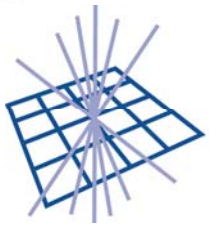
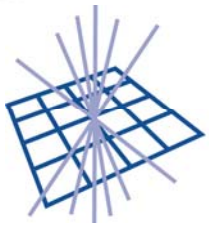


Portal Authentication and SSO

EGEE portal authentication workshop

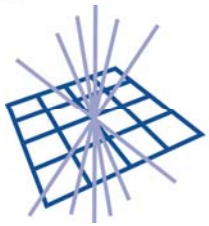
CERN, 2-3 May 2007

Jens Jensen STFC RAL
<j.jensen@rl.ac.uk>



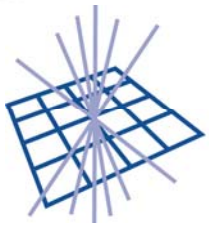
Contents

- Single Sign-on, where art thou?
- Credential Conversion
  - Hereinafter “CC”
- Portals in NGS
- SSO with a Real Life™ Alternative to Portals
- Robots in UK e-Science CA



SSO

Or how I learned to stop worrying
and start loving the Grid



Five steps to SSO

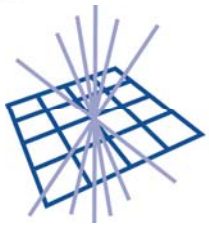
1. Account management: each user has a single registration
2. Single password: a single password is used to unlock all resource accounts
3. Single authentication – each user must type the password only once
   - Per day, per week, per login

Five steps to SSO

4. Credential gymnastics - CC
   - GT2 delegated proxies
   - Accommodate thin and thick clients
   - Support legacy apps
5. Delegation
   - (beyond scope of this talk)

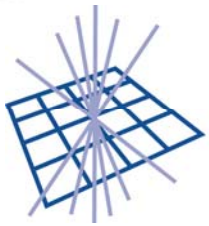
CC goals – web based

- 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



Web (HTTPS) based SSO

- Easier to implement servers
  - Apache can do Everything™
  - Not always trivial to integrate with existing portals
  - Apache vs Tomcat, StringBeans, uPortal, CHEF, SAKAI,…(insert portal framework du jour)
- Lots of HTTP tools that understand security
- Future proof, when UK goes to Shibboleth



Credential Conversion

Or how I learnt to stop worrying about one thing and start worrying about another

Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

MyProxy

- MyProxy useful for SSO to Grid
  - Because Grid requires X.509 certs
- Call out to site authentication
  - For username/password maintenance
- Investigating new MyProxy+PAM

NGS National Grid Service
core production computational and data grid

Status – Users

- Need certificates for Grid work
- Using e-Science certificate
  - Once every *year*, obtain/renew cert
  - Once every *week*, renew proxy
    - Upload tool in Java, another in python
  - Once every day
    - Log in to Windows (or Linux kinit)
- Or, …

Status - Users

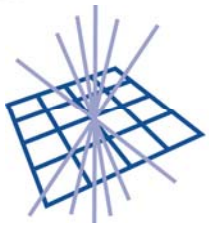
- Or, have MyProxy generate the certificate
  - Using built-in CA
  - Trust issues – MyProxy is local (SSO), or, in any case, not an accredited CA

Status – software

- Prototype portal (python)
  - Thin clients (web browser)
  - Fetches proxy from myproxy
  - AD/K5 works with IE and certain Linux browsers
- Components for thick clients
  - Fetches proxy locally from MyProxy

Status - Software

- Portal framework du jour
  - uPortal, StringBeans,
  - Some easier to SSO than others



