Single Sign-on to the Grid

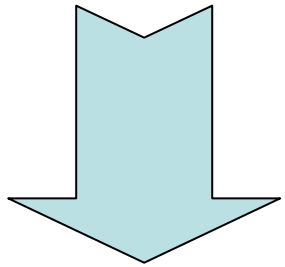
Authentication and Integrated Identity Management

HEPiX, CASPUR, Rome
3-7 April 2006

Jens G Jensen
CCLRC e-Science

The Problem

- Integrated Access (Authentication)
- Identity management
- Implemented locally…
- …integrate with future national efforts…
- …and international



National Grid Service
core production computational and data grid

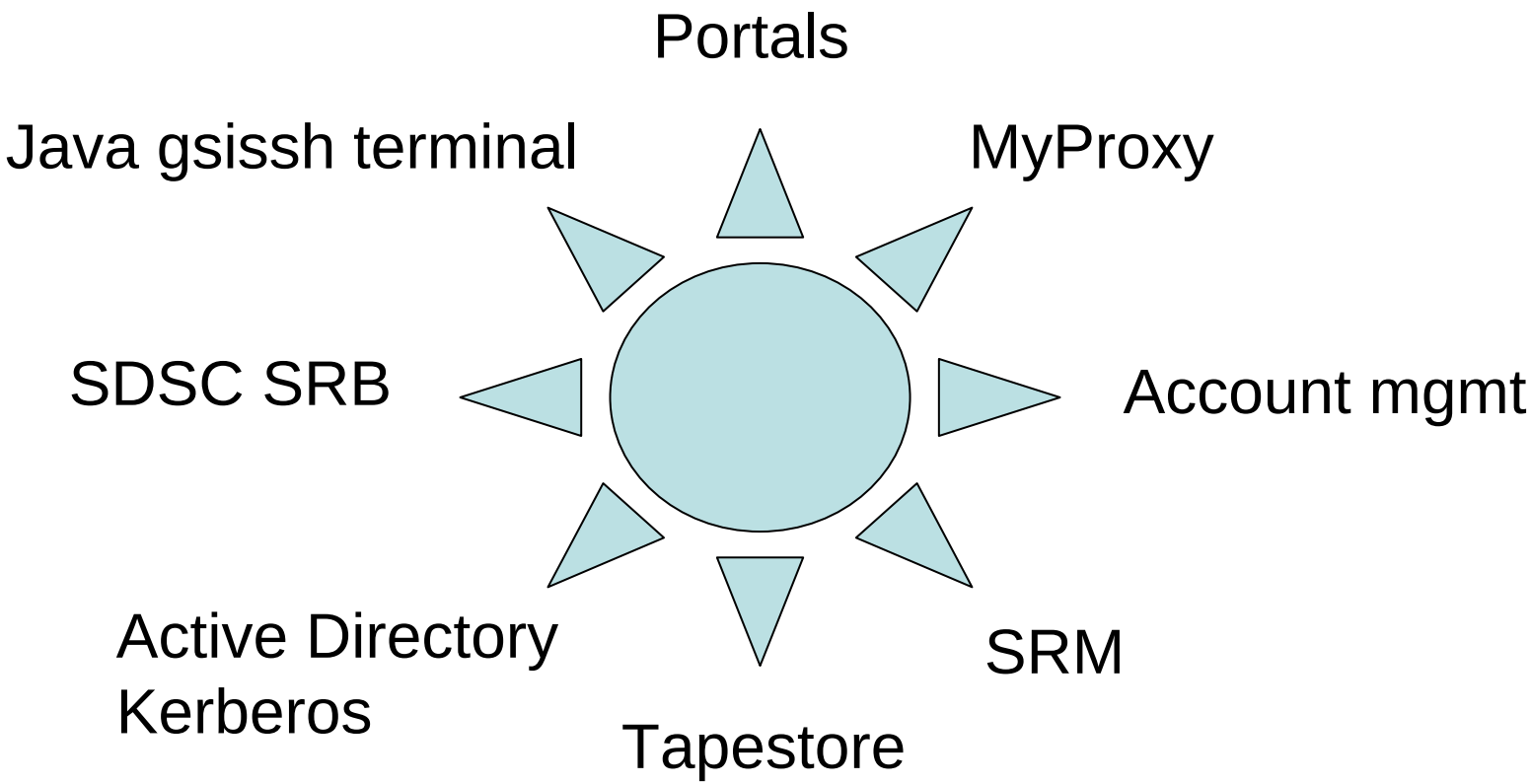
Jens G Jensen
CCLRC e-Science

What's in SSO?

- More than just "type password once"
- Identity mgmt, User mgmt
- Credential conversions
  - Certificates, AD/K5
  - Protection of credentials
- Thin clients vs thick clients
