Linux Client im Windows AD

Ein Erfahrungsbericht

RBG-Seminar WS 06/07
21.11.2006

Holger Kälberer

Übersicht

- Einleitendes: Infrastruktur und Dienste, was ist AD?

1. Authentifizierung
2. Home-Verzeichnisse
3. Drucken

Vorüberlegungen

- Anforderungen an den Client:
  - Komfort für Windows-Nutzer (USB-mounts, verknüpfte Extensionen, Zusammenspiel der Applikationen) $\rightarrow$ Desktop-Umgebung/-Distribution (ubuntu)
  - $\rightarrow$ Auswahl einer (!) Oberfläche (gnome/xfce)

Vorüberlegungen (Forts.)

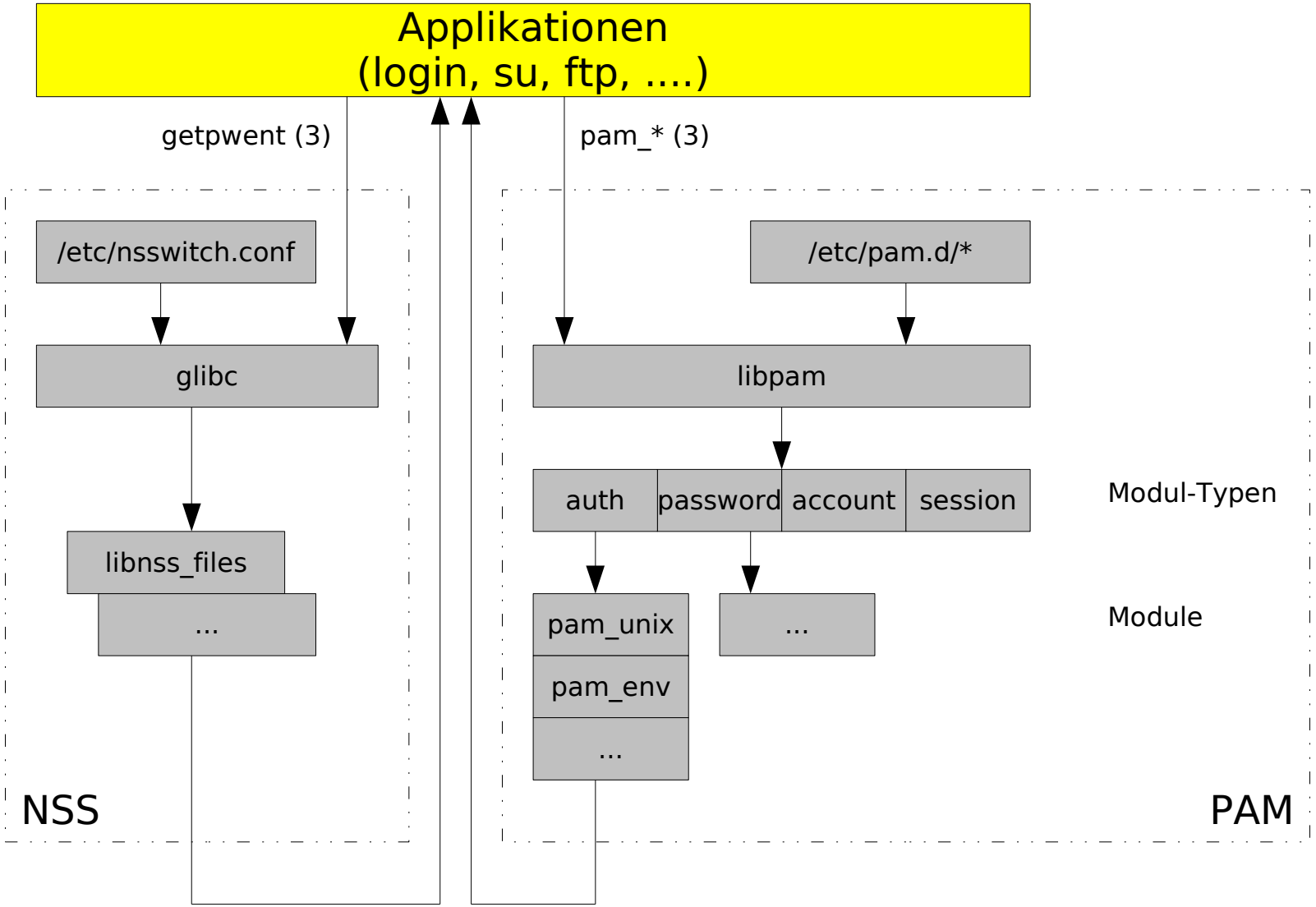
- Integration in die HRZ-Infrastruktur (AD):
  - Applikationen
  - viele Dienste, eine Authentifizierung --> “SSO”
  - Userbezogene Nutzung der Dienste:
    - smb-shares
    - individuelle Abrechnung der Druckerntuzung

