www.Qbizm.cz

Qbizm® TECHNOLOGIES

... the art of information.

Single sign-on enabled OpenCms

Architecture for Single sign-on implementation into OpenCms

- **Pavel Slavíček, pavel.slavicek@qbizm.cz**
  Brno, The Czech Republic, 2. 5. 2008

Content

- **Single sign-on introduction (SSO)**
  - Introduction to Single sign-on
- **SSO protocols**
  - Basic mechanisms
  - Simplified mechanisms of CAS, NTLM, Kerberos
- **Implementation of SSO into OpenCms**
  - General architecture
  - Architecture for concrete protocol
- **Experiences**
  - Our experiences in real projects

Qbizm® TECHNOLOGIES

... the art of information.

What is Single sign-on?

Single sing-on

- **Method of access control**
- **User enters his credentials once and has access to multiple applications**
  - » Without the need to enter multiple passwords
- **Heterogeneous systems**
  - » Intranet, emails, stock system, ...
- **Comfortable for users**

Single sing-on

- **Advantages**
  - Reduces sending password over the network etc.
  - Reduces human error
  - Comfortable for users
  - …
- **Disadvantages**
  - Single sign-on component failure
  - Single sign-on component must be component with high security
  - …

Protocols for Single sing-on

- **Central Authentication Service (CAS)**
- **NTLM (NT Lan Manager)**
- **Kerberos**
- **And others**
  - **CoSign (cookie based)**
  - **OpenSSO** (Sun Java System Access Manager)
  - …

Qbizm® TECHNOLOGIES

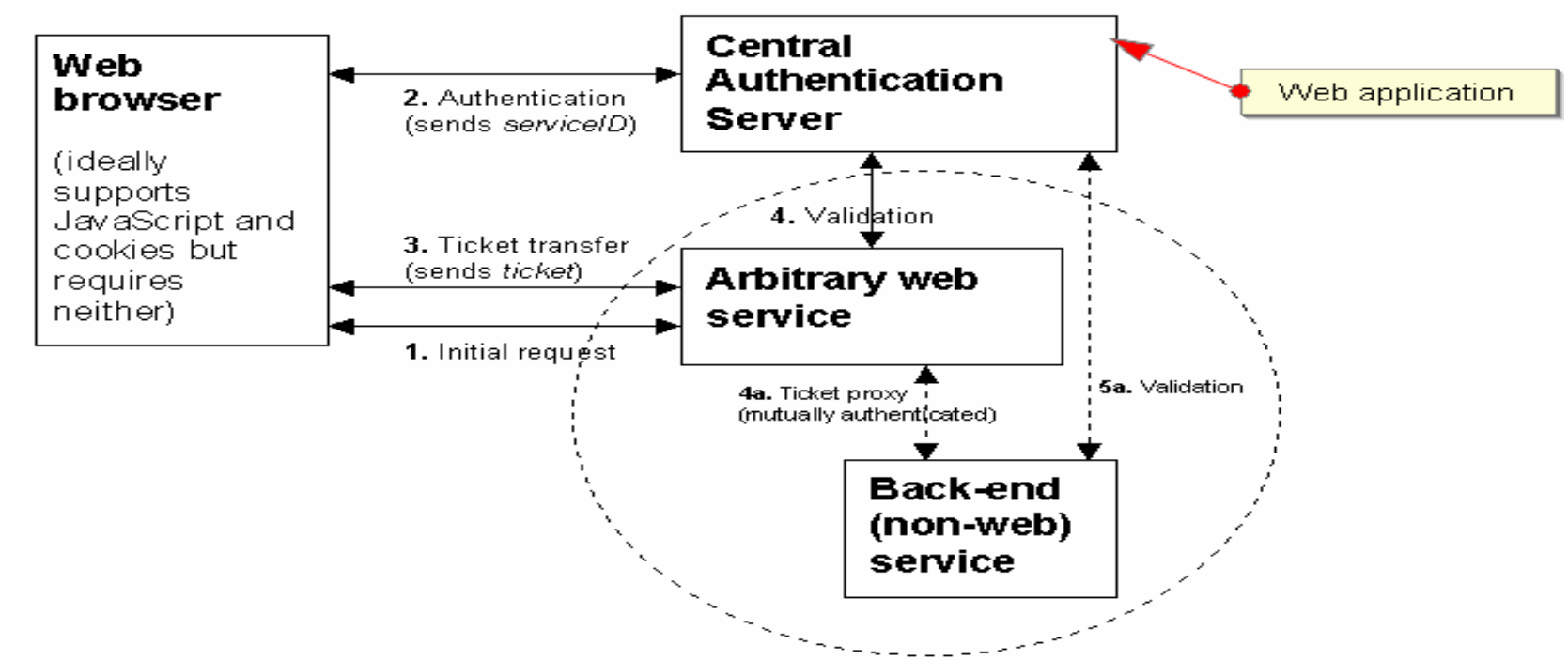
... the art of information.

