OpenCA and LDAP Authentication and LDAP based certificate requests

OpenCA Workshop, TU München, 18.11.2005

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management

Agenda

- Why Identity Management
- LDAP authentication in OpenCA
- LDAP based certificate request generation

DAASI International
Directory Applications for Advanced Security and Information Management

What is Identity Management?

- **Spencer C. Lee:**
  - ***Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials.***

DAASI International
Directory Applications for Advanced Security and Information Management

Why Identity Management?

- Publication of data about a person (White Pages Service)
- Non redundant data managementof staff data
- Consistency of data
- Fast automated provisioning of resources
- Fast automated deprovisioning after person leaves the organization
- Better inter domain communication: federated identity management (liberty, shiboleth, ws-fed)

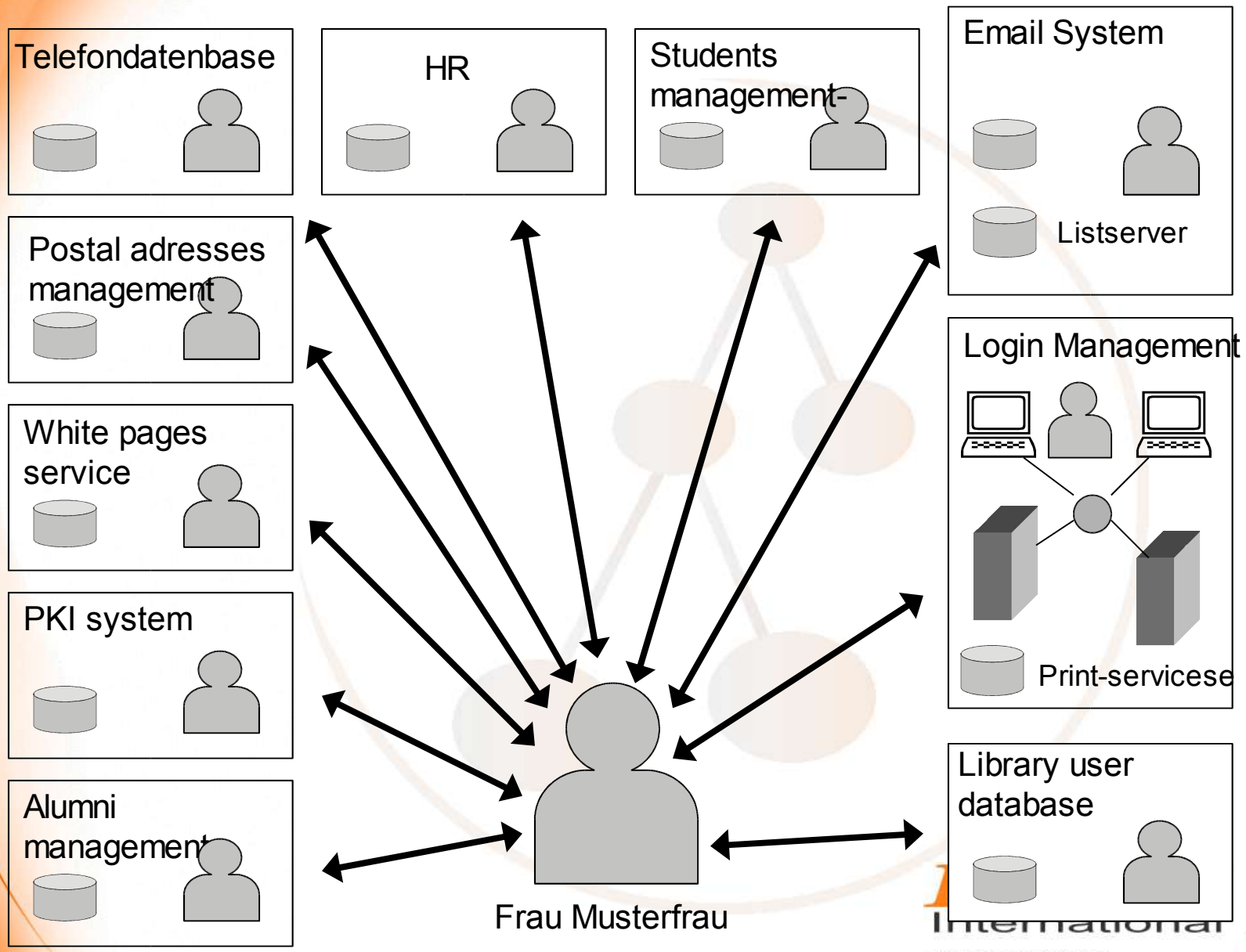
DAASI International
Directory Applications for Advanced Security and Information Management