AD

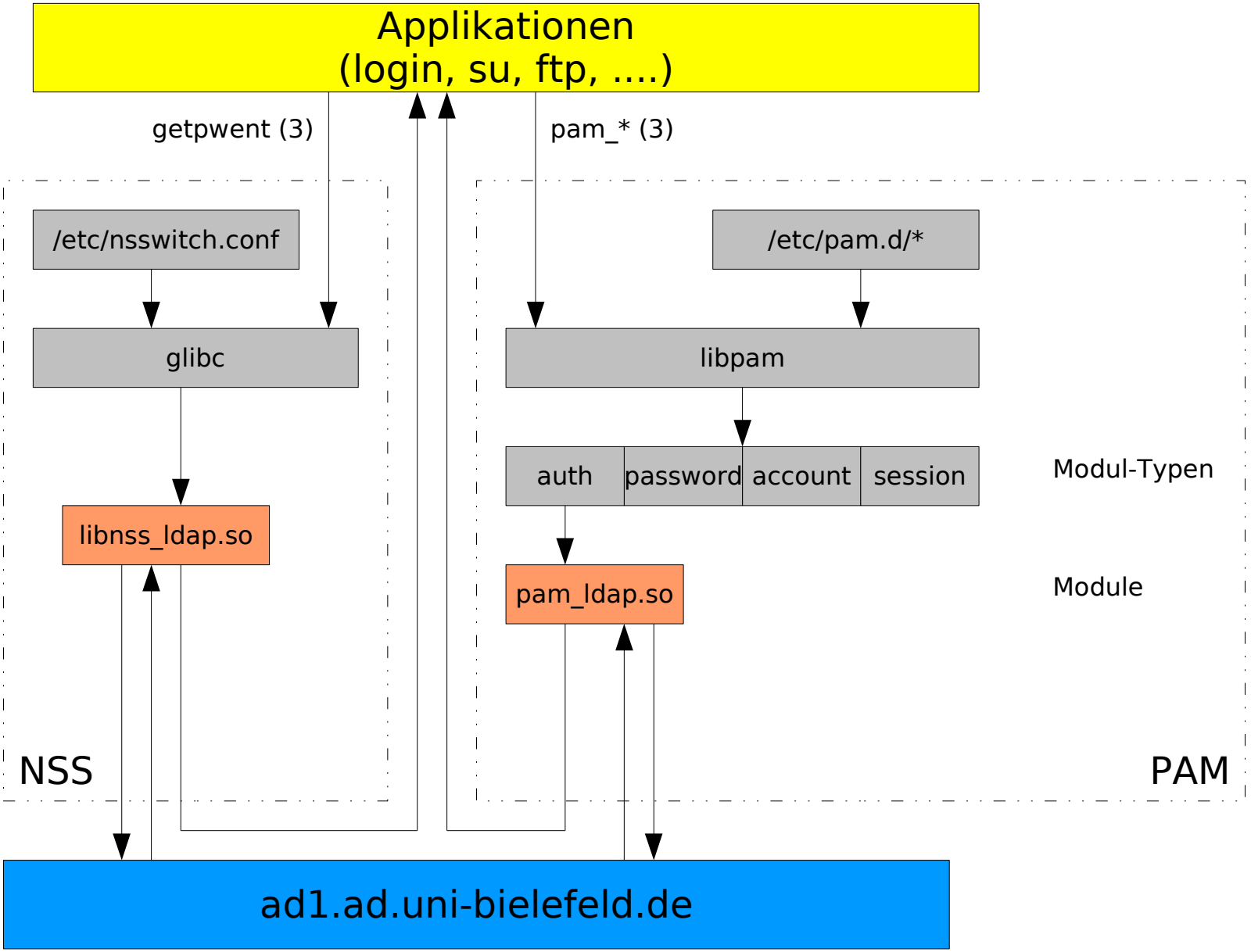
- hierarchischer Verzeichnisdienst fuer Nutzer, Ressourcen und Dienste
- AD = LDAP+Kerberos+CIFS +DNS
- AD-content= forest (trees (domains (OUs)))
- AD = Schemata+Konfiguration+Domains
- Multi-master Replikation zwischen rw-DCs durch trust-Beziehungen
- Identifikation von security principals: SID, RID, `sAMAccountName`

