

Identity Management - experiences from real life

Prof. Dr. Gerhard Schneider
direktor@rz.uni-freiburg.de

Albert-Ludwigs-Universität Freiburg

UNI
FREIBURG

DAAD

Deutscher Akademischer Austausch Dienst
German Academic Exchange Service

The scenario

Why do we need an identity management?

What is the problem?

How to do it?

How to endorse (enforce?) it?

How to get added value?

Make it a self-propelling solution....

Today's target:

management insight –no technical course

The structure of German universities – a humoristic description

Depends a bit on the State

Professors are in the center of attention

- A German professor can do everything
 - Teaching, research, administration
- And will do it
 - Interfere in admin. questions

Institutes and Faculties are the important structure

Central administration is a nuisance

The Rector is supposed to find more money and let the faculties spend it

A powerful rector appears to be a threat

**This makes
a university
a powerful
institution
working for
the better
of society**

**probably
the best
solution we
have**

UNI
REIBURG

consequences

Our universities cannot be run like companies

- A CIO cannot order the introduction of new services

So introduce useful services without asking

- Real challenge – you must succeed :-)

And be fast

- Faster than the other side

Example: Identity Management

- Administration has the relevant data
- The faculties and other organisations need it
 - Even if they do not know this

The situation

Administration knows everything about

- Staff with valid work contracts
- Matriculated students



Remember this?

Feed that data into the standard **LDAP**

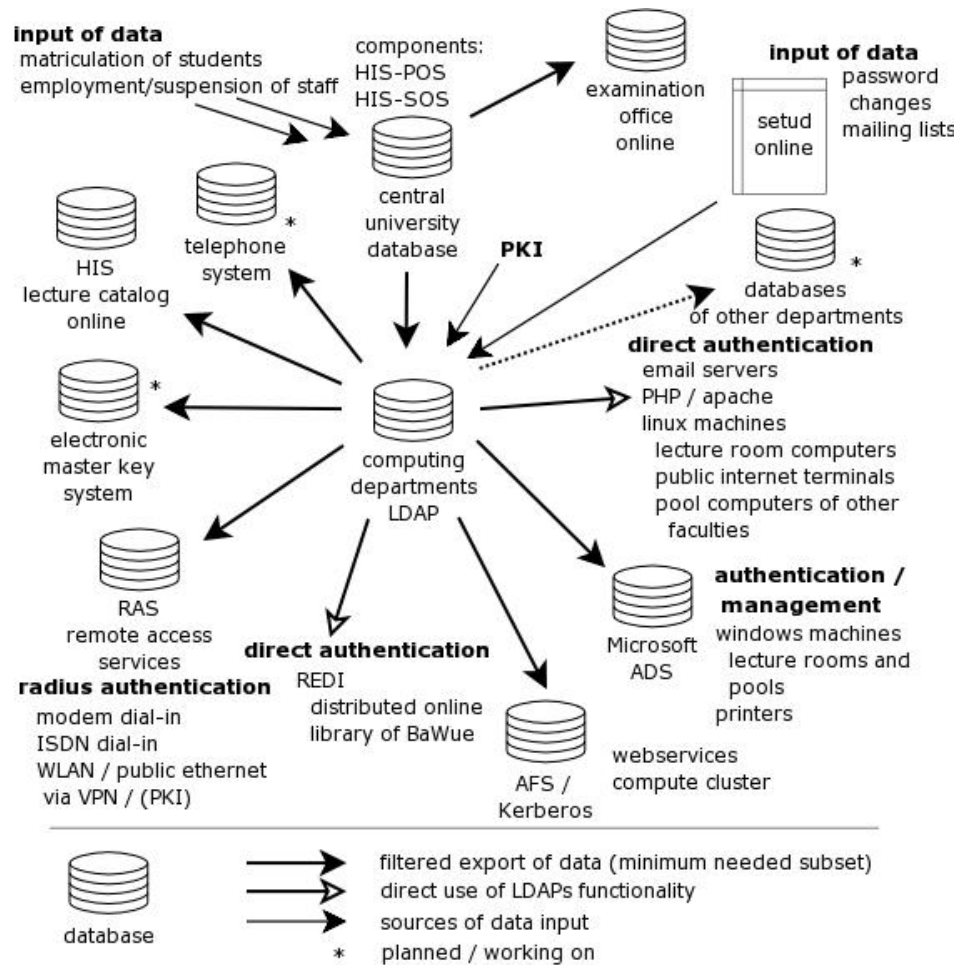
- Like reading punched cards containing changes

Users are allowed to modify other data on LDAP

- Which is mirrored back into the official systems
- Like email-adresses or phone numbers, or....