Single sign-on concepts and protocols

Central Authentication Service (CAS)

- **Yale University ⇨ JA-SIG project**
- **Mostly used for web applications**
- **Features**
  - Involves a client web browser
  - Cookies based mechanism
  - Password is send over network (https)

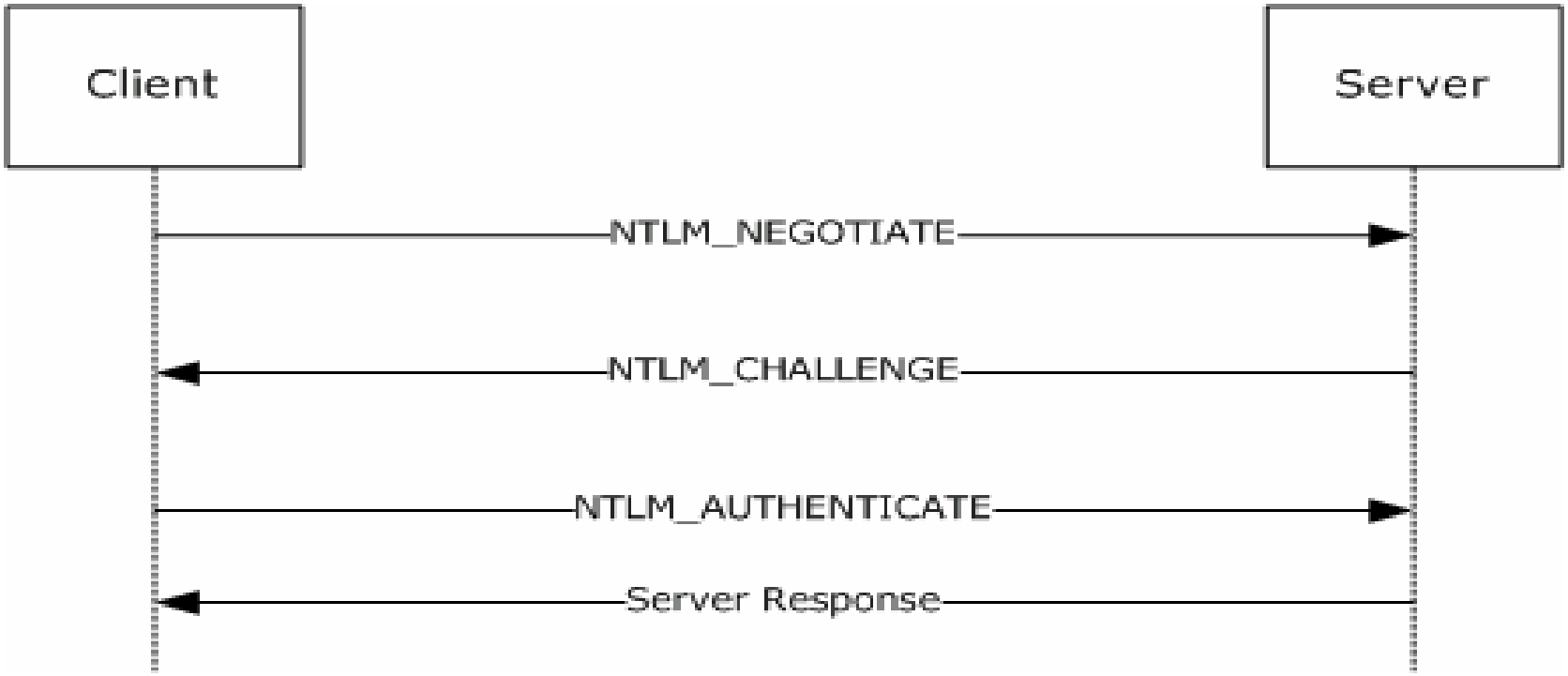
Central Authentication Service (CAS)