1. Authentifizierung

Linux PAM+NSS Architektur



(a) ldap


Applikationen
(login, su, ftp, ...)
getpwent (3)
pam_* (3)
/etc/nsswitch.conf
/etc/pam.d/*
glibc
libpam
auth
password
account
session
Modul-Typen
libnss_ldap.so
pam_ldap.so
Module
NSS
PAM
ad1.ad.uni-bielefeld.de

ldap (Forts.)

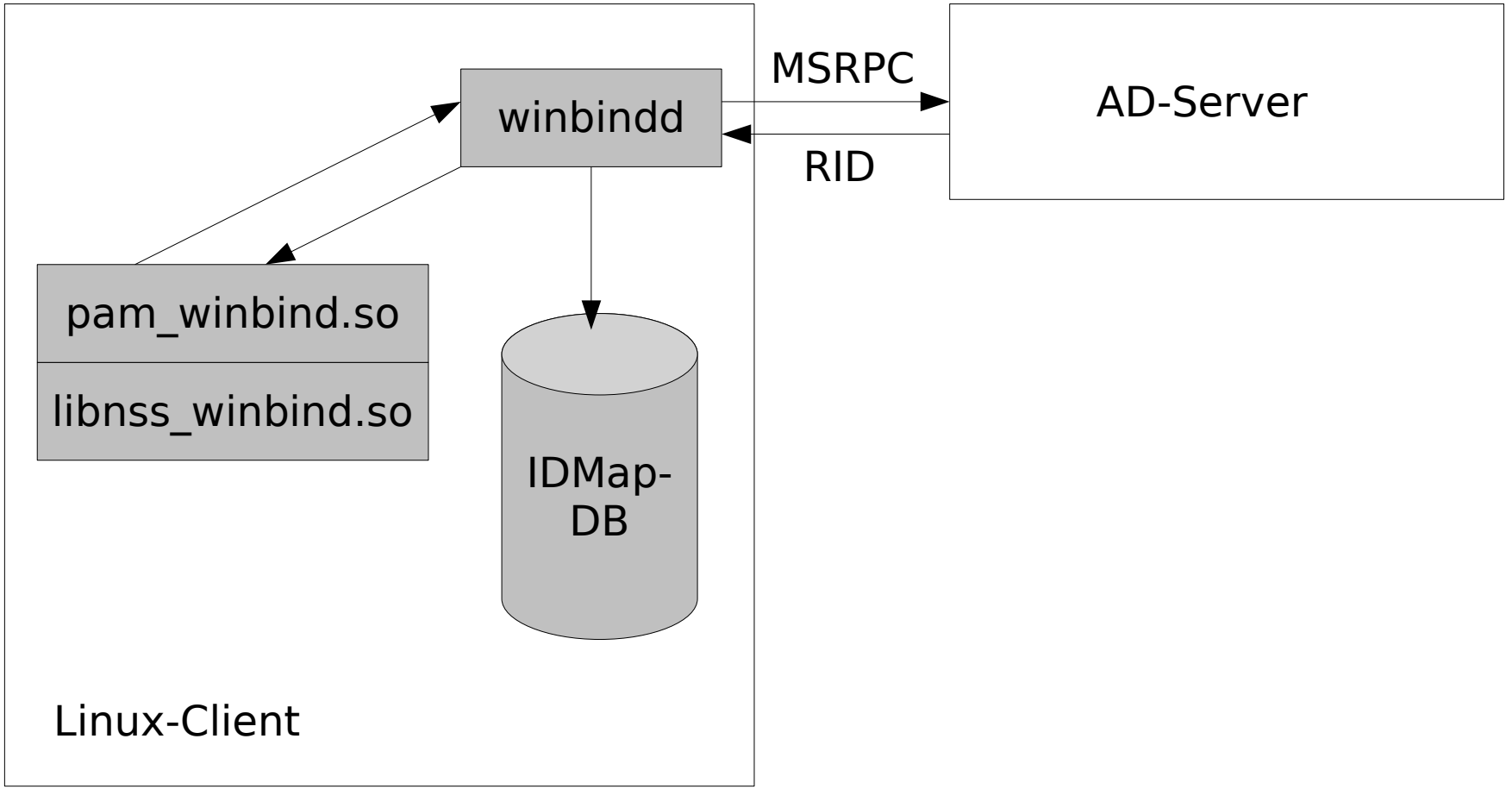
- direktes mapping von AD-Objekt-Attributen auf ldap-NIS-Attribute (`posixAccount`; RFC 2307)
- Voraussetzung: Schema-Erweiterung um die SFU
- potentielles Risiko --> Keine Option!

```
nss_map_attribute       uid                sAMAccountName
nss_map_attribute       uidNumber          uidNumber
nss_map_attribute       gidNumber          gidNumber
nss_map_attribute       uniqueMember       member
nss_map_attribute       givenname          givenName
nss_map_attribute       ou                 description
nss_map_attribute       gecos              displayName
nss_map_attribute       homeDirectory      unixHomeDirectory
nss_map_attribute       loginShell         loginShell
nss_map_attribute       shadowLastChange   pwdLastSet
```