- Passwords and –phrases validation
  - Single password to all resources

Jens G Jensen
CCLRC e-Science

What's in SSO (authentication)?



Challenge: get distinct components to talk together

Authentication – web based

- If on-site, use federal id (Active Directory/Kerberos)
- If off-site, use certificate
  - if loaded into browser
- Otherwise username/password
  - Same as fed username/password
  - Not allowed to store password…
- System must know these are the same

Java SSH Term

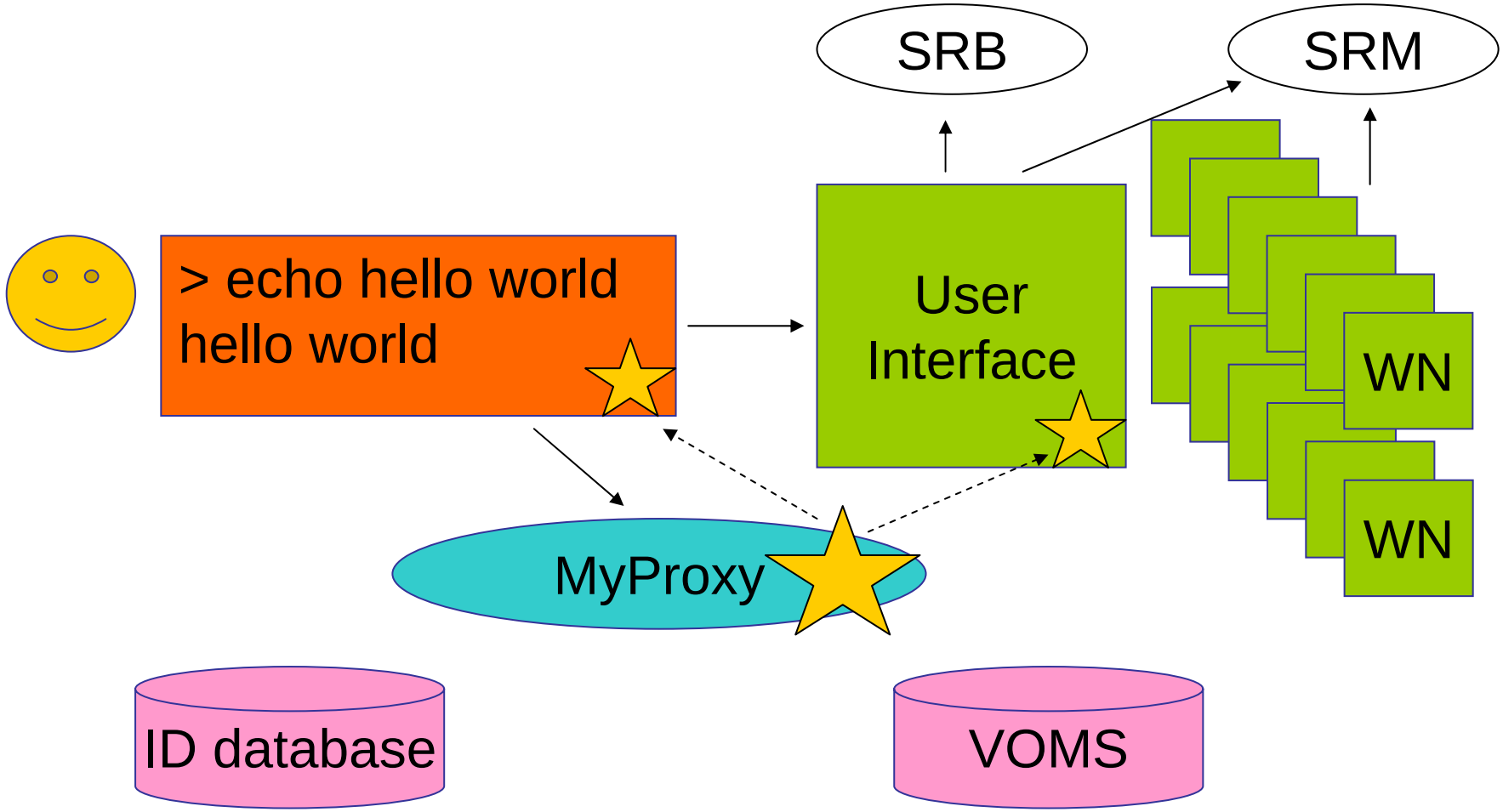
- Written in Java (no, really)
  - Standalone – untar and run
  - Applet
- xterm
  - Understands (most) ANSI control seqs