Identity management – basic concepts

IT touches real life!
Dealing with genuine user data



- Only export a minimal set of data (what is necessary? **Why??**)
- Most ID-based procedures do not need a view on all available data
- It works!!
- The true bottlenecks can now be identified
- Any ready-to-run solution will show up bottlenecks when operational

Alternatives from real life

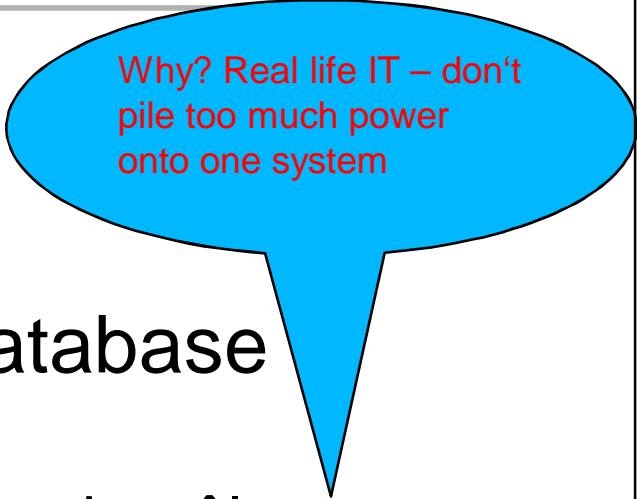
(as taught in class)

- Evaluate existing id-management solutions
- Choose the best
 - What is „the best“ - who decides?
- Buy hardware and software, trial runs
- Install upgrades for the software
- Enforce the solution onto the active players
 - They will be extremely happy – and love you :-)
- After the first runs under real conditions you will need new hardware
- Months or years of unstable operation

Get going!

Add more value to convince the crowd

- We now know who is an active member of the university
- Feed this information into the database for the electronic doorlocks
 - Only the existence – not the rights nor the rôle
 - If people leave the uni, doors will be locked for them
 - Rights management will still be done in the corresponding system – by the people in charge
- Almost automatic question: can we manage the university card in LDAP?
 - This makes life easier for the doorlocks – and for the administration



Why? Real life IT – don't pile too much power onto one system

Doorlocks – why are they interesting?

- door locks = real access
- Make sure that an ex-user can no longer get into security relevant rooms!
 - Chemistry labs
 - Animal experiments
 - Dean's office
 - Parking lots
- Online solutions **and** offline solutions
 - Download the „rights for today“ onto card



experiences

- The central keycard system has its own database
 - No way to change this – no online check vs. LDAP
 - Pay money to the company to have an import interface like in the old „punched card days“
 - Data is not available in real time – but within 24 hours.
 - Which is enough for a university 😊