(b): winbind

- 3 Funktionen:
  1. Authentifizierung von credentials (`pam_winbind.so`)
  2. ID-Mapping zwischen AD und Linux (NSS)
  3. DB für die Mappings (`winbind_idmap.tdb`; erlaubt ldap-backend für einheitliche Mappings)
- Erlaubt Windows-auth für samba DCs

(b) winbind (Forts.)



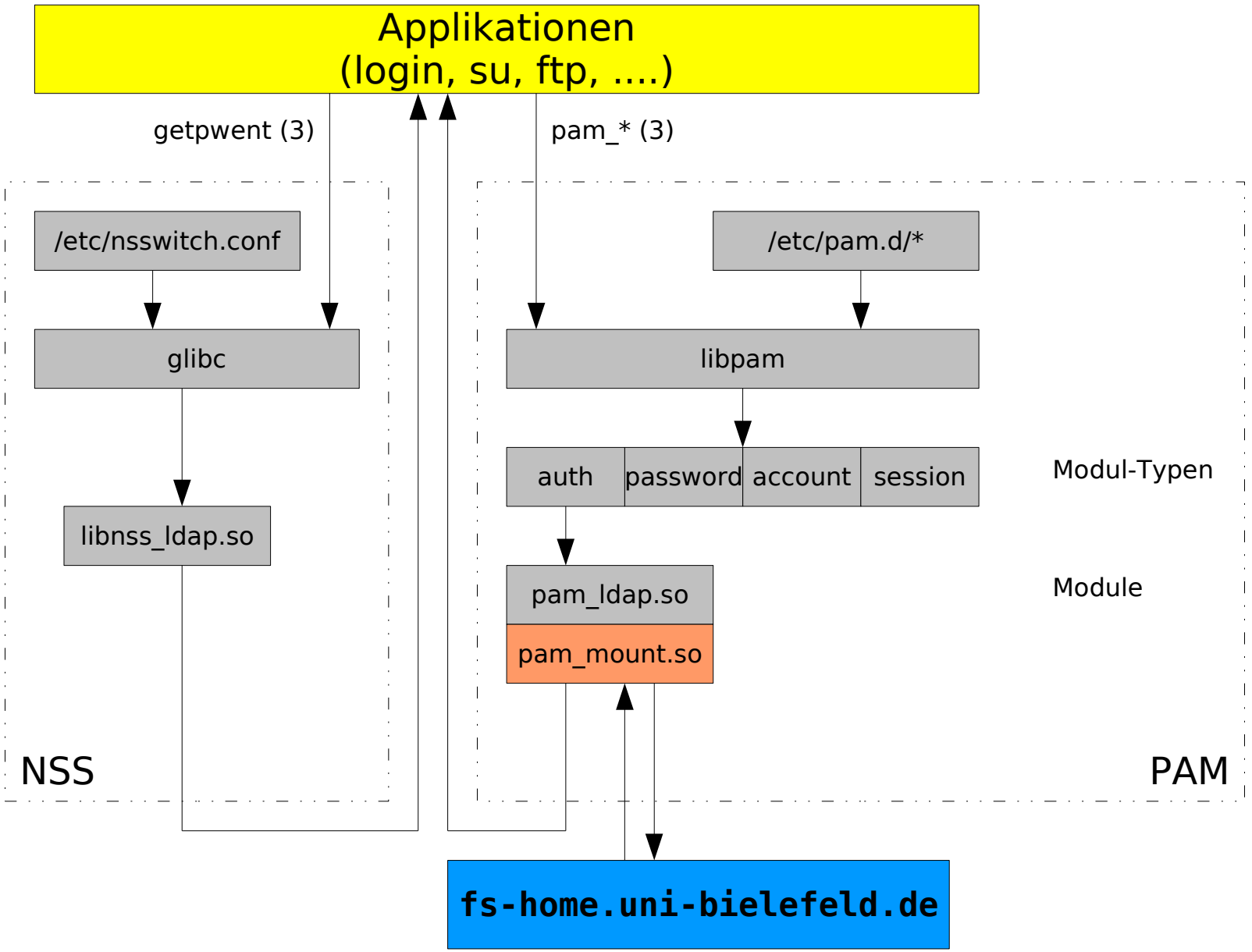
smb.conf für winbind

```
[global]

workgroup = AD
server string = %h
security = ads
realm = ad.uni-bielefeld.de
password server = ad1.ad.uni-bielefeld.de
encrypt passwords = true

# ...

winbind separator = \
idmap uid = 10000-100000
idmap gid = 10000-100000
# allow enumeration of winbind users and groups
winbind enum users = yes
winbind enum groups = yes
# give winbind users a real shell (only needed if they have
telnet access)
template homedir = /home/%D/%U
template shell = /bin/bash
# ...
```

2. home-shares

- home-Verzeichnis bei login einbinden
