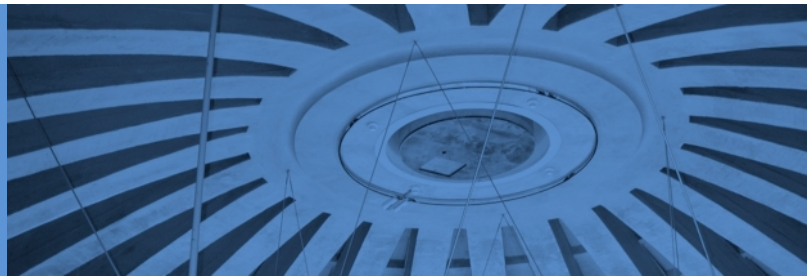


The Evolution of an Integrated User Directory

23 March 2004 :: David McLaughlin, Informatikdienste ETH Zurich

The Evolution of an Integrated User Directory

- Creation of many databases …
- The need for integration
- Creation of the NETHZ database
- Some NETHZ services
- Sources of data for the NETHZ database
- Some uses of the NETHZ database
- Creation of an AAI “Home Organization”

Creation of many Databases … (1990's)

- Staff database moved from Bern to ETHZ
- Creation of a Personnel database (PDB) containing staff & student records
- Creation of a Network database (CMS)
- Creation of a Buildings database (GIRBS)
- Creation of a Telephone database (Aladin)

The need for Integration (1998)

- Academic departments provided computer rooms for their own students
- Each student had several user accounts
- The Informatikdienste was given the task of managing the student computer rooms
- The “single sign-on” concept started to look like a good idea …
- The idea of a “services” database for computing & networking services was born

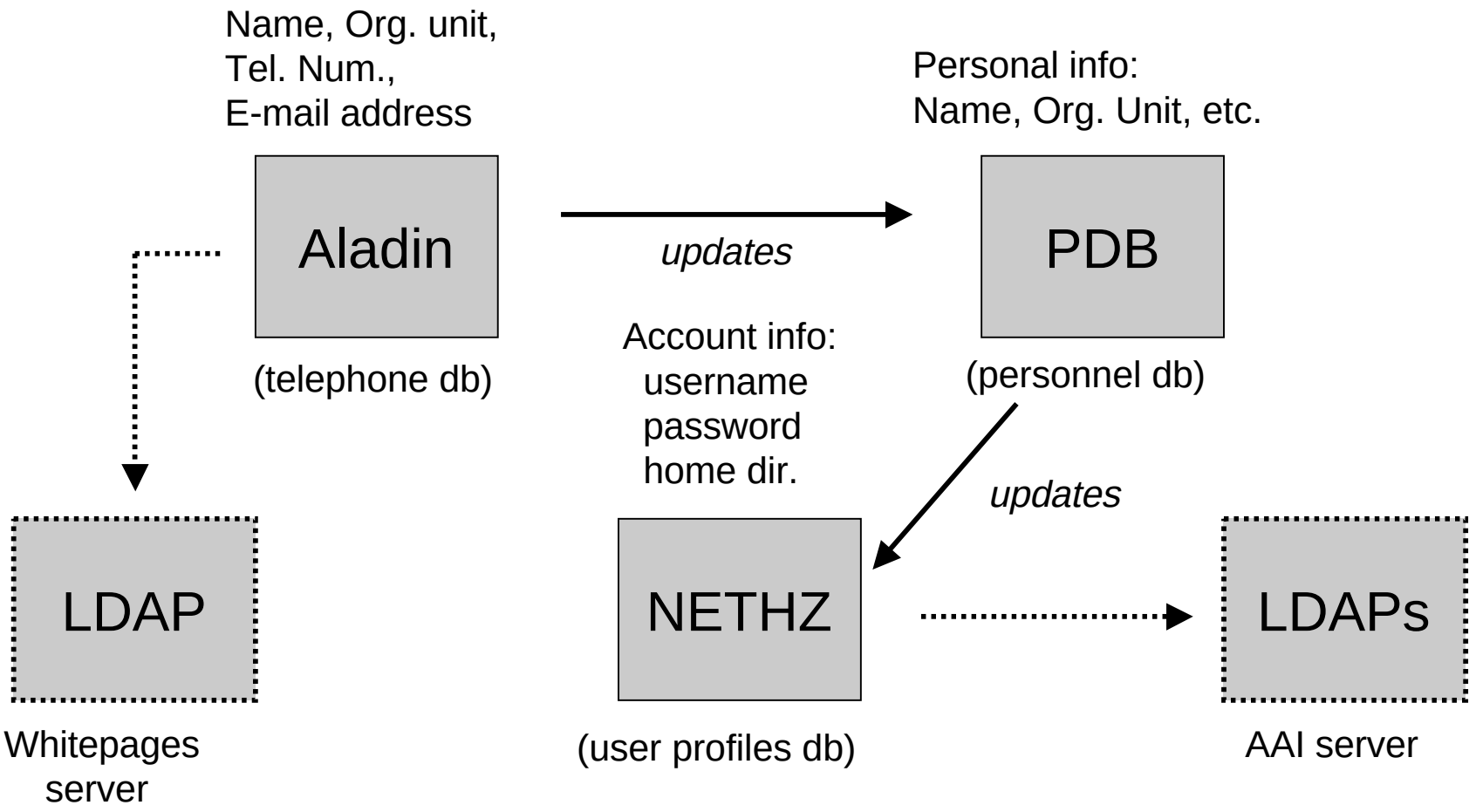
Creation of the NETHZ database (1998)