A few numbers from the Meta Group

- Meta Group: The Value of Identity Management:
- In Enterprises with over $500 Millionen revenue:
  - 45% of help desc activities is resetting passwords
  - 11% of employees have at least one access right problem per month
  - Provisioning processes need between 6 and 29 hours
  - Information about users is stored at 22 different data stores

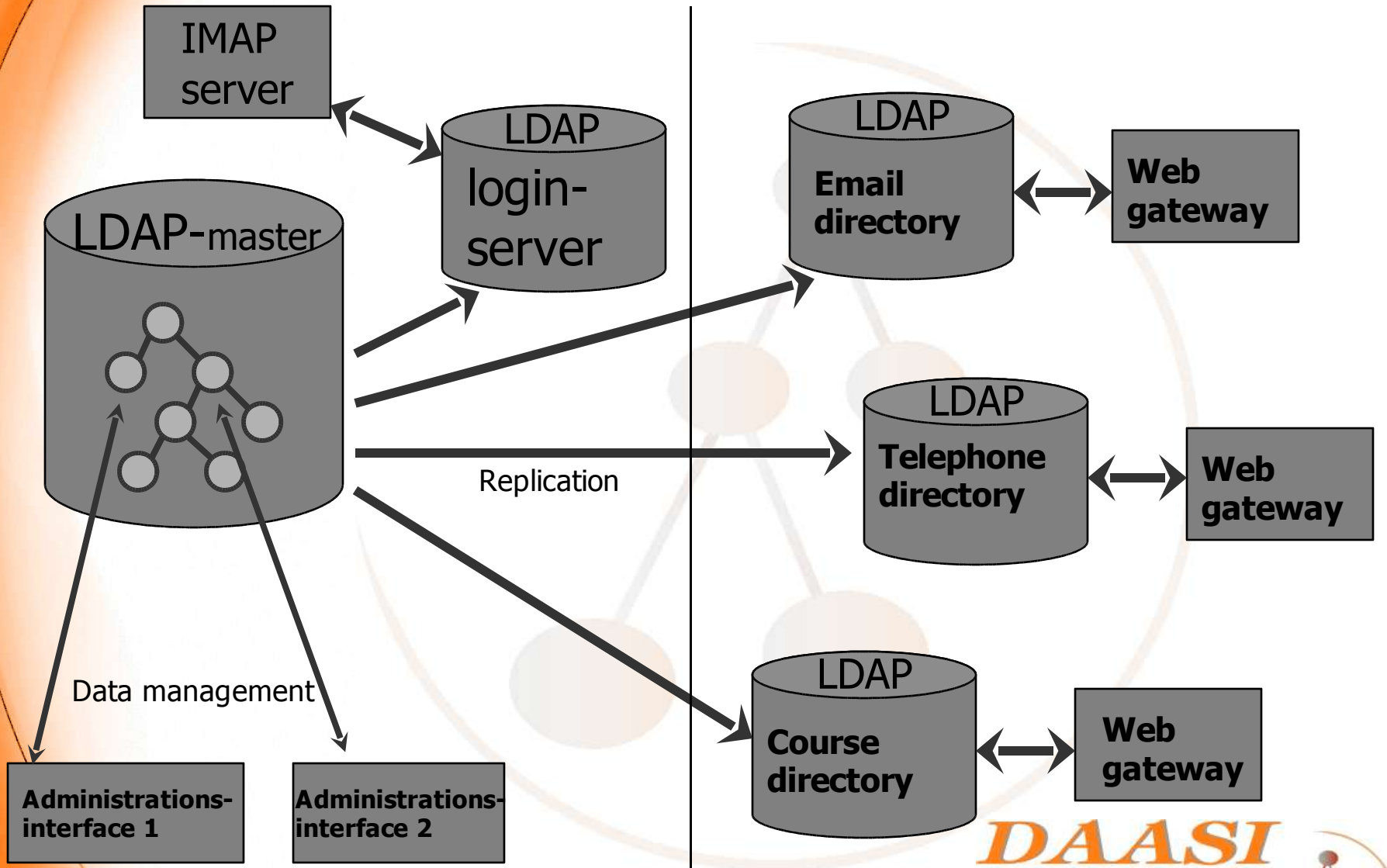
DAASI International
Directory Applications for Advanced Security and Information Management