- pam_mount mountet bei login von fs-home.uni-bielefeld.de
- Nachteile: braucht suid auf smbumount
- (pam_cifs)

pam_mount


Applikationen
(login, su, ftp, ...)
getpwent (3)
pam_* (3)
/etc/nsswitch.conf
glibc
libnss_ldap.so
/etc/pam.d/*
libpam
auth
password
account
session
Modul-Typen
pam_ldap.so
pam_mount.so
Module
NSS
PAM
fs-home.uni-bielefeld.de

homes: Probleme +Lösungen

(1) die home-Verzeichnisse (`\\fs-home.uni-bielefeld.de\\home\\hkaelberer`) sind "keine shares"

- bind-mount?
- "anonymer mount" des kompletten home-Baums

```
smbmount /usr/bin/smbmount   //%(SERVER)/%(VOLUME) %(MNTPT) -o
"username=%(USER),uid=%(USERUID),gid=%(USERGID)%(before=\",\"
OPTIONS)"

volume * smbfs fs-home.uni-bielefeld.de home/ /home/AD/
uid=&,dir_mode=0700,workgroup=AD - -

#volume * smbfs fs-home.uni-bielefeld.de home/& /home/AD/&
uid=&,dir_mode=0700,workgroup=AD - -
```

homes-Probleme (Forts.)