- Existing student & staff usernames were collected and fed into an Oracle database called “NETHZ”
- Home directories were created in AFS
- The NETHZ database controls access to systems, to particular resources on systems, and to various network services
- NETHZ allows decentralized administration of user accounts

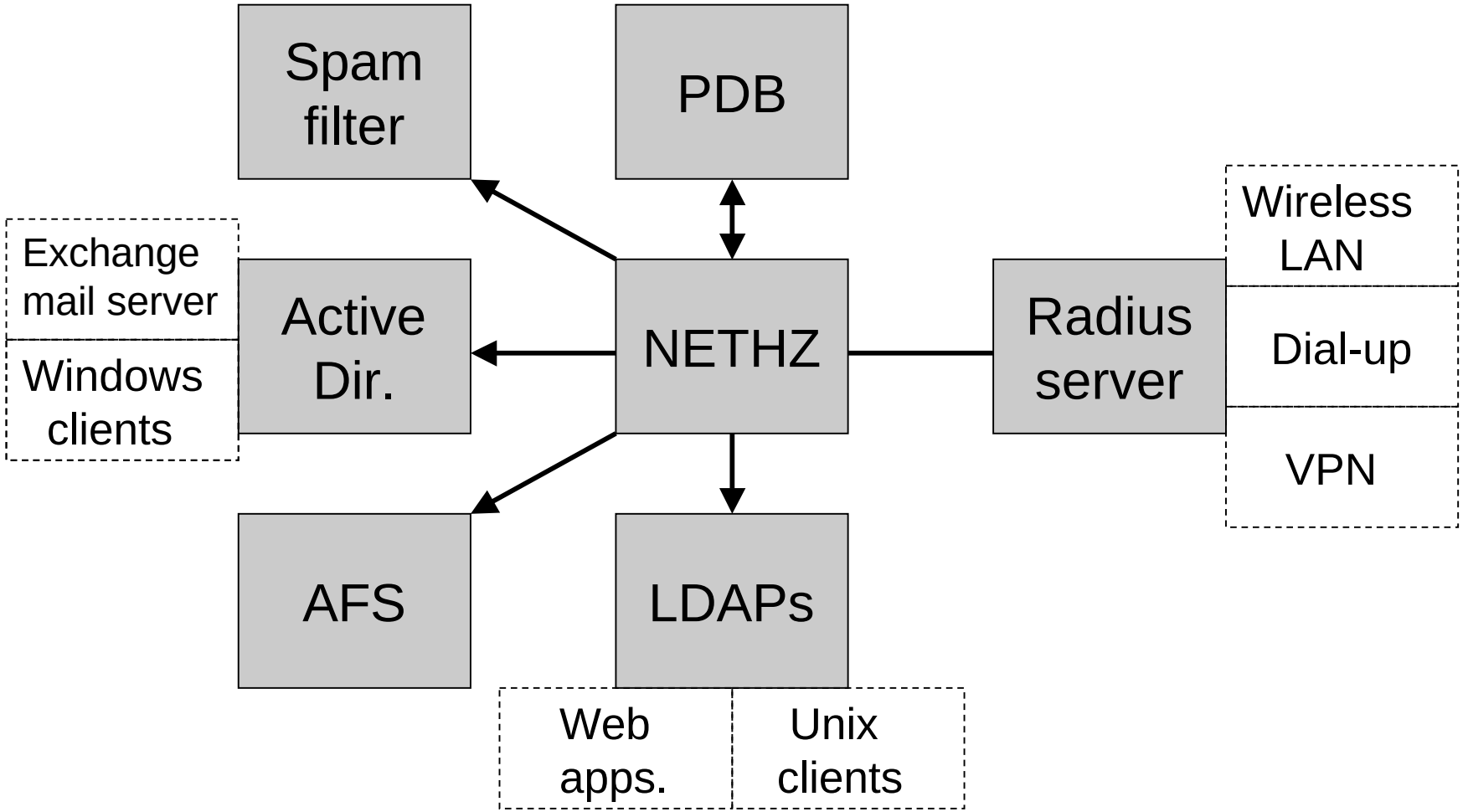
Some NETHZ Services

- AFS home directories
- E-Mail
- Spam Filter
- Dial-Up home access
- CableCom home access
- Laptop-Docking
- Wireless LAN
- VPN
- Message Tree
- PDB
- IPASS
- IDES
- Personal Web Pages