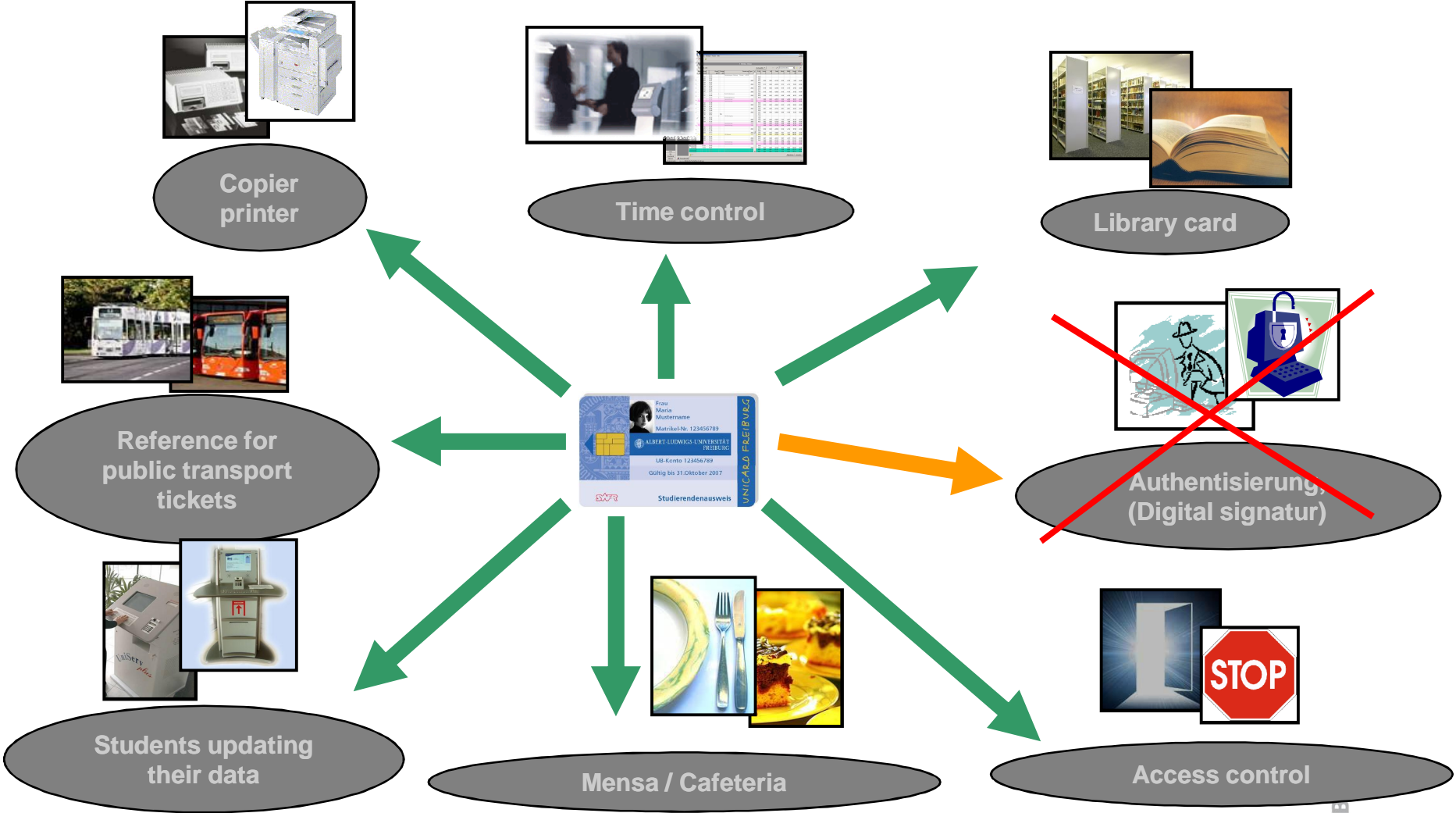
-

The university card

- For payment
- Work time management
- Rudimentary access control to main doors and parking lots
- At first „lack of a killer application“
- Now more and more features are added



Functions of our UniCard



Get going!!

- **Electronic mailing lists**
 - Email addresses are collected because electronic processes rely on them
 - Self-service administration
 - Warn about expiry of book loans in the library
 - Collect rather than assign
 - People's private email addresses will be read, those assigned by the university not necessarily
 - Well, you could legally enforce this, but this is extra work
 - Why fight legal battles if they are not necessary?
 - Grant the right to sign off
 - Otherwise there is always one who will complain
- **We can now reach people **again****

Get going!!!

- VoIP: new phones show who is calling
 - Okay, this is old stuff for private users – but you have to maintain your own database
 - New phone system talks to LDAP
 - People can put their data (i.e. the data they want to be displayed) into LDAP
 - Using their existing account
 - Saves endless discussions about what should be displayed....
 - If you want to display the name/picture of MickeyMouse – why not? Your colleagues will comment, not the CC

Get going!!!

- Offer digital certificates
 - Run the DFN solution and check the existence of some applicant via the LDAP database
- The library needs to know the members of the university
 - For deciding on whether to grant access to electronic journals
 - Use shibboleth as tool
 - Offer a solution which gives you a shibboleth ticket via userid/passwd versus the LDAP

An important tool – it requires a working identity management = wait a few slides

Get going!!!!