(2) Einschränkungen der Dateitypen und -Operationen im smb-mount → keine xfce-/gnome-/kde-logins

- Lösung: `iceauth`-Informationen nach `/tmp/`
- kein KDE

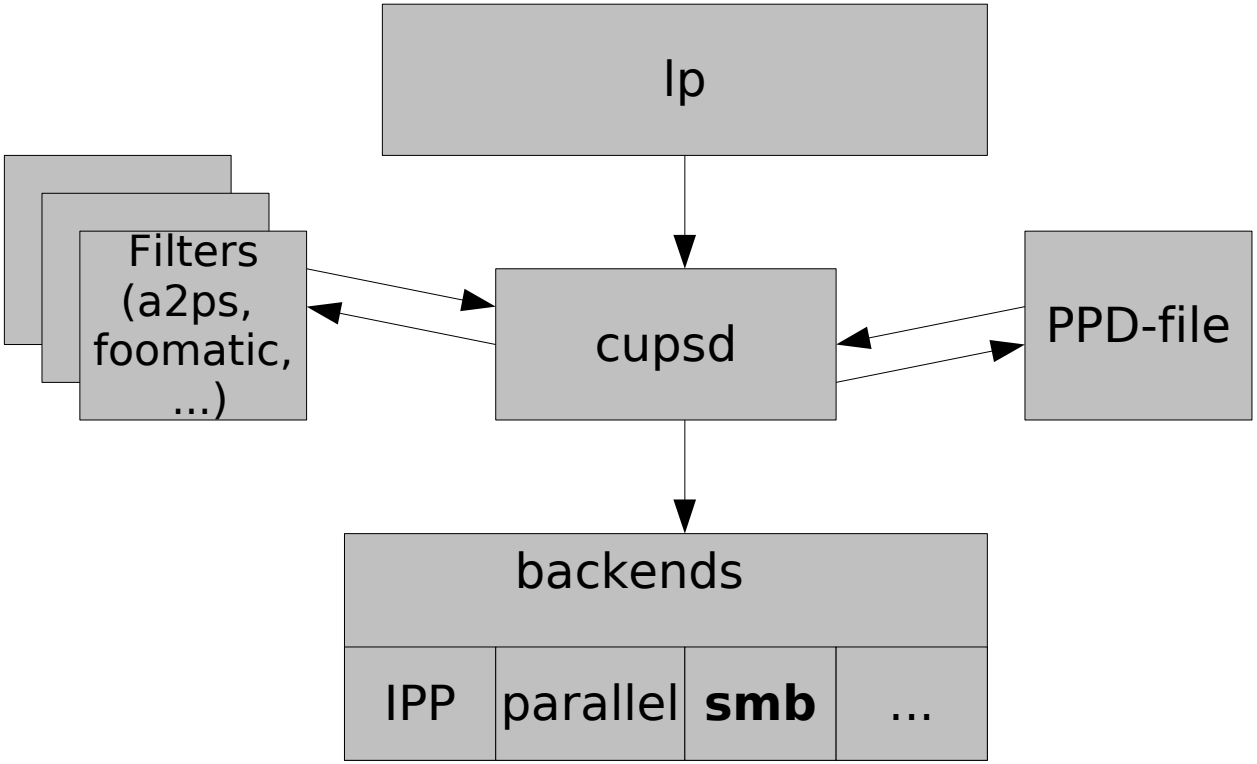
```
/---  /etc/gdm/Xsession
ICEAUTHORITY="/tmp/.ICEauthority-${USER}"
export ICEAUTHORITY
---/
```

3. Drucken

- Anforderungen (HRZ):
  - SSO
  - individuelle Drucker-Nutzung (und Kosten-Abrechnung) !!!:
    1. aktuellen Nutzer kennen
    2. mit diesem Nutzer authentifizieren
- `hrz-pserv.ad.uni-bielefeld.de` spricht nur smb

a) CUPS

- Architektur:



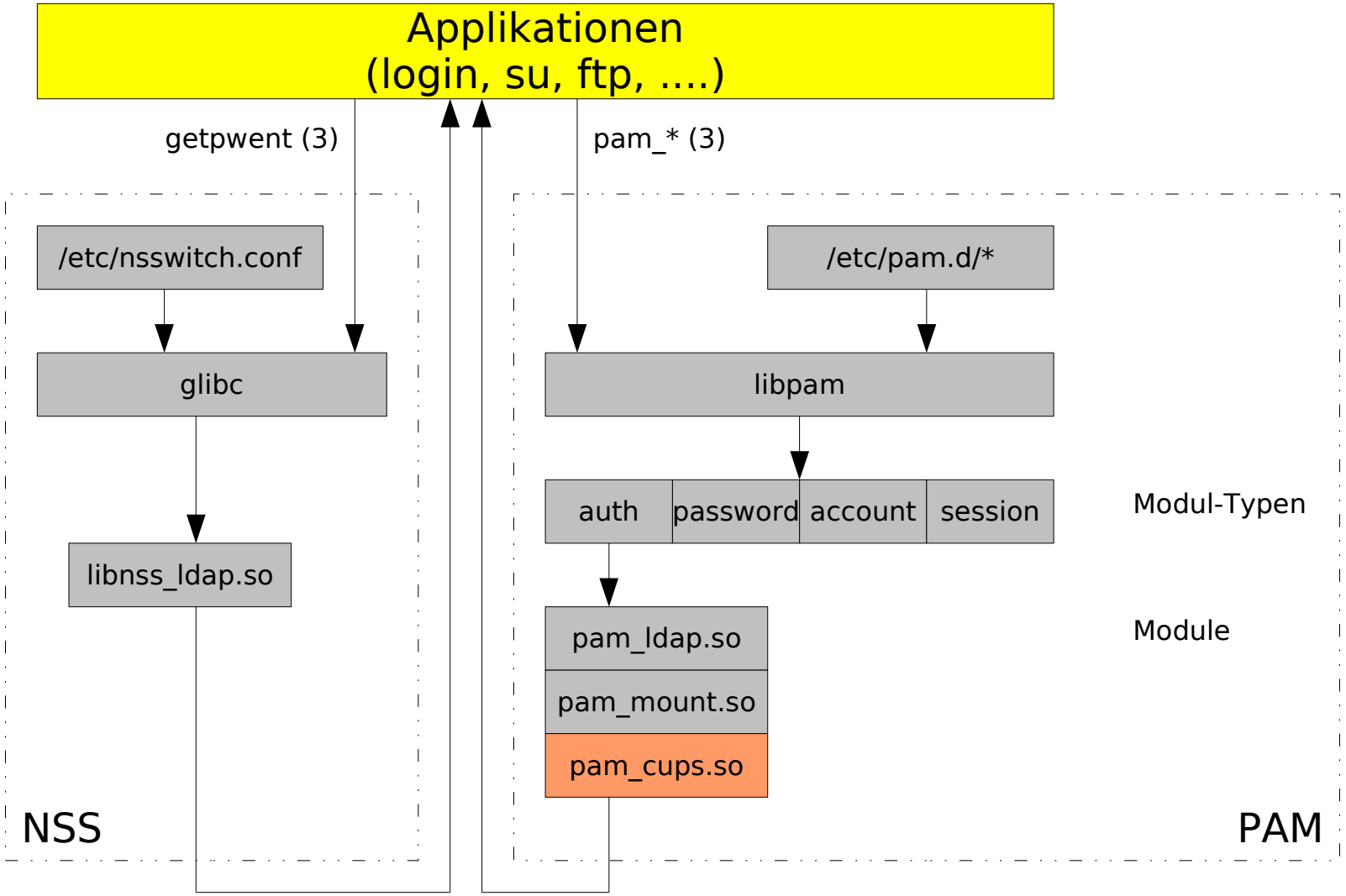
CUPS – smb-backend

- smbspool bekommt zwar Nutzer-Informationen von cups ... kann aber kein Kerberos und braucht ein Klartextpasswort

