Charles University Authentication Services

Michal Voců

Charles University Computer Center

March 26, 2007

Motivation

Why authentication service?

- unified access to central web services for students, staff and external users
- single login and password for all services
- known and guranteed security level
- dissemination of personal information:
    - affiliations
    - identity cards
- simplified administration tasks (account creation, forgotten passwords, . . .)

Motivation

Why authentication service?

- unified access to central web services for students, staff and external users
- single login and password for all services
- known and guranteed security level
- dissemination of personal information:
    - affiliations
    - identity cards
- simplified administration tasks (account creation, forgotten passwords, . . .)

Simple requirements, but see later...

Use Cases

IS Web Services

- applications for accomodation
- accomodation stipendia
- information about dorm payments
- grant applications

Library Services

- Onelog — online access to information sources
- DigiTool — digital repositories

Account Management

- password reset for AD domains
- eduroam passwords

Where do the personal data come from?

- 17 faculties, more institutes and other parts
- high degree of autonomy and diversity
- each faculty uses its own instance of IS
- data is "replicated" to the central DB

Implementation – Data Sources

Where do the personal data come from?

- 17 faculties, more institutes and other parts
- high degree of autonomy and diversity
- each faculty uses its own instance of IS
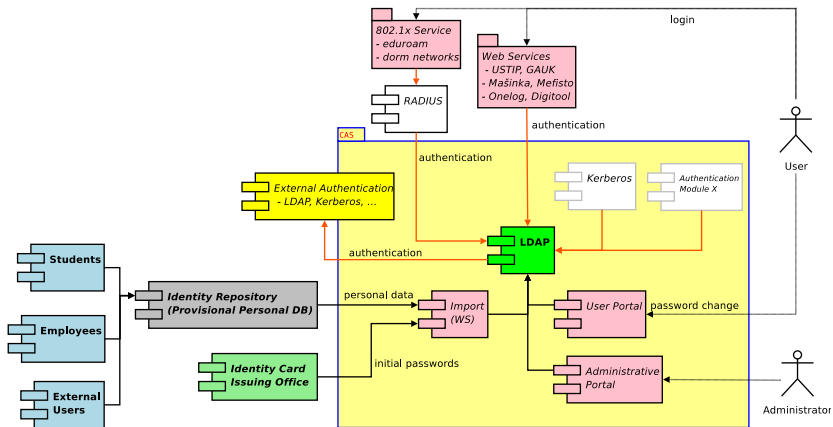- data is "replicated" to the central DB

Data sources

Student IS — single product, but tailored for faculties (sligthly different data schema, different values)

Personal IS — various applications and versions

External Users Data — obtained from interested faculties using agreed interface

Implementation – Components

Repository of Identities

- provisional personal database
- every identity has 8 digit *personal number*
- identity creation based on personal data (name, birth code)

Directory Server

- information about people (*eduPerson* standard)
- data about issued identity cards (card number, chip number)
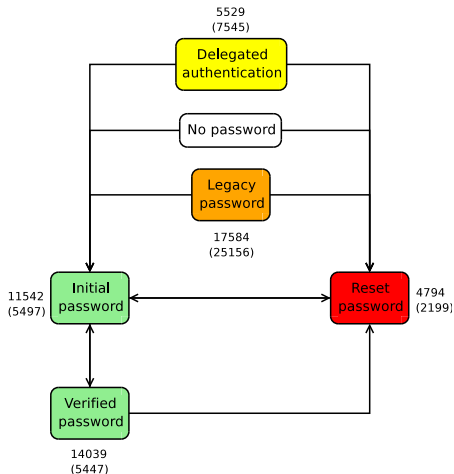- authentication information (passwords or external services)

ID Card Application

- sort of "registration authority"
- initial passwords and password reset

Web Applications

- user and management portal

Account States and Statistics

- still high number of passwords taken from applications
- growing number of verified passwords (and forgotten ones)

Conclusion and Future Work

Conclusion

- implemented identity creation, directory and authentication service
- more advanced functionality needs solving organizational issues

Future Work

- documentation
- user friendly login names
- more applications (Student IS, . . .)
- authorization service
- real identity management (if possible)
- federation projects

Questions?