NETHZ Data Sources



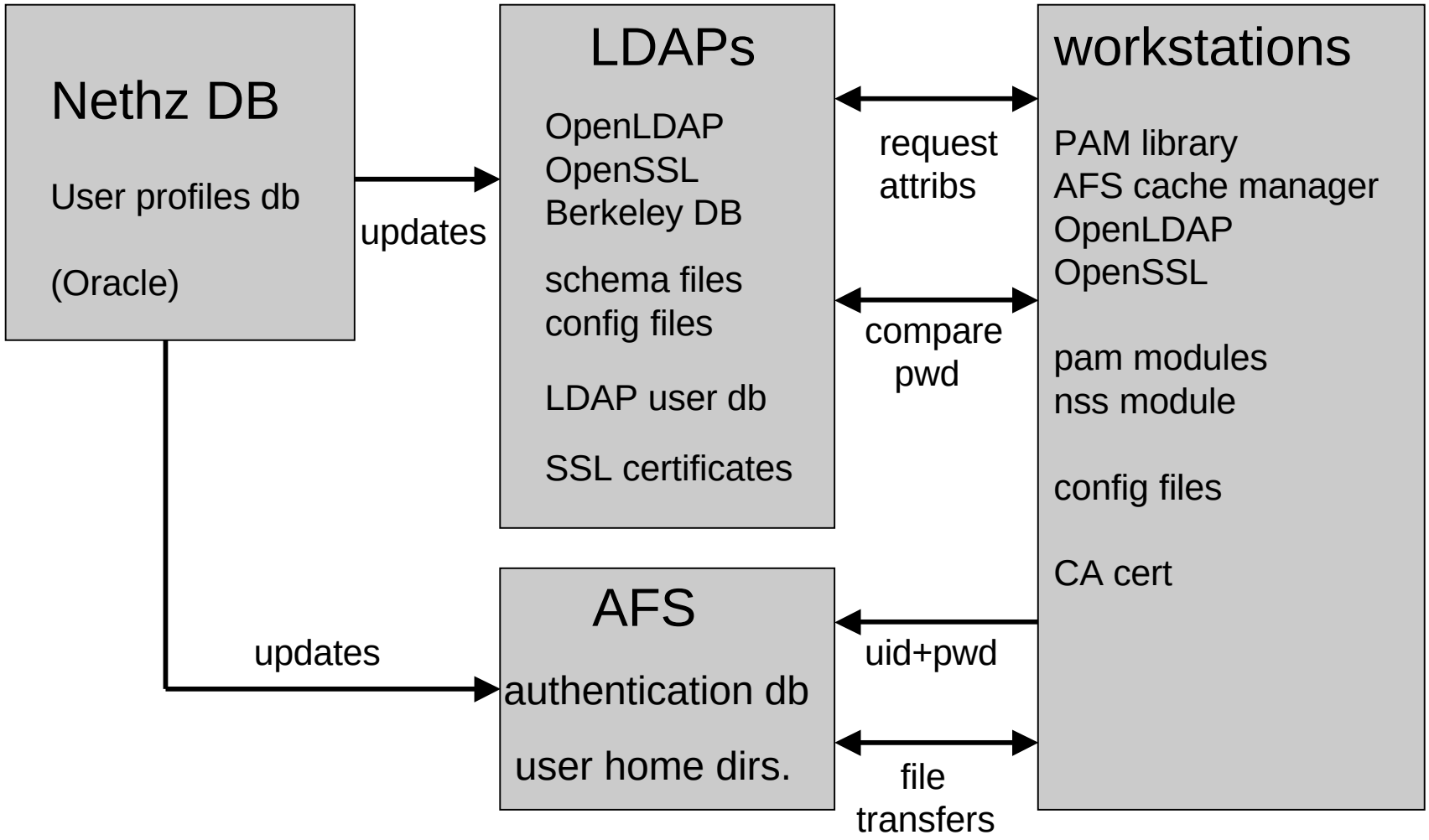
Some uses of the NETHZ db