- E-learning: new learning management software
 - Buy it with LDAP connectivity
 - Students need the id which also opens the WLAN
- Convince the administration to use the id for access to the electronic course/marks/exam system
 - Students need the id which also opens the WLAN ☺
- Thus set up a working infrastructure which is good for more
 - Master online – a new venture for the university
 - Funding secured against fierce competition, thanks to...

Judging the effort

- The solution sometimes reminds me of an old battered car held together with sticky tape
- But the car is successfully on the race course, doing round after round
- While the others are still in their boxes, under service
- We start to understand what we really need
 - And we will be able to buy an industrial system when needed and necessary
- Main effort: getting everybody to drive their systems in a systematic manner
 - Writing the connector scripts is easy

Who is in the driving seat?

- Start a political process (rectorate, senate)??
- Just do it??
 - IT people in the admin IT centre, scientific computer centre can cooperate
 - If theya want 😊
 - Conspiracy??? Be aware!
- Do it with cover from the rectorate!
 - Make the CC boss vice rector 😊
 - Win a few prizes 😊
- And then never change a running process

Fundamental prerequisite to success

- Find out
 - **Where** you have authoritative data
 - And **how** to synchronize reliably
 - Perhaps by writing „orders“ to people
- Do not force people to disclose information
 - Only to please your setup – „prove“ it is necessary
- It is all about organisation
- We do not teach this enough in our courses
 - And tend to use yet another system
 - Or are asked to use yet another system
 - By those who do not understand but think that „dirty“ solutions can never work

Don't overdo it!

- **Do not abuse your data**
 - Don't send out many emails on the mailing lists
 - Or people will „sign off“
 - Don't sell the list to others
 - Don't do advertising for others
- **Always allow for manual interaction**
 - If the system can't do it
 - Like email/accounts for new, not yet appointed profs
- **People will only give you their data, if they feel secure about it.**

Intermediate summary



- **Introduce a new service**
 - Do not alter existing solutions
 - Make sure that the responsibility for updating data is clearly laid out
 - Ensure that existing services use the new data management
 - Wlan, shibboleth,
 - Ensure that new services do use the data management
 - Electronic doors, elearning, digital certificates
- **Move faster than the competitors in the faculty**
 - So they can't keep up with you

Shibboleth – what do we want?

- **User view**
- Access to licensed material should be possible **independent** of the actual **work place** or the **access method**.
- All licensed contents should be available after one initial login (**Single Sign-On**).
- No personal data should be handed to third parties
- **Institutional view (e.g. universities)**
- Institution should be allowed to choose any local authentication scheme. But it must have an Identity Management System (IdM)
- **Content provider**
- The contents licensed from content providers must be protected against unauthorized access.

What is Shibboleth??