Jens G Jensen
CCLRC e-Science

Java SSH Term

- Took open source terminal (in sf.net)
- And GSISSH plugin contrib'd from Canada
- And developed:
  - Integration with myproxy
  - Various tweaks and fixes

Java SSH Term



Jens G Jensen
CCLRC e-Science

Java SSH Term

- Integrate with site Active Directory
- Works!
- But only with Java 1.6
  - Available in beta

Java SSH Term – User view

- Use “proper” Grid (X.509) cert
  - Upload a proxy to myproxy once a week
  - Terminal gets proxies where you need them
- Or use a proxy from the built-in CA
- No need for PKCS#12 → PEM conv
  - Or even no need for understanding certs

Jens G Jensen
CCLRC e-Science

Java SSH Term – Admin view

- Can shut down vanilla ssh
- Key mgmt is Somebody Else's Problem™
- Decreased support load…(potentially)
- Must trust a MyProxy CA
  - UK: Tie into CA hierarchy

Java SSH Term

- Try it!
- http://www.grid-support.ac.uk/

Jens G Jensen
CCLRC e-Science

User Management

- DLS and ISIS have 14-15000 users
- Already ~6-7000 unique users in DB
  - How to establish – and maintain – uniqueness?
- Users get accounts locally
  - Accounts set up by User Office ☺
  - Give them Unix UID?
    - RFIO and NFS use 16 bit UID… ☹

Vintela

- Used by Diamond Light Source (synchroton) – not all of CCLRC/RAL
- Commercial
- Manage user accounts across Linux and Windows
- Uses RFC2307-with-extensions
  - "Make more scalable"
- Caching daemon makes system scalable

Vintela

- “Active Roles”
- Users can unlock their own accounts
  - Questions
- Scriptable user creation
- NSS module for NIS
- PAM module calls out to Active Directory
- Suport for RH, SuSe, Solaris, HPUX, AIX

Future work

- Better database integration (eduPerson++)
- Related Shib work with Oxford
  - Now funded, 2 p.yr.
- Authorisation
  - VOMS integration
- Ponder credential conversions/protection
  - Need extra info (staff, temp'ry, visitor)
  - Work on-going between CAs in IGTF

Future work

- Integrate Grid services with UK-wide infrastructure (JISC)
  - Shibboleth for all higher and further ed
  - Lots of add'l middleware effort
- CCLRC involved in writing JISC 10 yr AAA roadmap

Summary

- Terminal access to Grid
  - In production
  - Non-certificate access via myproxy
    - To integrate with CA rollover
  - Handles all grid-proxy-init
- Much of account mgmt solved
- Integrating with future SSO efforts