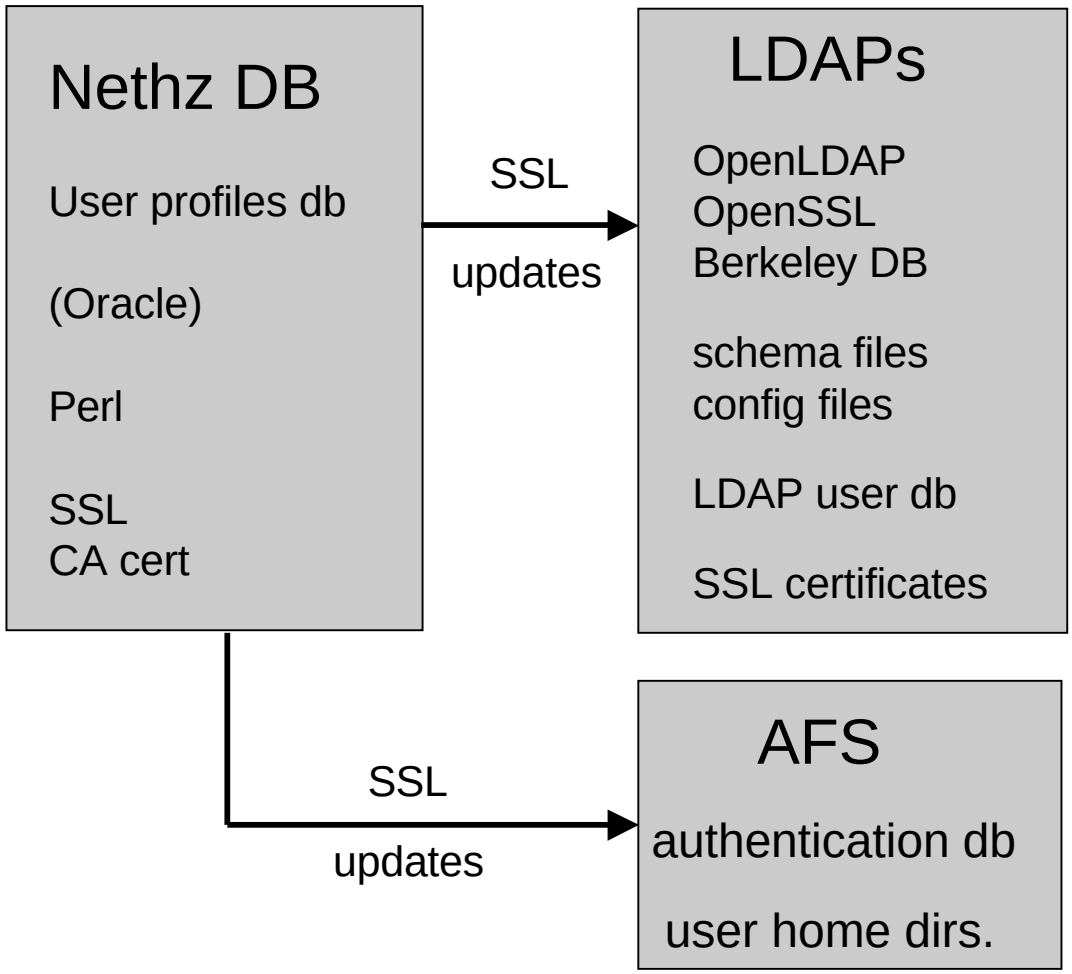
AAI Home Organization (2002)