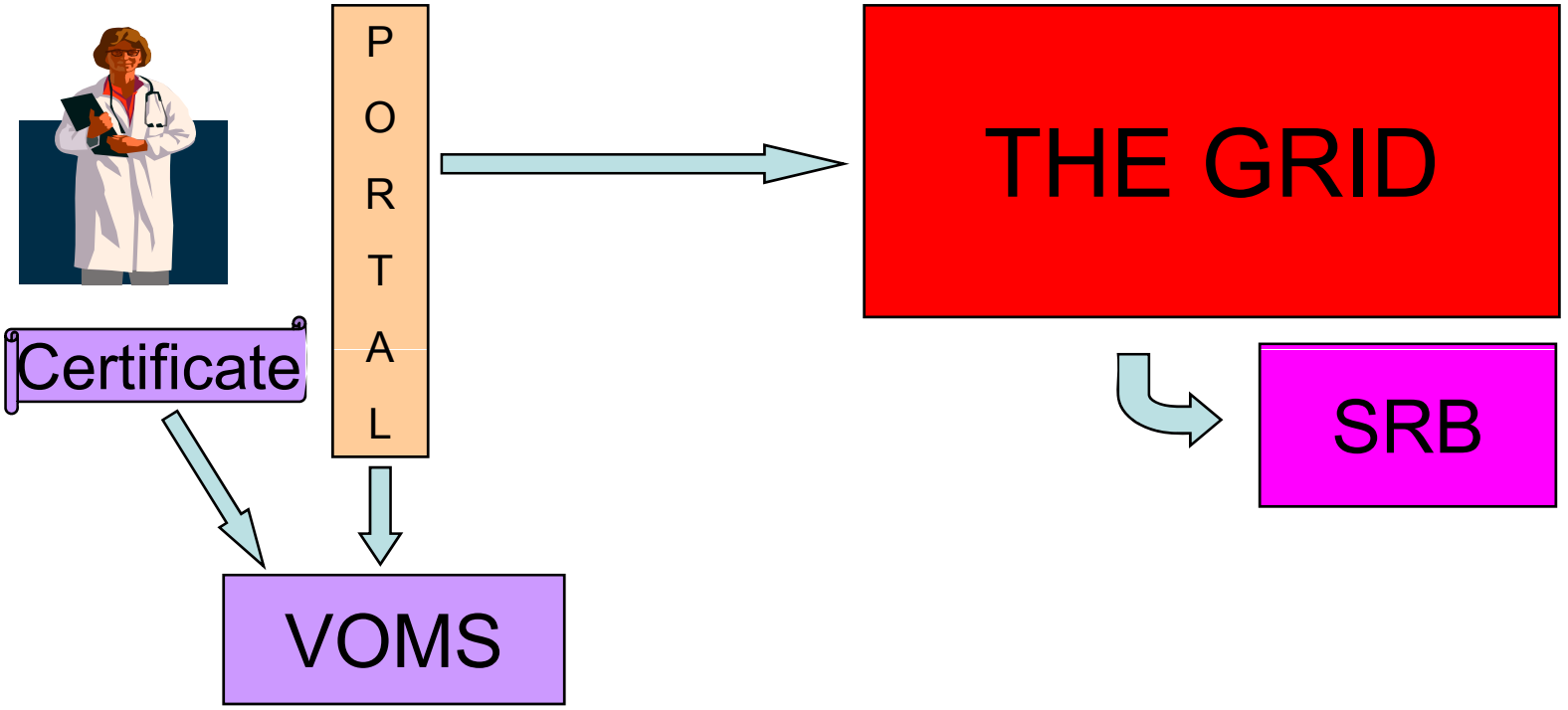
Portals and Authentication

Or how I learnt to start worrying about my deadlines

Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

Client Side – from outside



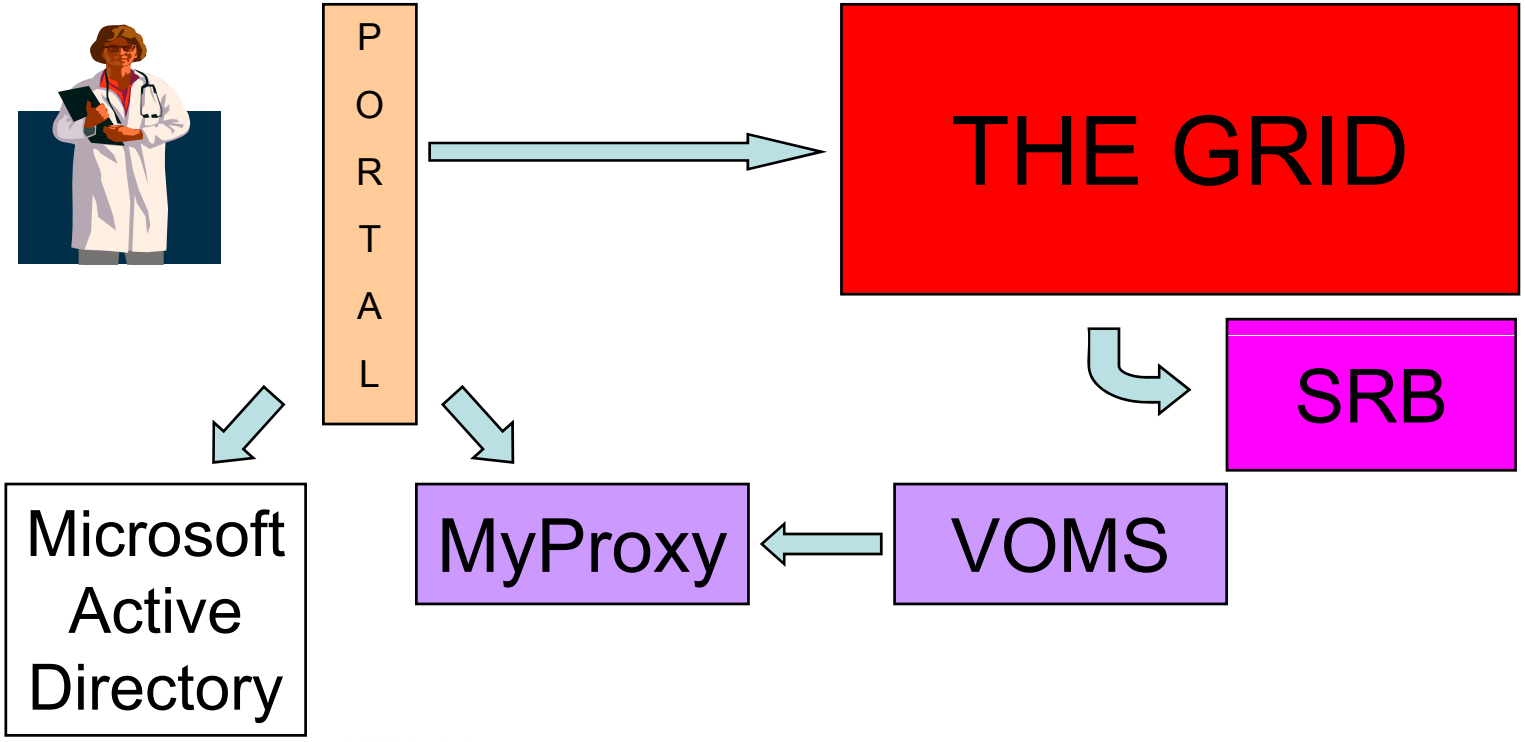
NGS National Grid Service
