as two fundamental services
  - LDAP is used as catalog format and protocol, for consistency
  - LDAP object classes for representing logical-to-physical mappings in an LDAP catalog

DAASI International
Directory Applications for Advanced Security and Information Management

New Trends in Grid Computing

- Web Services (see above)
  - Open Grid Services Architecture (OGSA)
  - Using SOAP and WSDL
  - A whole set of new GGF working groups
- CIM (see above)
  - Used for modeling grid related data
  - New working group on modelling Job Submission Information
  - CIM will be integrated in OGSA

DAASI International

Directory Applications for Advanced Security and Information Management

Visions for the future

DAASI International

Directory Applications for Advanced Security and Information Management

Well ....

- Almost everything I told you about is in status nascendi
- I didn‘t mention the term middleware
  - Lets have a short definition here:
  - A software layer between the network and network applications that provides standardized interfaces to commonly needed services

DAASI International

Directory Applications for Advanced Security and Information Management

The Vision

- Globally used LDAP based Middleware that provides:
  - The same Authentication services to different applications
  - Ontology information to intelligent services
  - Information about automated services to agents
  - Policy information to network devices for intelligent routing

DAASI International

Directory Applications for Advanced Security and Information Management

The good news:
we are allmost there!

Questions?

- DFN Directory Services
  - peter.gietz@directory.dfn.de
  - www.directory.dfn.de
- DAASI International GmbH
  - Info@daasi.de
  - www.daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management