Worst Case Scenario at an University



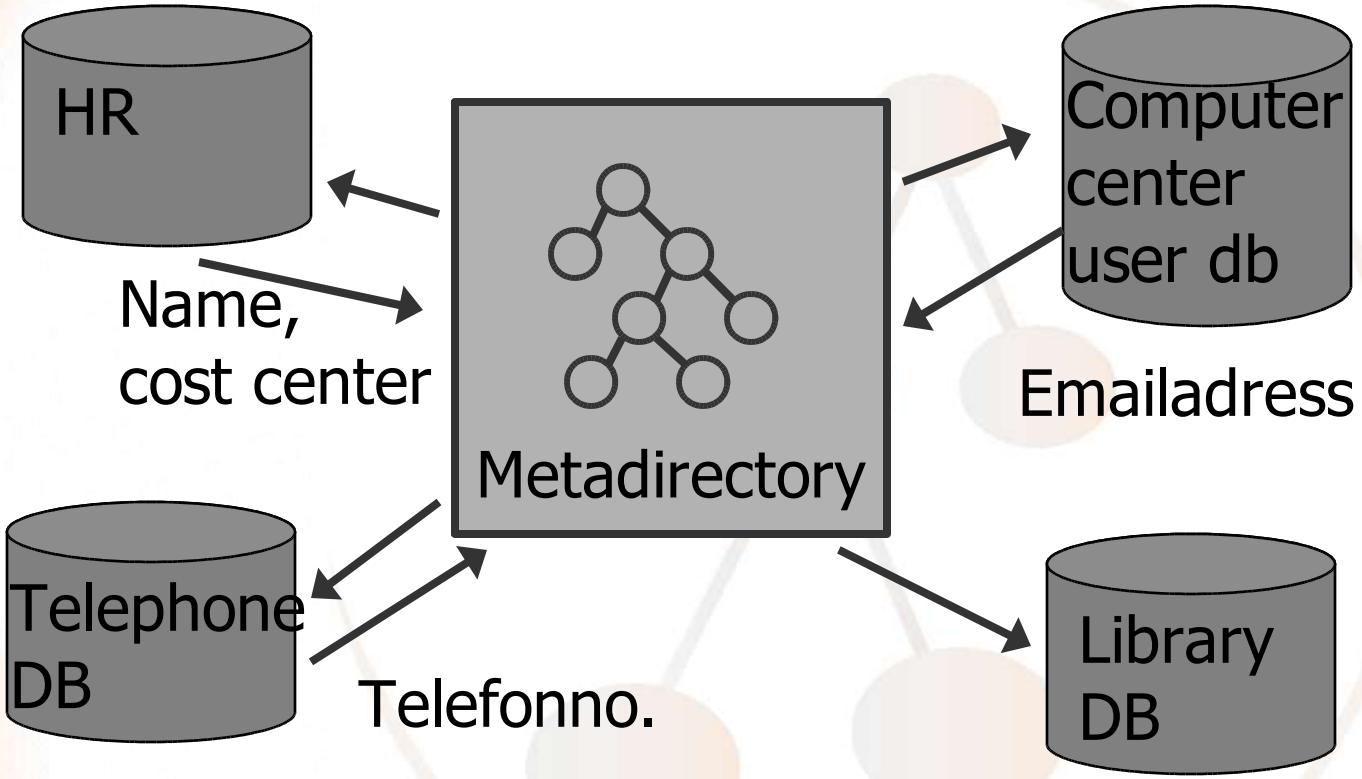
Directory Applications for Advanced Security and Information Management