core production computational and data grid

(old slide)

Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

Client Side – from within



NGS National Grid Service
core production computational and data grid

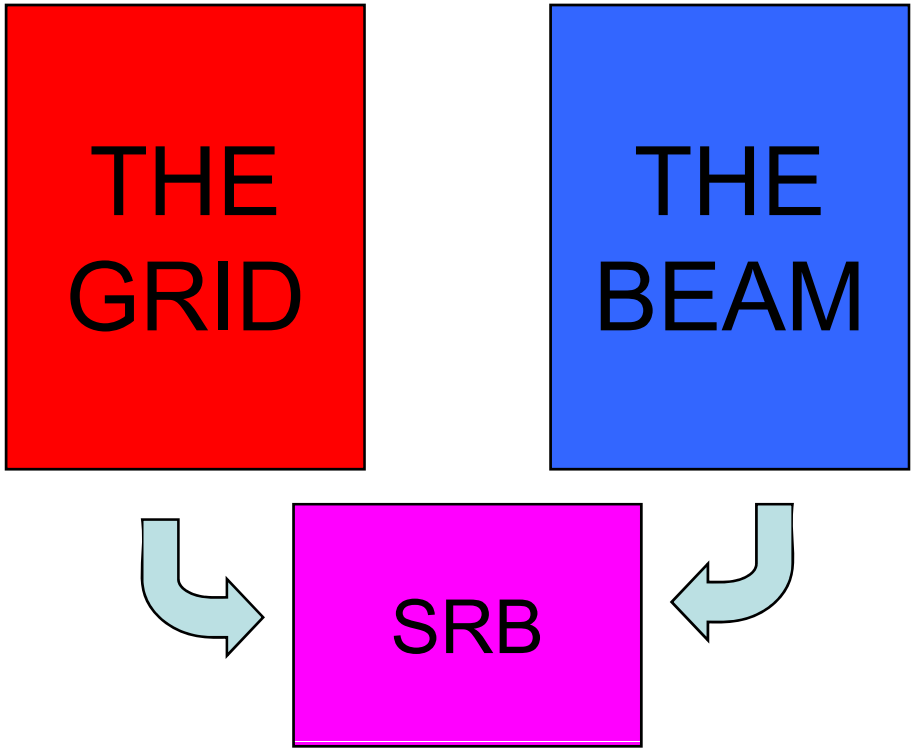
(old slide)

Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

SRB

- SRB provides SSO
- But ∫ with everybody else's…
- S commands can be used with GSI and with username/password
- inQ doesn't understand certificates

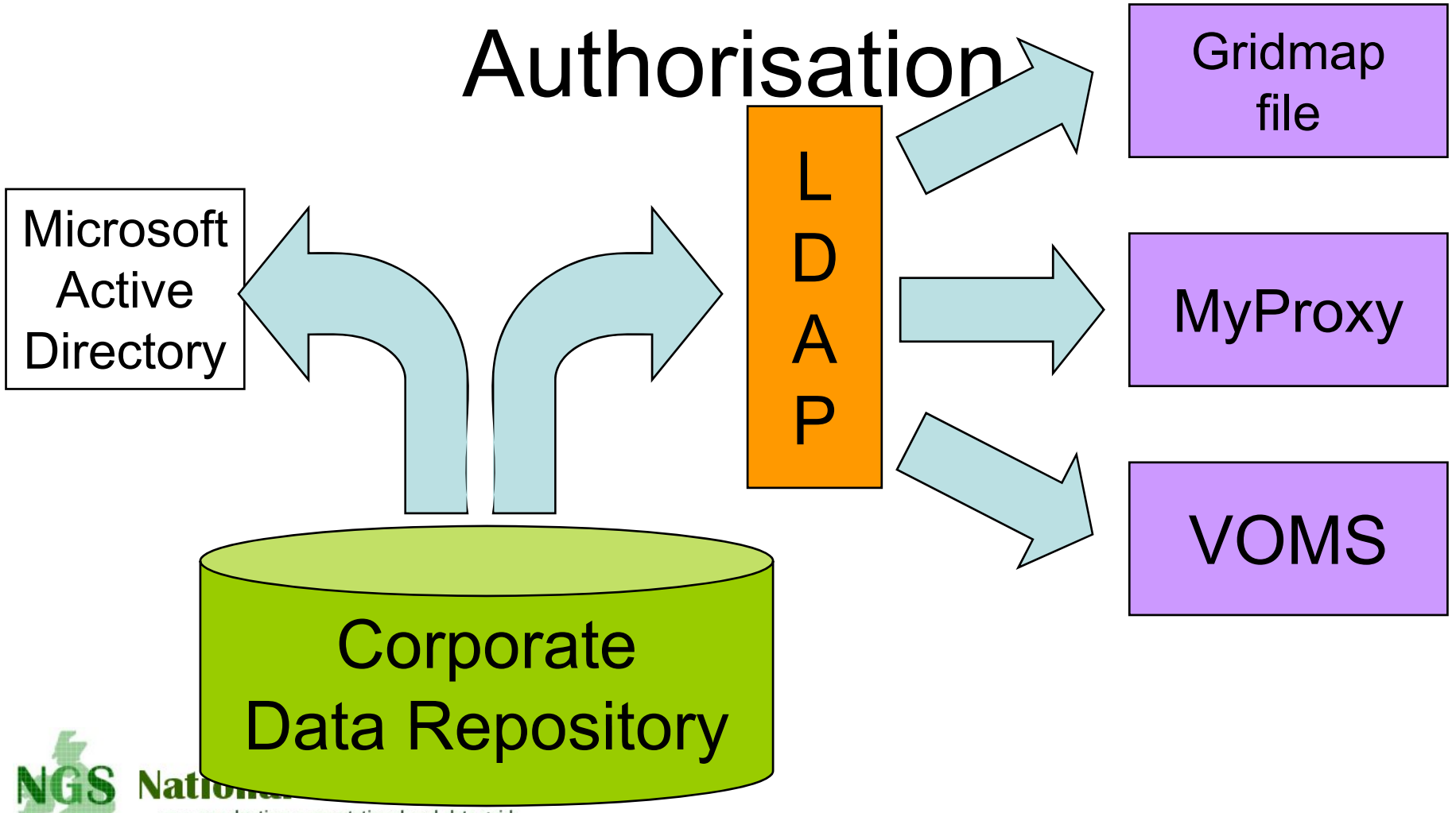


NGS National Grid Service