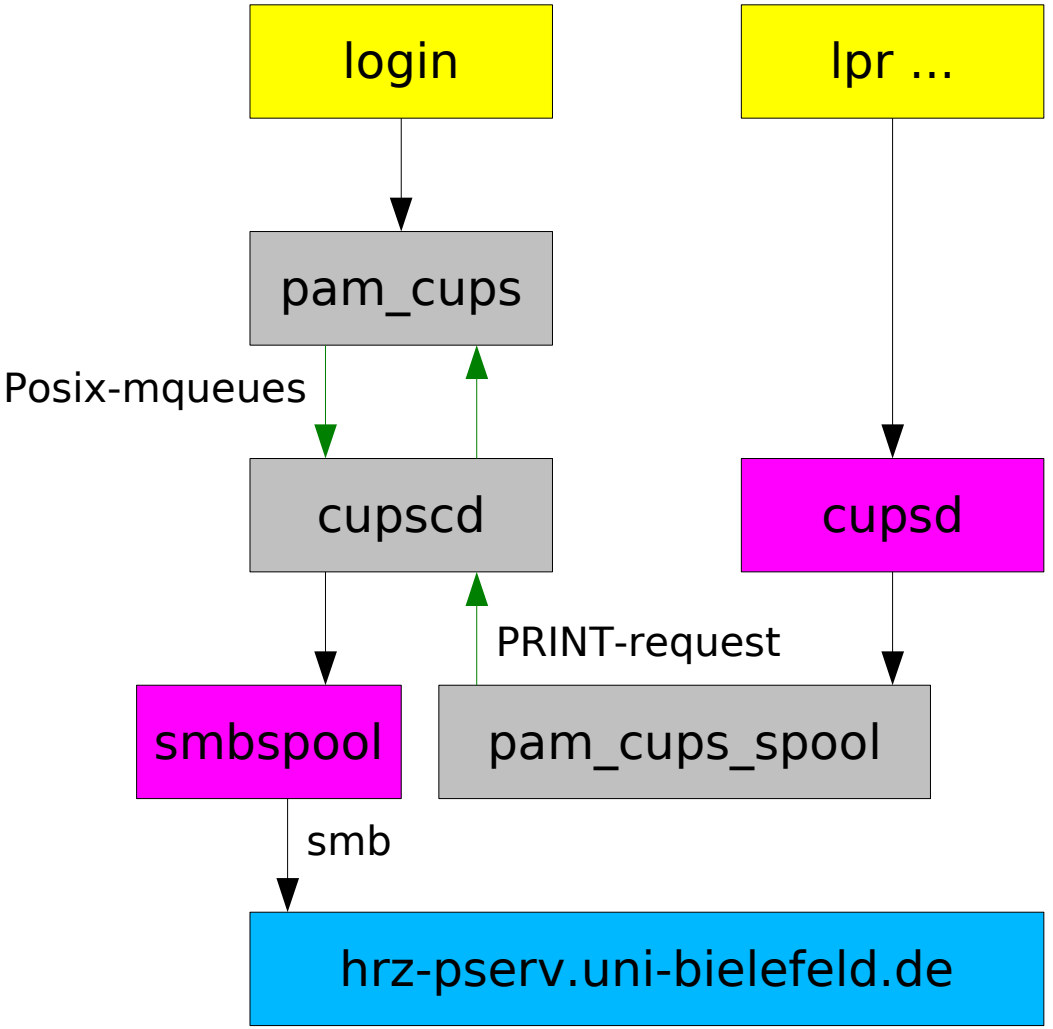
```
/--- /etc/cups/printers.conf
<Printer HRZ_HP_LASER>
[...]
DeviceURI smb://hkaelberer:SECRET@hrz-pserv.uni-bielefeld.de/HRZ_HP_LASER
[...]
---/
```

- Speichern der credentials im home ist keine Option

pam_cups (Forts.)



pam_cups


login
lpr ...
pam_cups
Posix-mqueues
cupscd
cupsd
PRINT-request
smbspool
pam_cups_spool
smb
hrz-pserv.uni-bielefeld.de

b) Alternativen

- smb-backend mit Kerberos-Unterstützung
  - evtl. als wrapper-script um smbclient; (nicht-triviale backend-Spezifikationen!)
- LPRng: smbprint als filter-script kann via smbclient credentials übergeben

```
cat FILE.ps | smbclient //hrz-pserv.uni-bielefeld.de/HRZ_HP_LASER
-U hkaelberer -k -c "print -"
```

Zusammenfassung

- Integration eines Linux-Client in ein Win-AD ist auf Umwegen (samba-tools und pam-Module) möglich
- Nachteile (gegenüber Win-Clients):
  - nicht jeder WM
  - kein browsen der Drucker (müssen fest konfiguriert werden)
  - bisher ungelöst: kein smbumount bei logout
  - (weniger Applikationen)