Central directory for a number of services



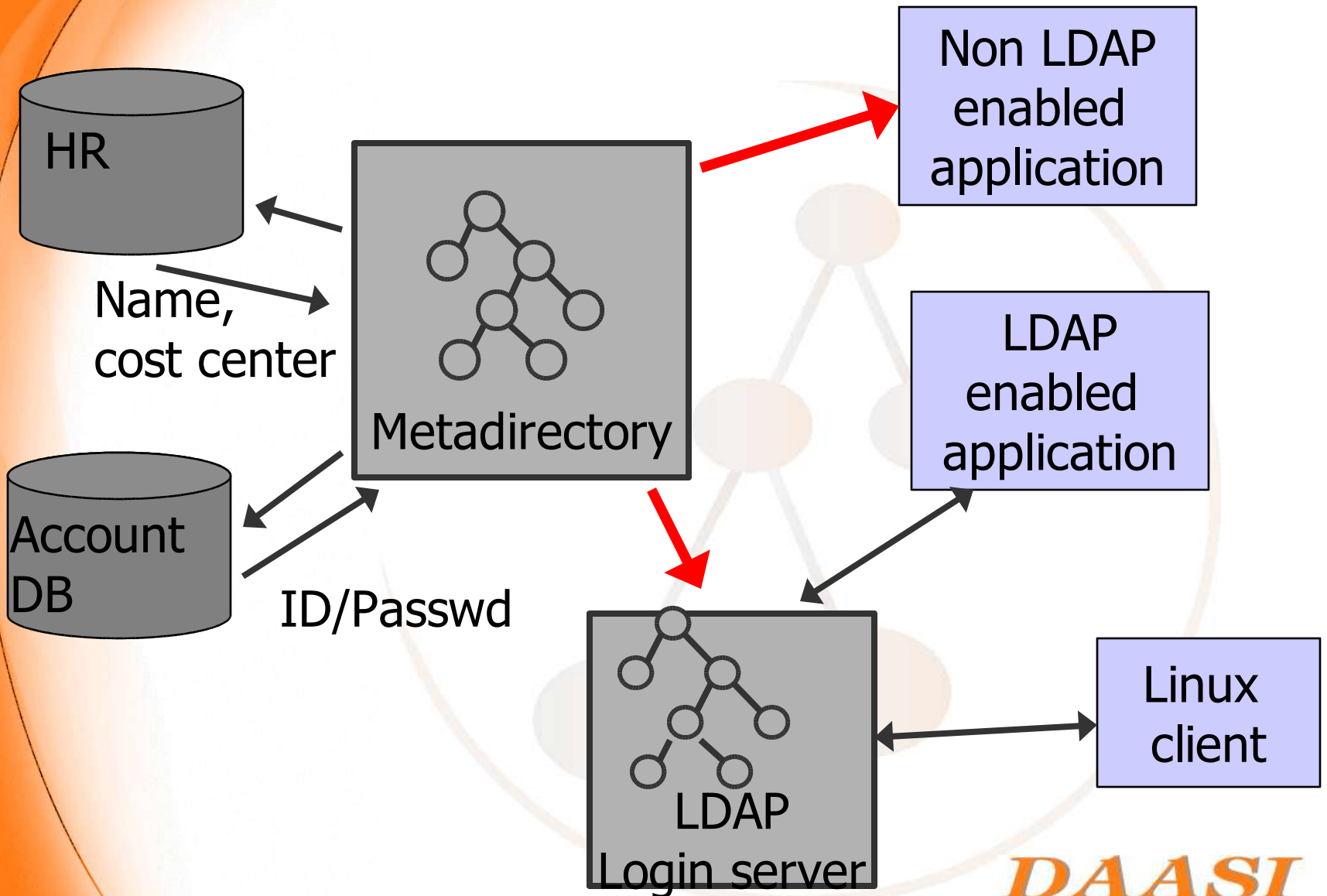
DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory solution



DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory with provisioning



DAASI International
Directory Applications
for Advanced Security
and Information Management

Provisioning vs. LDAP enabling

- Provisioning
  - causes additional data redundancy
  - Heterogeniuos Security mechanisms with different strengths
  - Password changes are more complicated (different hashes)
- LDAP enabling
  - Possible in any Open Source product
  - Quite simple to do because of good LDAP libraries
  - Password changes easy
  - LDAP has a variety of strong and well established authentication methods
  - De facto standard for network applications