core production computational and data grid

Authorisation Model

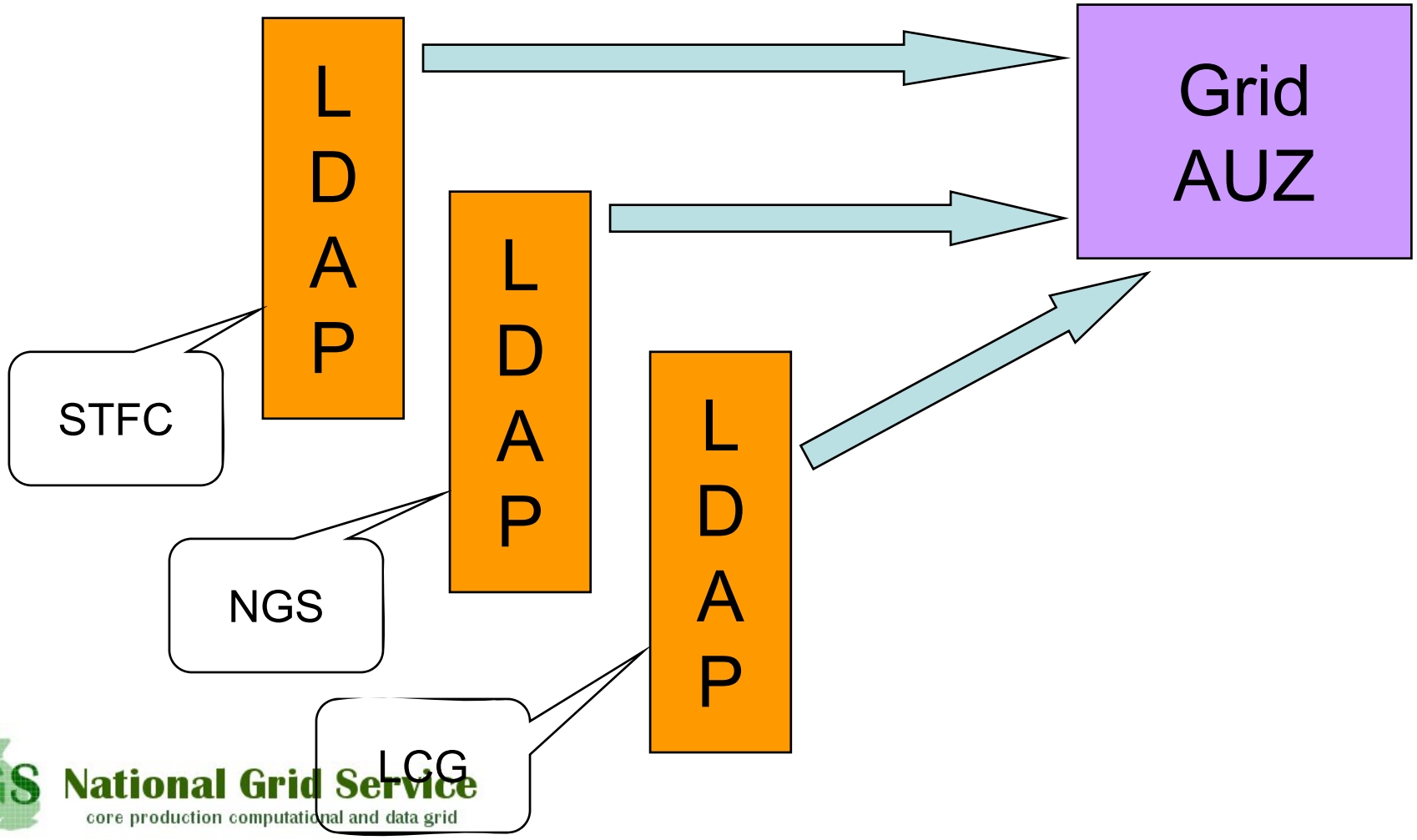
- Delegate authorisation?
- Need to authorise to multiple resources

Authorisation



Science & Technology Facilities Council

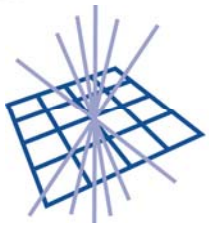
GridPP
UK Computing for Particle Physics