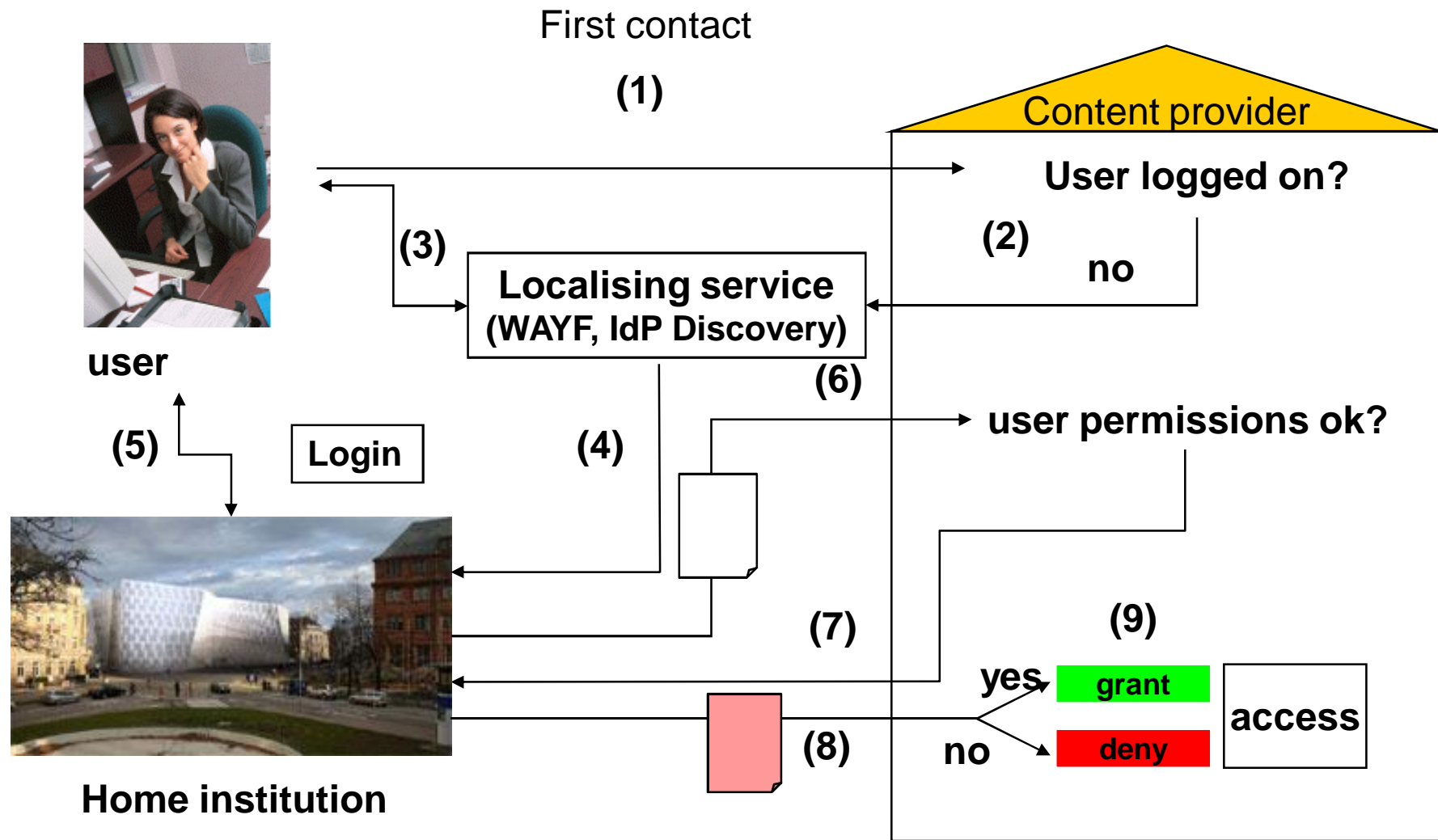
- **Shibboleth** is an **Internet2/MACE**-project
(MACE = Middleware Architecture Committee for Education)
- Shibboleth develops and provides:
 - **architecture** (protocols and profiles),
 - **structures for guidelines**
 - **Open Source-Implementation**for a cross-institutional access to protected (www)resources
- Shibboleth is based on a **federated approach**:
Each **institution administers and authenticates** its members and the contents **provider controls access** to his resources.



5 reasons for Shibboleth

- **Cross-institutional Single Sign-On**
- Authorisation and access control via **attributes** with the added possibility to access contents **anonymously or with pseudonyms**
- Based on **well established software and standards**
(SAML: XML, SOAP, TLS, XMLsig, XMLenc)
- **Integration** into an existing IdM and into (webbased) applications is - in most cases - **relatively easy**
- **High acceptance worldwide**, especially with commercial publishers (Elsevier, JSTOR, EBSCO, Ovid, GBI, CSA, ...)

How does it work?