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP Authentication in OpenCA

- Done for a customer with a mediumsized PKI
- Integration of the central Active Directory
- Different users should be able to use different authentication mechanisms:
  - Those with windows accounts
  - Those without
- Role data were also to be retrieved from LDAP/AD
- Additional integration by using LDAP for retrieving all non configural data for certificate requests
  - Yes the point in the PKI work flow where users make a lot of mistakes

DAASI International
Directory Applications for Advanced Security and Information Management

Implementation of LDAP authentication in OpenCA

- OpenCA already uses LDAP for certificate publication
- Nevertheless authentication information could be stored in a different LDAP server
- It could all be done in the access control module AC.pm
  - Good design of OpenCA software
- It was done with OpenCA 0.9.2.2
- I now tested it with OpenCA 0.9.2.4
  - Just replaced the AC.pm and configured the interface, e.g. .../etc/access_control/ra.xml

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration example

```
<openca>
 <access_control>
   <channel> ... </channel>
   <login>
     <type>passwd</type>
       <database>ldap</database>
       <ldapdata>
<!-- first you have to specify the LDAP server used: -->
          <host>smb.daasi.de</host>
          <port>389</port>
          <base>o=smb,dc=daasi,dc=de</base>
          <binddn>cn=admin,o=smb,dc=daasi,dc=de</binddn>
          <bindpw>secret</bindpw>
        ...
```

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration example

should the communication to the ldap server be encrypted via TLS? If so you need to store the cacertificate for authenti cating the LDAP server into the directory specified here

<usetls>yes</usetls>
<cacertpath>/opt/</cacertpath>

What is the attribute to search the name/ID for?

<searchattr>uid</searchattr>

Some LDAP/AD Attributes have some characters in front of the actual value that should be ignored in searches, e.g. the attribute proxyAddresses has strings determing the protocol like "SMTP:misterx@foo.bar". In this case you would want to configure SMTP: in searchvalueprefix, so your users will not have to care about it

<searchvalueprefix/>

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration example

There are different methods for authenticating with LDAP. This module supports two by now.

1.) bind (using the password stored in attribute userPassword)
2.) pwattr (using the password stored in a freely configurable attribute, see below)

You can use both methods in parallel, but then the module must know which method to use for which entries. This can

be defined by values of a certain attribute, which can be defined in the configuration as ldapauthmethattr:

<ldapauthmethattr>userType</ldapauthmethattr>

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration example

Then you must define which values of that attribute should lead to which authentication method. A good example would be to take the attribute objectClass as ldapauthmethattr and say if the entry contains the objectclass posixaccount to use the ldap bind method, if it contains objectClass externalUser to use pwattr. Such mappings can be done with the following structures:

```
<ldapauthmethmapping>
 <ldapauthmethattrvalue>intern</ldapauthmethattrvalue>
   <ldapauthmeth>bind</ldapauthmeth>
</ldapauthmethmapping>
<ldapauthmethmapping>
<ldapauthmethattrvalue>extern</ldapauthmethattrvalue>
  <ldapauthmeth>pwattr</ldapauthmeth>
</ldapauthmethmapping>
```

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration example

If none of the conditions configured here are fulfilled by an entry, a default mechanism has to be used, which is configured here:

```
<ldapdefaultauthmeth>bind</ldapdefaultauthmeth>
```

For the pwattr method you need to specify which attribute contains the passwords to use. This is done here:

```
<ldappwattr>myPasswd</ldappwattr>
```

The values in that attribute can and should be stored as hash values. If so, the module needs to know which hashing algorithm was used. supported are: sha1, md5, crypt and none (=clear text)

```
<ldappwattrhash>sha1</ldappwattrhash>
</ldapdata>
```

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration example

<passwd>

The LDAP Login module also provides for role mapping, where certain values of a certain attribute map to certain OpenCA roles. first you have to specify which LDAP attribute contains the role mapping information:

<roleattribute>businessCategory</roleattribute>

Now you can easily define the mappings (as known from the above authmethmapping):

<rolemapping>
<roleattributevalue>RA Admin</roleattributevalue>
<role>RA Operator</role>
</rolemapping>
</passwd>