- A user profiles directory (such as NETHZ) must exist before an AAI Home Organization can be established
- LDAP records are built from NETHZ db records
- Access to services can be controlled by the use of additional OU attributes (or objectclass attributes)
- The ***ethzOrgPerson*** objectclass allows us to have some locally defined attributes
- The ***swissEduPerson*** objectclass provides compatibility with other Swiss universities

LDAP AAI Components



Nethz DB Server



LDAPs Servers

LDAPs

OpenLDAP
OpenSSL
Berkeley DB

core.schema	required by LDAP
cosine.schema	“account” attributes
nis.schema	“posixAccount” attribs.
local.schema	“ethzOrgPerson” attribs.
swissedu.schema	“swiisEduPerson” attribs.

slapd.conf – database def., access rules, etc.
ldap.conf – used by ldap utilities

LDAP user database

CA certificate
Server certificate & private key

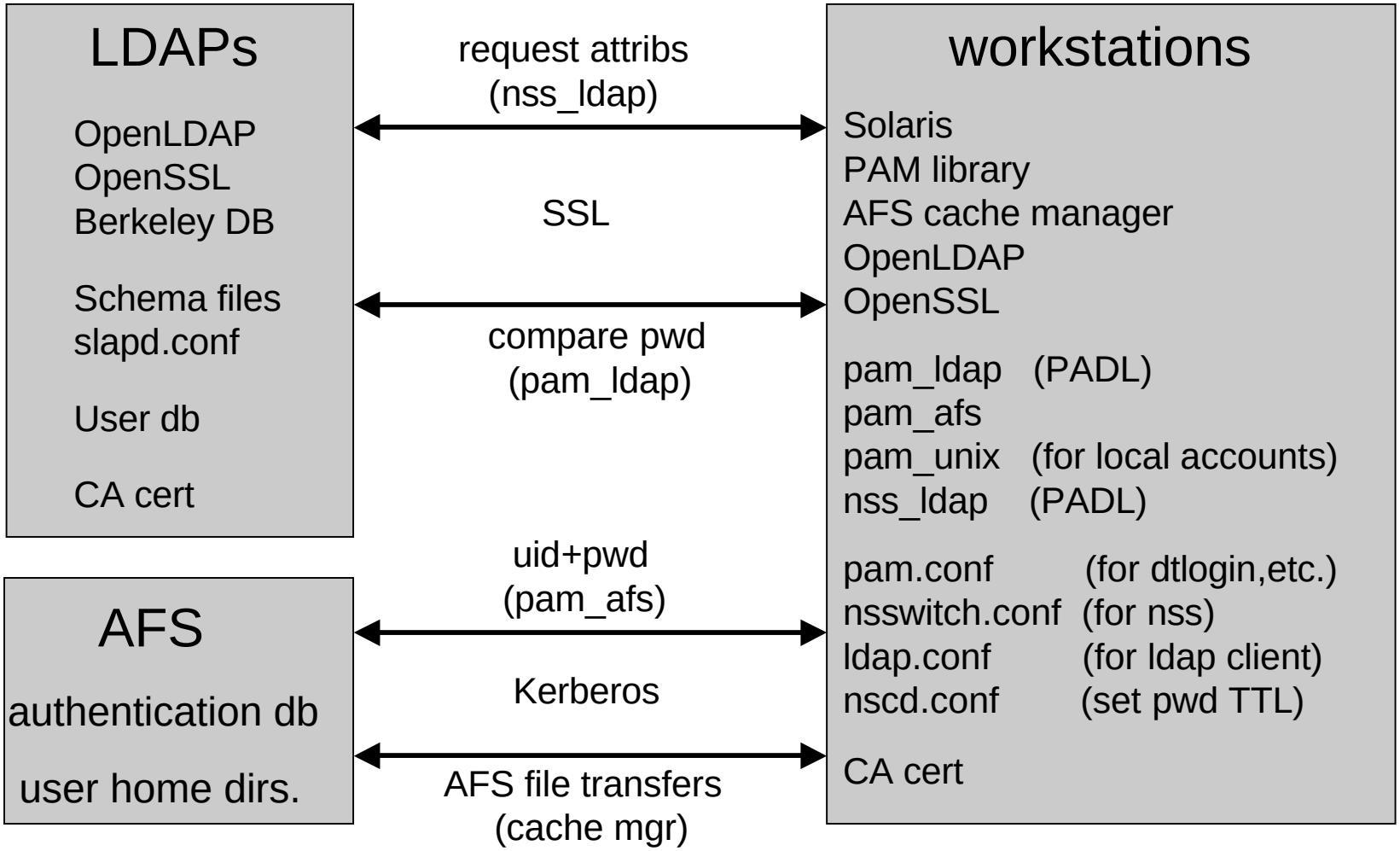
AFS Servers

AFS

authentication db
(uid + pwd)

user home dirs.

Workstations



An LDAP Record

dn: cn=hmuster,ou=nethz,o=ethz,c=ch