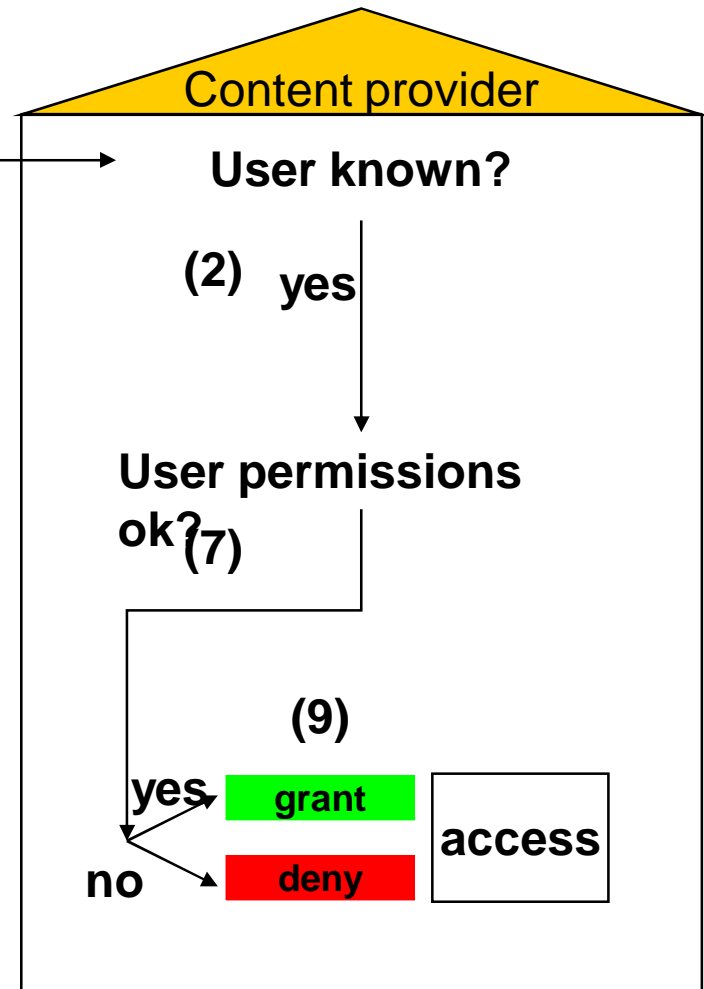
Shibboleth – how does it work?

Future contact (same provider)