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration gimmicks

you might want to have an self defined headline in stead of "Login to OpenCA". You can specify the new string here:

<loginheadline>Login using LDAP authentication</loginheadline>

You might also want to have a different text for prompting the login name of the user in stead of "login", indicating what type of ID info is requested:

<loginprompt>SMTP Email-Adresse</loginprompt>

</login>
</access_control>
</openca>

DAASI International
Directory Applications for Advanced Security and Information Management

Implementation status

- Done this in a slightly specialized way for a custumer
  - Used in ready for production service
- Made a slightly more general version for contribution to OpenCA
  - Including documentation
  - Including gettexts for all additional error strings etc.
  - Including well documented config example
- Posted to core developpers (quite some time ago)
  - Will it be included into 0.9.2.4?
- For the next generation code I am afraid that some patches will have to be done
  - New access control paradigm

DAASI International
Directory Applications for Advanced Security and Information Management

More LDAP Integration

- If LDAP/AD is the main repository for staff information
  - It makes sense to automate the certificate request
  - Additional role handling would be possible
- In the same project we created a new command for this (based on some proof of concept code from Michael)
  - ldapAutoCreateCSR
- Not yet generalized but yet the customer software
  - Thus not yet contributed
  - Will be done within a new customer project

DAASI International
Directory Applications for Advanced Security and Information Management

Configuration of ldapAutoCreateCSR

```
## ==================== [ Begin LDAP based CSR Section ] ===
LDAP_BASED_CSR_GENERATION "AUTO"

DN_TYPE_LDAP_KEYGEN_MODE  "SERVER"
DN_TYPE_LDAP_KEYSIZE 2048
DN_TYPE_LDAP_PINGEN "AUTO"
DN_TYPE_LDAP_PASSWDGEN "PIN"

DN_TYPE_LDAP_SECURE_PIN_LENGTH 22
DN_TYPE_LDAP_SECURE_PIN_RANDOM 0

DN_TYPE_LDAP_REPLACE_SUBJECT_DN "YES"
DN_TYPE_LDAP_REPLACE_SUBJECT_RULES "admin" "user"

DN_TYPE_LDAP_SOURCE_DN_1 "OU=Administrativa,DC=Ou,DC=org,DC=DE"
DN_TYPE_LDAP_DEST_DN_1 "OU=OU,DC=org,DC=de"
DN_TYPE_LDAP_INCLUDE_SUBOUS_1 "NO"

DN_TYPE_LDAP_SOURCE_DN_2 "OU=Benutzer,DC=OU,DC=ORG,DC=DE"
DN_TYPE_LDAP_DEST_DN_2 "OU=OU,DC=org,DC=de"
DN_TYPE_LDAP_INCLUDE_SUBOUS_2 "NO"
```

DAASI International

Directory Applications for Advanced Security and Information Management

Configuration of ldapAutoCreateCSR

```
LDAP_CSR_BIND_DN_PREFIX "uid="
LDAP_CSR_BIND_DN_SUFFIX ", OU=Users, DC=org, DC=DE"

DN_TYPE_LDAP_BASE      "DC" "DC"
DN_TYPE_LDAP_ELEMENTS "emailAddress" "CN" "OU"

DN_TYPE_LDAP_BASE_1 "ORG"
DN_TYPE_LDAP_BASE_2 "DE"

DN_TYPE_LDAP_SUBJECTALTNAMES    "mail" "IP"

DN_TYPE_LDAP_SUBJECTALTNAME_1   "email"
DN_TYPE_LDAP_SUBJECTALTNAME_1_MINIMUM_LENGTH 3
DN_TYPE_LDAP_SUBJECTALTNAME_1_REQUIRED     "NO"

DN_TYPE_LDAP_SUBJECTALTNAME_2   "IP address"
DN_TYPE_LDAP_SUBJECTALTNAME_2_MINIMUM_LENGTH 7
DN_TYPE_LDAP_SUBJECTALTNAME_2_REQUIRED     "NO"
```

DAASI International

Directory Applications for Advanced Security and Information Management

Thank you for your attention

- Any questions?

- DAASI International GmbH
  Wilhelmstr. 106
  D-72074 Tübingen
  - www.daasi.de
  - Info@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management