NTLM (NT Lan Manager)

- **Microsoft authentication protocol**
- **„Old" protocol**
  - Microsoft adopted Kerberos
  - In several cases Kerberos can't be used
- **Features**
  - Challenge-reponse sequence
  - Messages between client and server
  - Password **is not** send over the network (Hash, DES)

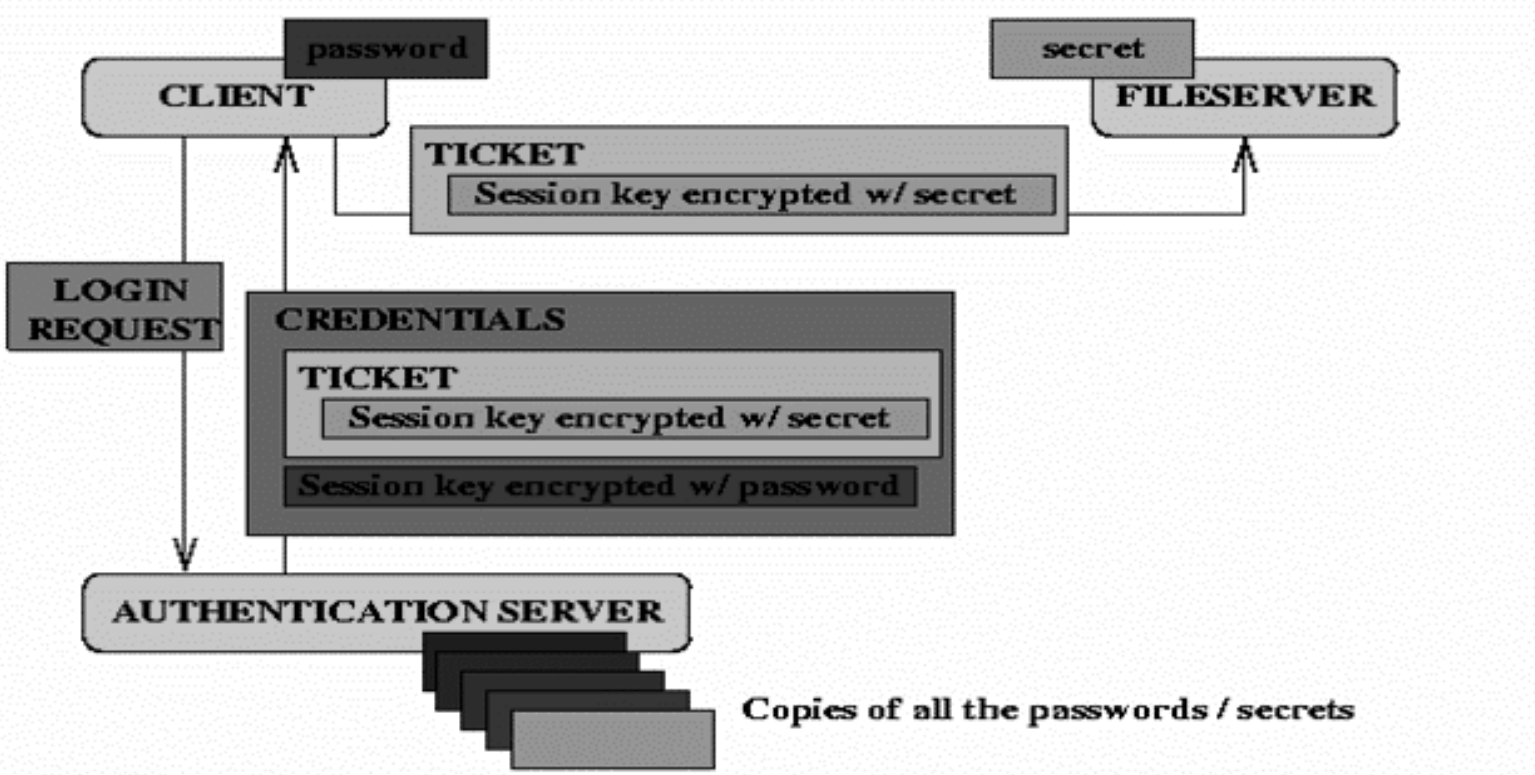
NTLM (NT Lan Manager)