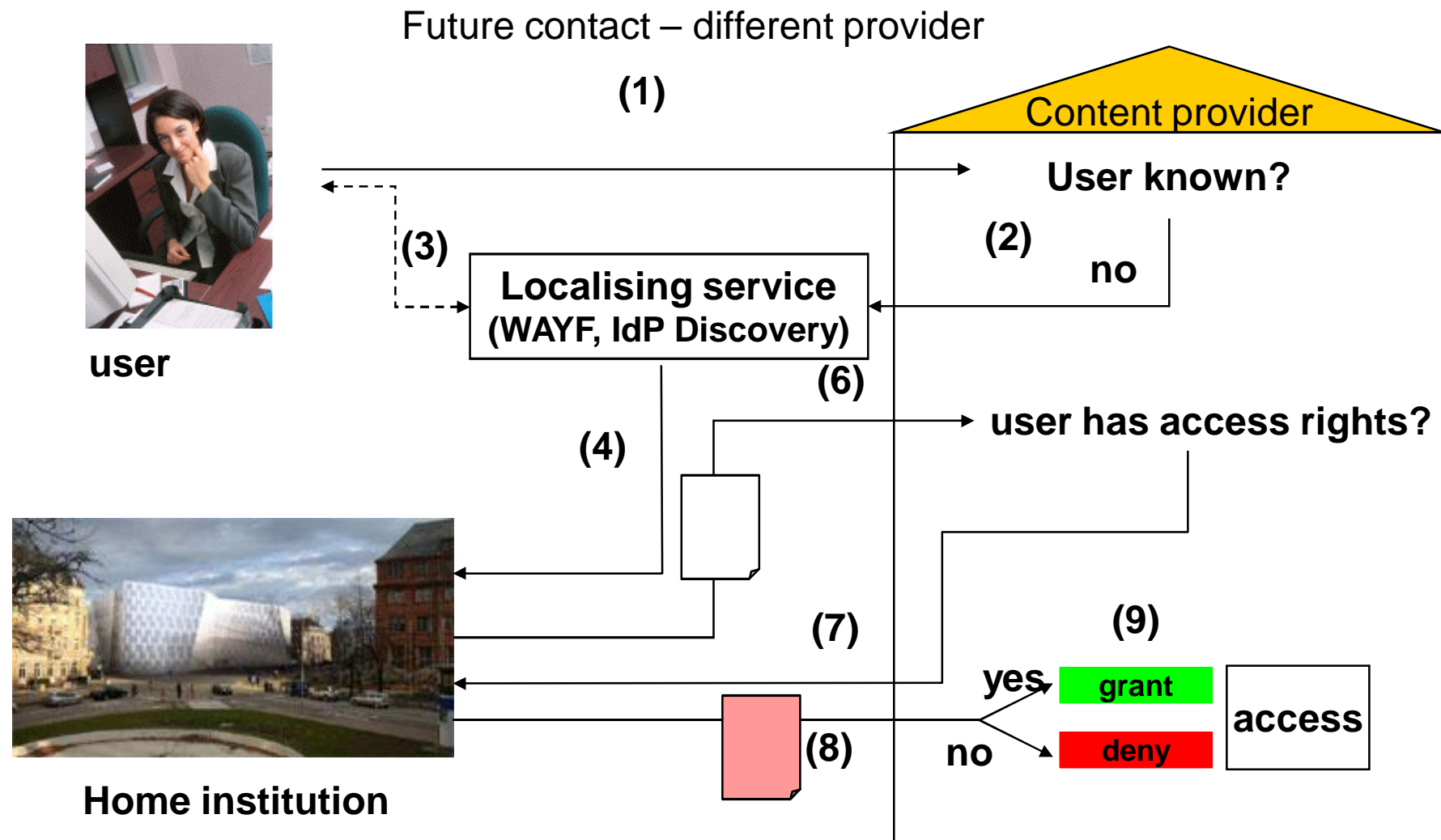


user

(1)



Shibboleth – how does it work?



The federation DFN-AAI

- **Why is there a problem?**
 - The content provider must **trust** the user
 - It is all about **money**.
 - „**trust**“ in business language means: „**contract**“.
 - You have to implement **legally binding rules** and the rector has to sign them.
 - You need binding rules for the **technical operations part**.
- **DFN-AAI** is a service of the DFN (explained later) for scientific institutions and also for (commercial) content providers.
- **DFN-AAI** provides the necessary **basis of trust** and an **organisational and technical framework** for the exchange of user information between the many users and the large number of content providers

SingleSignOn usage cases (Germany)

- Access to protected (especially commercial) electronic contents:
 - E-papers, data bases, e-portals, ...
 - Portals (e.g.. vascoda, ReDI)
 - DFG national licenses
 - Repositories
- e-Learning
- e-Science
- Administrative systems
- Grid-Computing
 - Remember the „grant access“ problem?

The **myLogin** project of Freiburg University

Basis:

- Based on the **IdM-System** of Freiburg Uni there exists **myAccount** for self administration of the individual Uni-account
- Many (internal) applications use the central IdM via LDAP

aim:

- Build a **Single Sign-On** environment for these applications
- Unified authentication and authorisation methods
- Hide LDAP behind a metaframe (IdP)
- No more login data in decentral applications (privacy....)