objectclass: top
objectclass: person
objectclass:organizationalPerson
objectclass: inetOrgPerson
objectclass: swissEduPerson
objectclass: eduPerson
objectclass: posixAccount
objectclass: shadowAccount
objectclass: ethzOrgPerson
cn: hmuster
givenName: Hans
sn: Muster
uid: hmuster
uidNumber: 28647
gidNumber: 10
mail: hans.muster@id.ethz.ch
gecos: Hans Muster
loginShell: /bin/tcsh

userPassword: {SSHA}GfoHxHWdNB
homeDirectory: /afs/ethz.ch/h/hmuster
nUID: 644300
nPID: 849056
PERSID: 44217
shadowExpire: -1
shadowLastChange: -1
shadowFlag: -1
shadowInactive: -1
shadowMin: -1
shadowMax: -1
shadowWarning: -1
eduPersonAffiliation: member
swissEduPersonOrganizationType: university
swissEduPersonDateOfBirth: 19840124
swissEduPersonHomeOrganization: ethz.ch
swissEduPersonUniqueID: 849056@ethz.ch

Helpful Hints

- Some versions of OpenLDAP with Berkeley DB are unstable under heavy loads, so test carefully before deploying a new LDAP server.

- A useful LDAP book:

  LDAP System Administration

  by Gerald Carter, 2003, O'Reilly pub.