Kerberos

- **Massachusetts Institute of Technology (MIT)**
- **Protocol was adopted by Microsoft**
  - Windows 2000 and Windows Active Directory server 2003
- **Features**
  - Client-server model, mutual-authentication
  - Symetric key kryptography
  - Over non-secure networks (eavesdropping, replay)
  - Password **is not** send over the network

Kerberos


password
CLIENT
secret
FILESERVER
TICKET
Session key encrypted w/ secret
LOGIN REQUEST
CREDENTIALS
TICKET
Session key encrypted w/ secret
Session key encrypted w/ password
AUTHENTICATION SERVER
Copies of all the passwords / secrets

Qbizm® TECHNOLOGIES

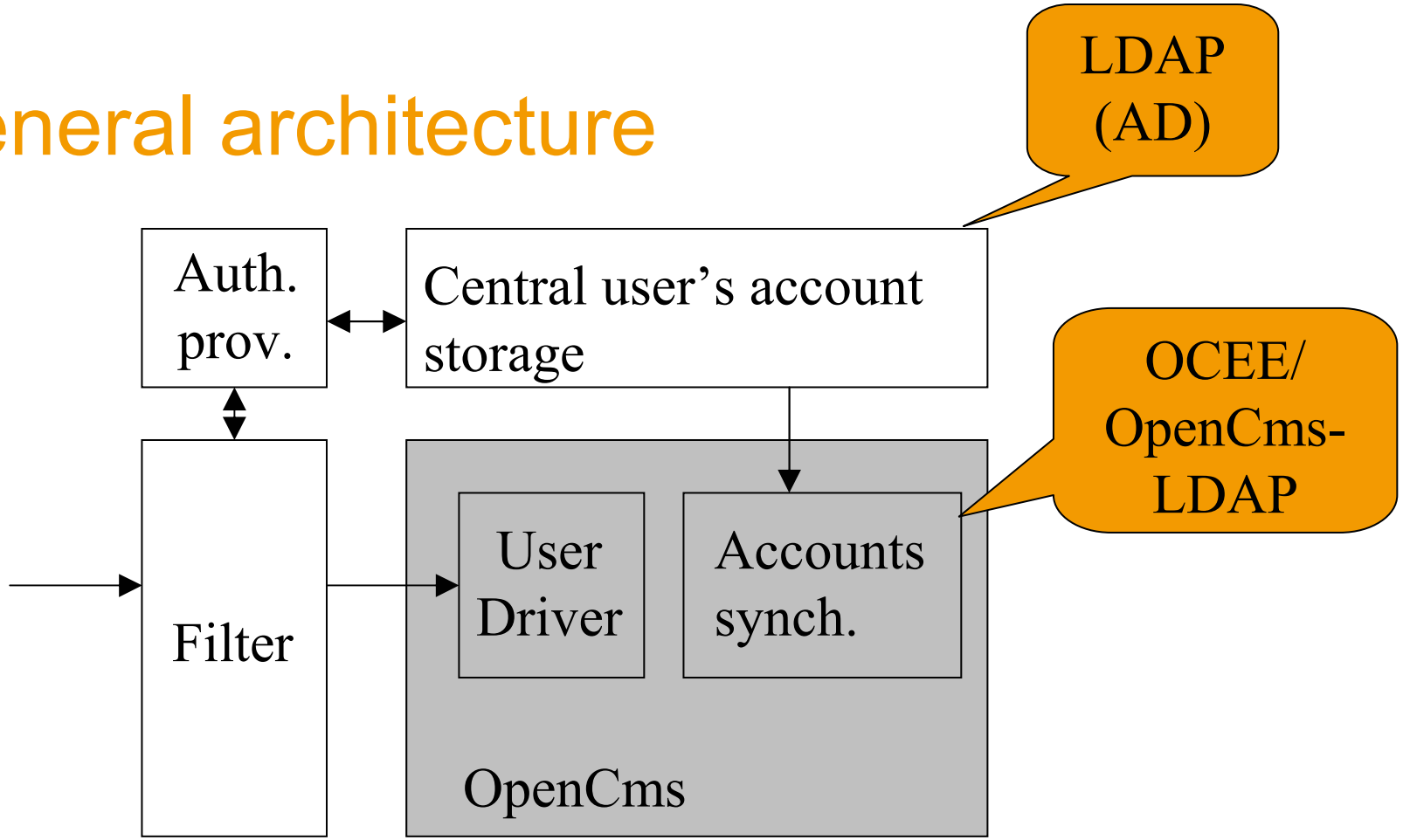
... the art of information.