NGS National Grid Service
core production computational and data grid

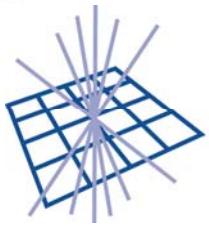
Using Institution IdP

- Puts identity management in institution
  - That's good – they do it anyway
  - That's bad – the CA has no control
    - Associate DN with identity
    - Institute does not (usually) release information
    - Institute does not describe vetting policy
  - So lower assurance then…



Using Institution IdP

- Solves scalability problem
- Shibboleth does this too!
  - Why not use Shibboleth then?
- We do!
  - ShibGrid (not to be confused with GridShib)
  - SHEBANGS



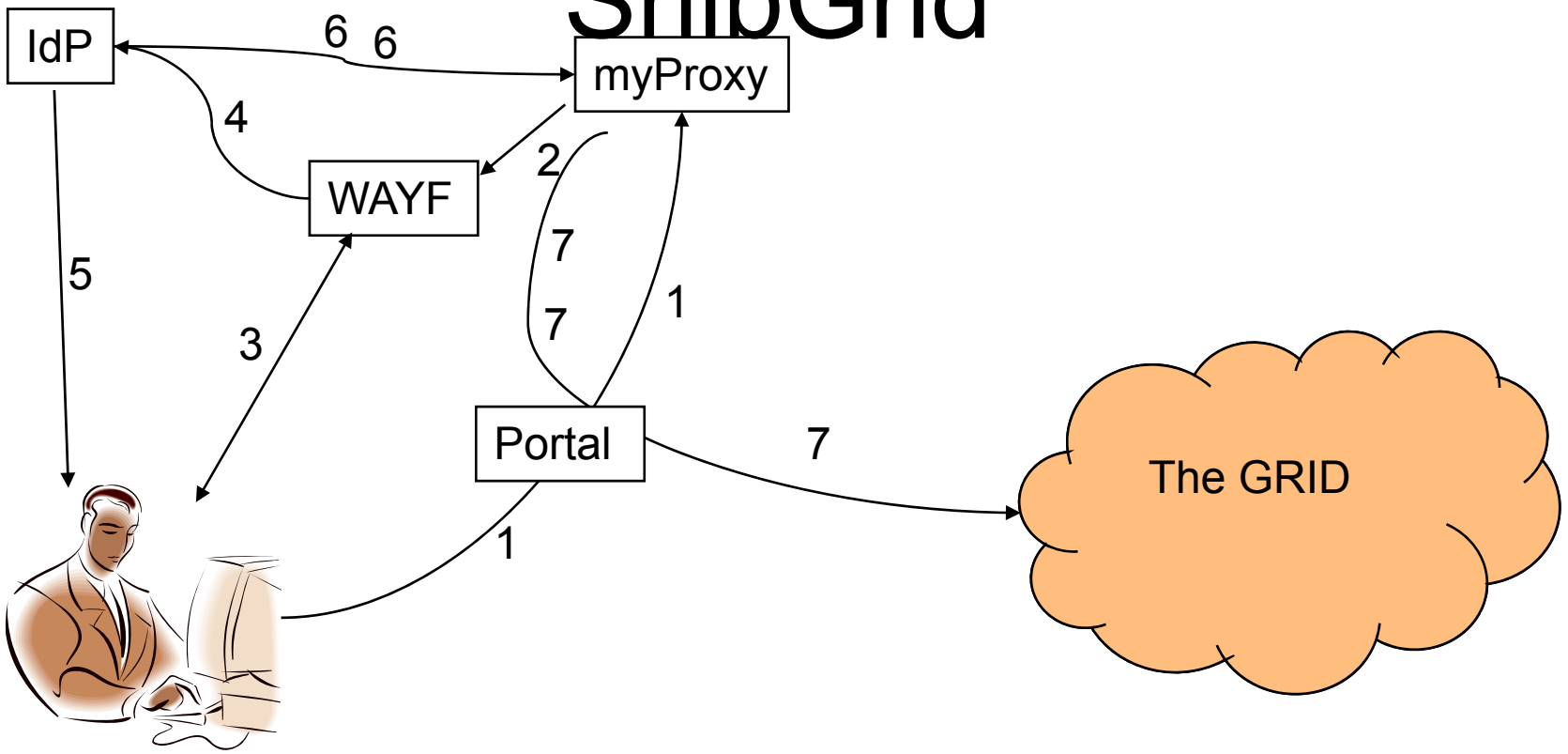
Comparing CC to Shibboleth

- Complementary – coexist with Shib
- Simpler – no need for attributes (at this level)
- Simpler – used only to access Grid
- Simpler – no WAYF but on site only
- Joining is infinitely cheaper
  - Driven by the NGS Grid, not institution
  - Some similar data protection issues

Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

ShibGrid



-Upload and download certificates to myProxy
-(this slide stolen from NG)

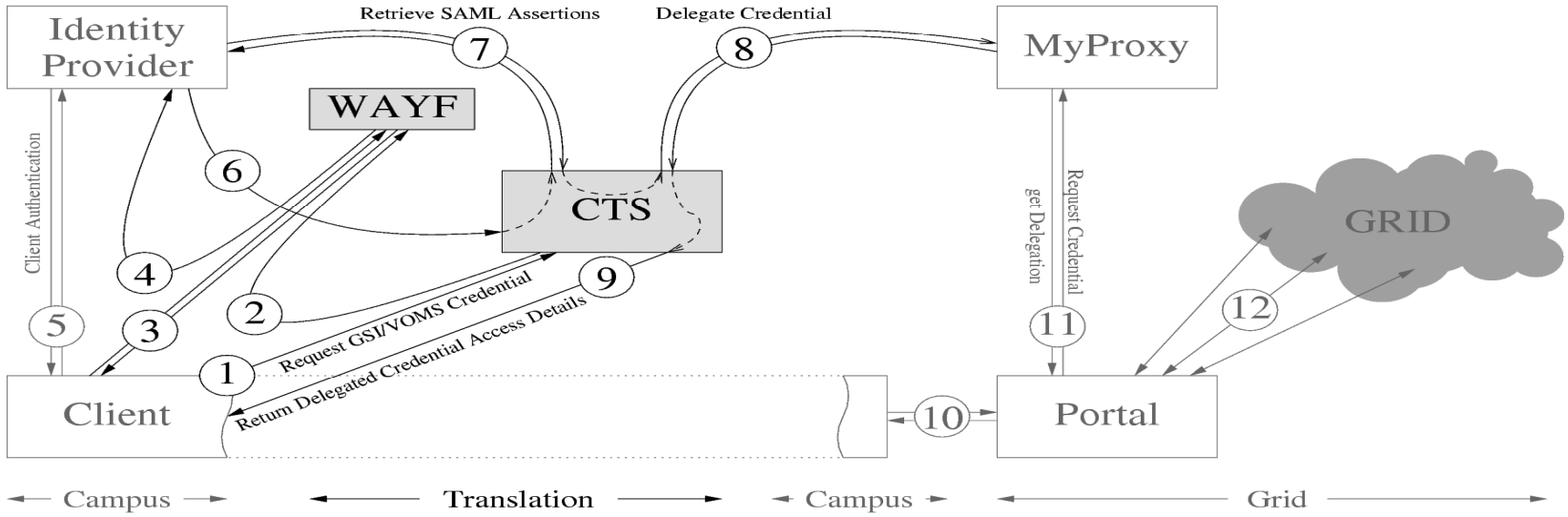
NGS National Grid Service
core production computational and data grid

Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

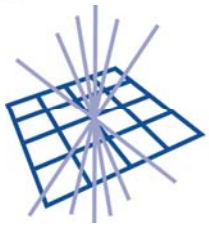
SHEBANGS

Integrates VOMS attrs into credential



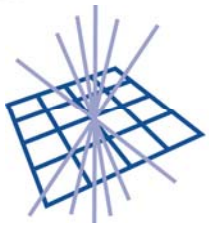
NGS National Grid Service
core production computational and data grid

(Image from SHEBANGS)