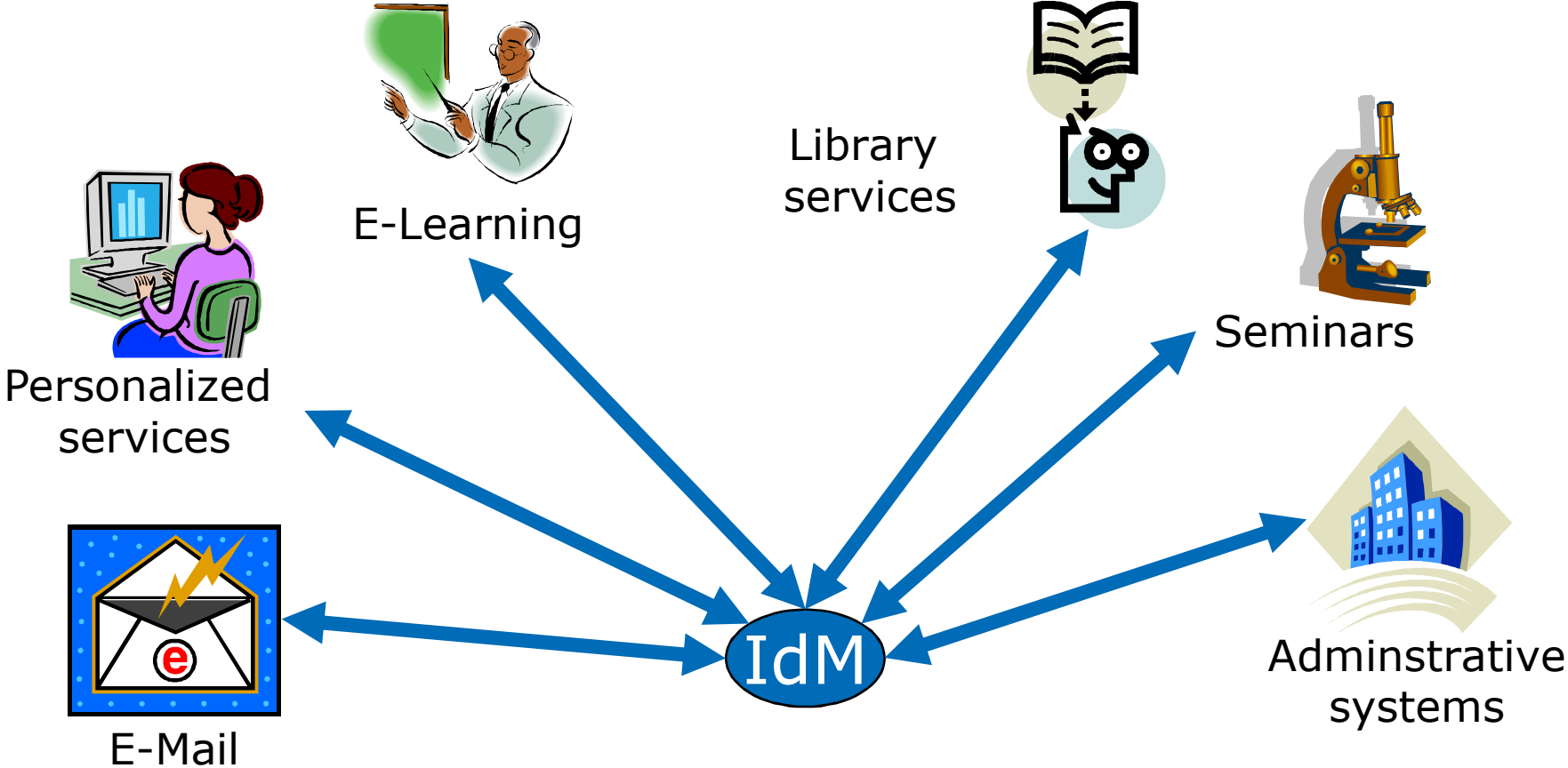
partners:

- University library (AAR): runs Shibboleth
- University IT centre (URZ): runs Uni-LDAP
- Clinical IT centre (KRZ): runs KRZ-LDAP
- Rektorate (D1): IdM data provider

Time frame:

- Start march 2007
- Start of operation 1.9.2007
- Constantly expanded to new services.

The myLogin project of Freiburg University



The myLogin project of Freiburg University



The missing link: PKI

- **Public key infrastructure**

- Certificate authority CA
- Registration authority RA
- Certificate revocation list CRL
- Directory service
- Validation authority VA

- Certificate policy
- Certification practice statement
- Policy disclosure statement

- **Strong hierarchy**

- Solution to „why should I trust someone I don't know“

Alternative approach: PGP
Trust the friends of my friends

Hard to control, hard to break
But: who is legally liable??

Do-it-yourself PKI?

- Nice to do – from the scientific „gain experience“ point of view
- But: who is interested?
 - With your own PKI you are pretty alone
- You need a larger infrastructure which ...
 - has standard contracts and conditions with you
 - can do external negotiations due to internal standards – like
 - Have the root certificate in the browsers
 - you can trust and which trusts you
- In Germany, DFN is the partner for the universities and is settled under the root certificate of Deutsche Telekom

DFN-PKI (Germany)

- We can now issue certificates
 - Generated by DFN – no own infrastructure required
 - Check passport before handing it over
 - Thus ID problem „solved“
- Thanks to the „generally accepted“ provider we can join the world wide Shibboleth federation
 - And the library can sign contracts with publishers on a reliable basis
- Suddenly everything fits together – and makes sense
 - Problem: the *high ranks* have no idea about the complexity – and won't appreciate the result