Architecture for SSO implementation into OpenCms

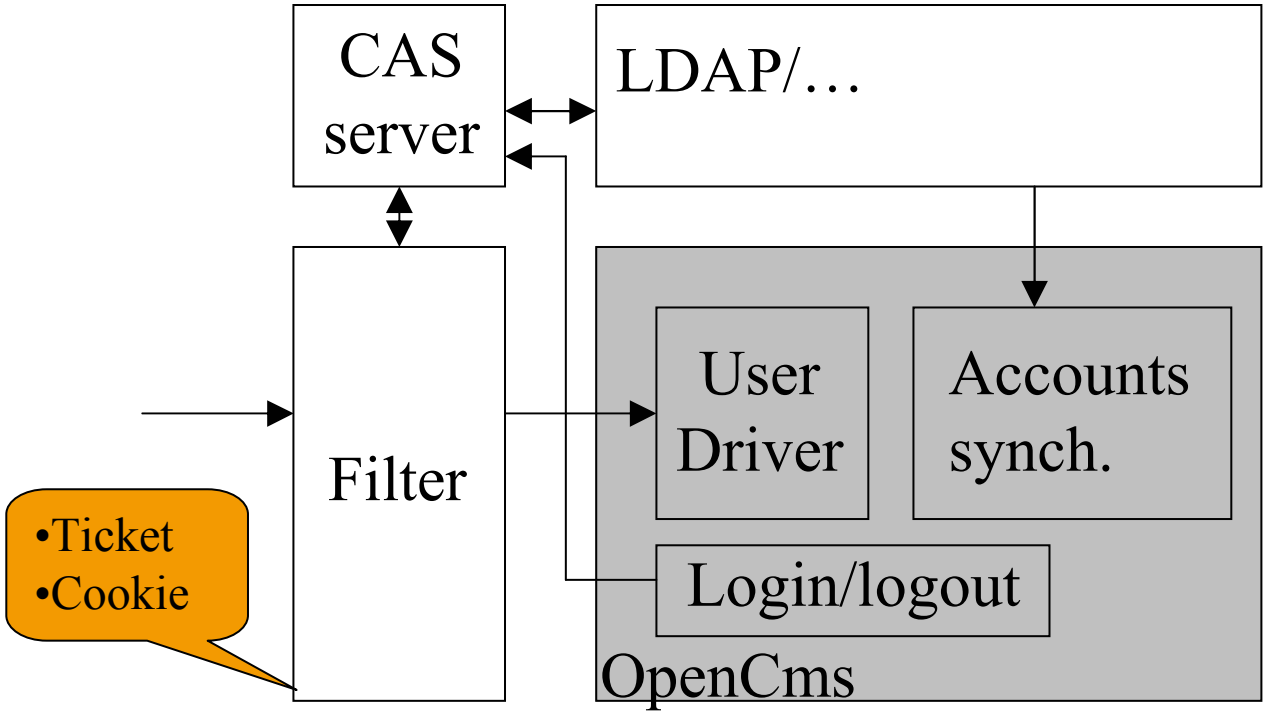
General architecture

- **Concrete architecture depends on chosen Single sing-on protocol**
- **We do not have user's password**
  - We have to trust to Single sing-on component
  - Special authentication mechanism
    - We have to implement own user driver
    - User name transforming
    - We have to modify authentication mechanisms in OpenCms
- **Central user's account storage**
  - User's account synchronization from LDAP server
    - **OCEE Modules** from Alkacon
    - OpenCms-LDAP module from sourceforge.net

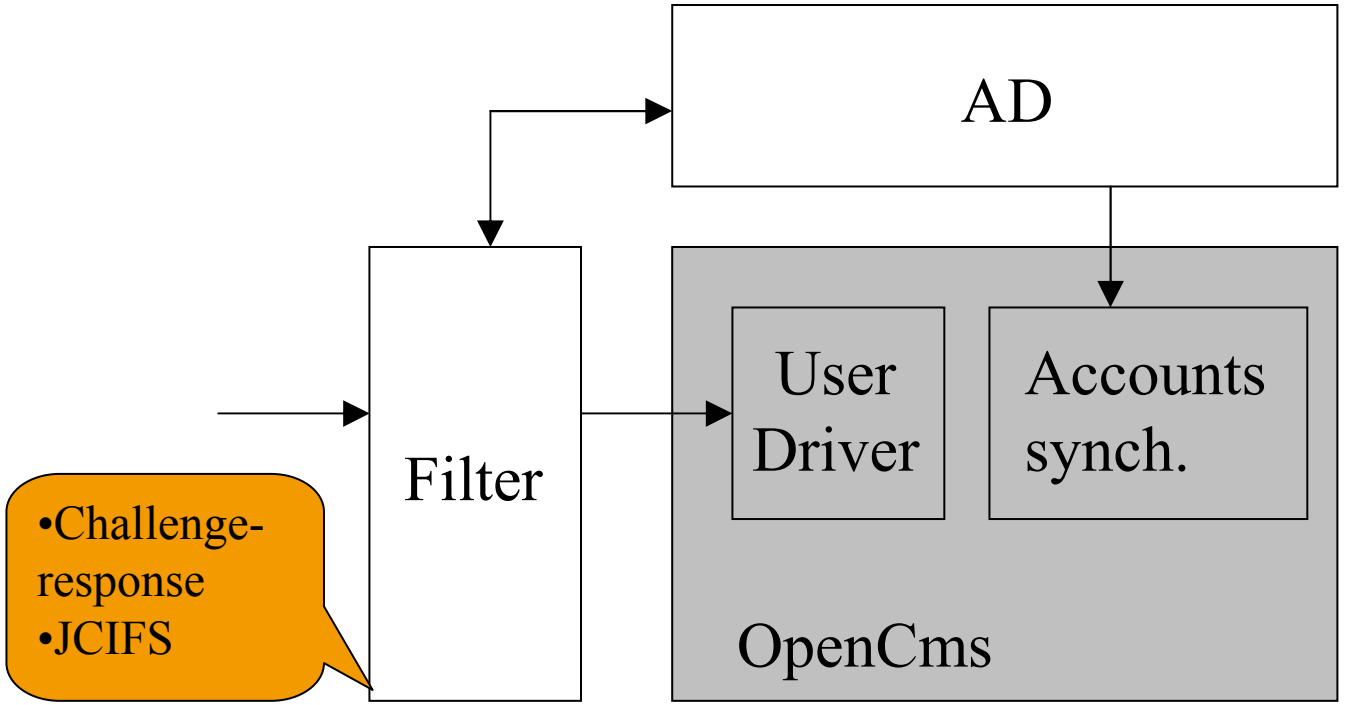
General architecture



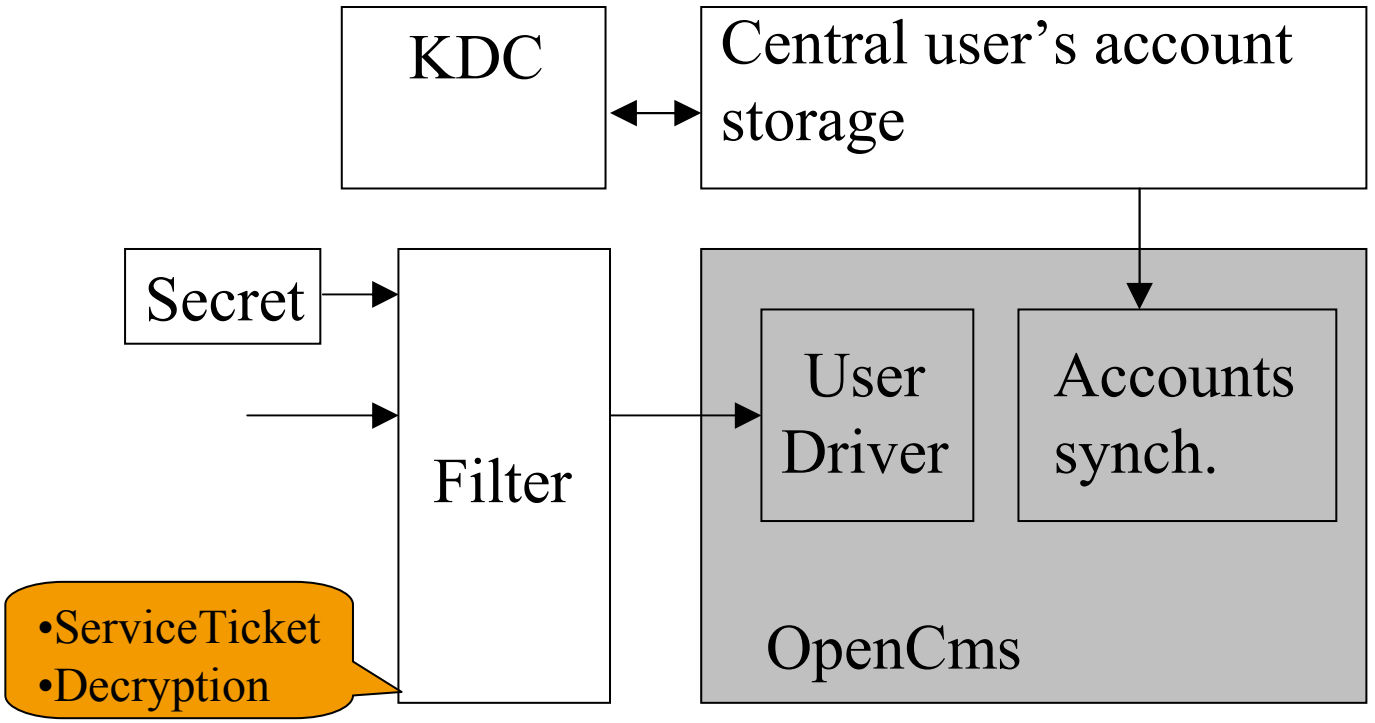
CAS


CAS server
LDAP/…
Filter
User Driver
Accounts synch.
Login/logout
OpenCms
•Ticket
•Cookie

NTLM


AD
Filter
User Driver
Accounts synch.
OpenCms
•Challenge-response
•JCIFS

Kerberos


KDC
Central user's account storage
Secret
Filter
User Driver
Accounts synch.
OpenCms
•ServiceTicket
•Decryption

Qbizm® TECHNOLOGIES

... the art of information.

Experiences with Single sign-on

Experiences with Single sing-on in real projects

- **Popular, user friendly**
- **Good feedback from customers**
- **Projects**
  - CAS
    - Intranet/extranet
    - Over 30 000 of users
  - NTLM
    - Intranet, company with affiliates
    - About 5 000 of users
  - Kerberos
    - Intranet

Summary

- **Single sing-on is attractive for customers**
- **Usefully for intranets**

- **Architectures of modules were presented**
- **Implementation of our modules are based on presented architectures**
  - » Knowledge of Single sing-on mechanisms

- **Thank you for your attention, any questions?**

References

[1] Introduction to Single Sign-On,
http://www.opengroup.org/security/sso/sso_intro.htm/

[2] Single sign-on,
http://en.wikipedia.org/wiki/Single_sign-on

[3] Central Authentication Service,
http://en.wikipedia.org/wiki/Central_Authentication_Service

[4] NTLM,
http://en.wikipedia.org/wiki/NTLM

[5] Kerberos,
http://en.wikipedia.org/wiki/Kerberos_(protocol)

[6] The Java CIFS Client Library,
http://jcifs.samba.org/

[7] JA-SIG Central Authentication Service,
http://www.ja-sig.org/products/cas/

[8] TagLab,
http://dev.taglab.com/

[9] Single Sign On Concepts & Protocols,
http://www.sans.org/reading_room/whitepapers/authentication/1352.php