A Real Life™ Alternative to Portals

Or how I learnt to stop worrying and get on with my work



Java SSH Term

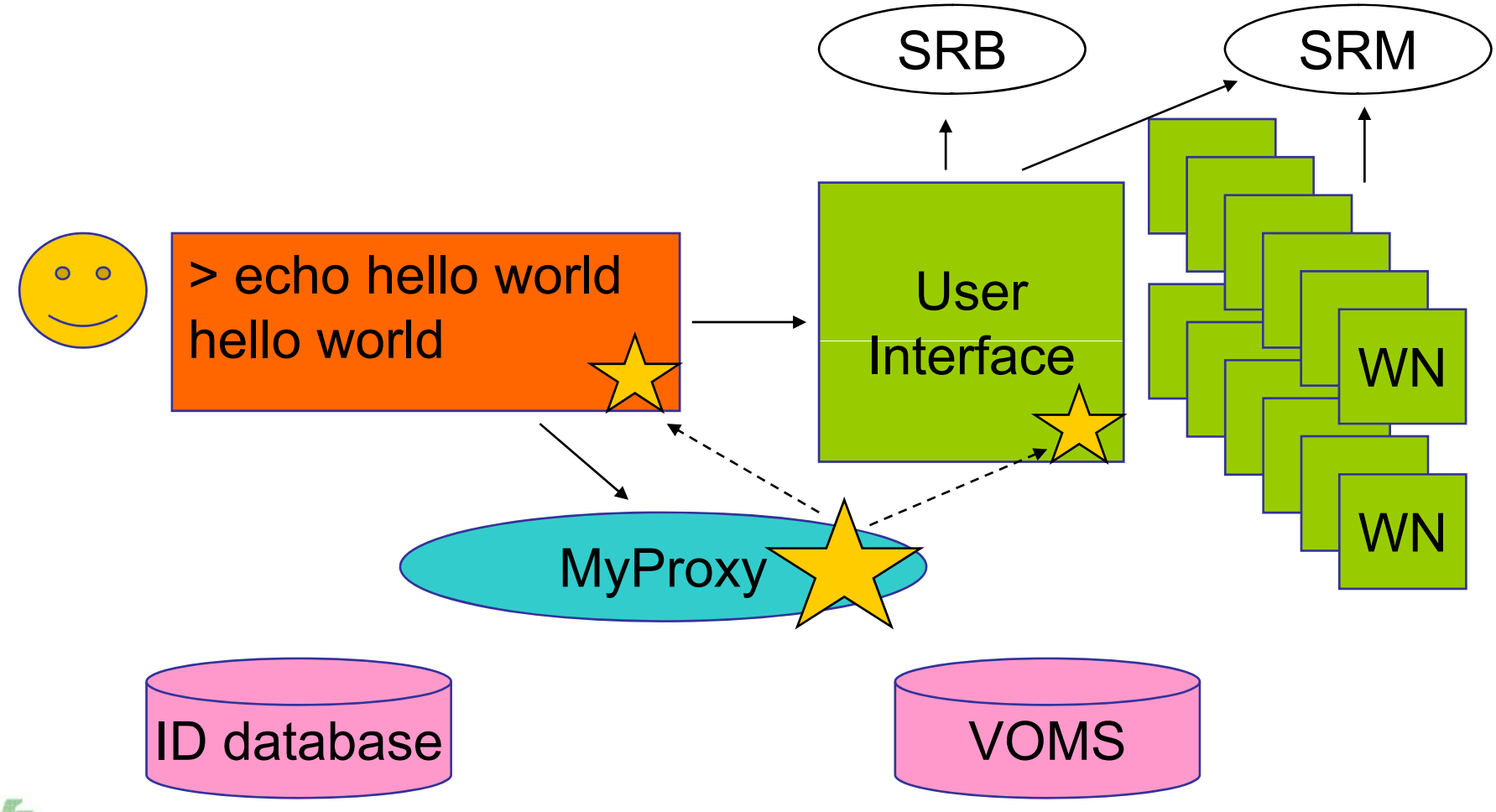
- Written in Java (no, really)
  - Standalone – untar and run
  - Or run as an Applet
- xterm
  - Understands (most?) ANSI control seqs
  - vi works!

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

Science & Technology Facilities Council

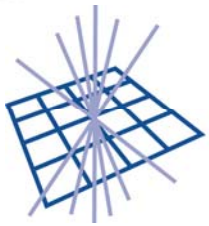
GridPP
UK Computing for Particle Physics



NGS National Grid Service
core production computational and data grid

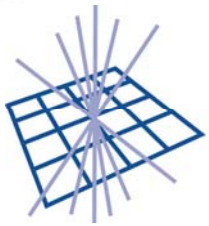
Java SSH Term

- Can integrate with site Active Directory
- Works!
- But only with Java 1.6
  - Available now!



On Robots

Or how I dream about stopping worrying, and about Laziness, Impatience, and Hubris, too



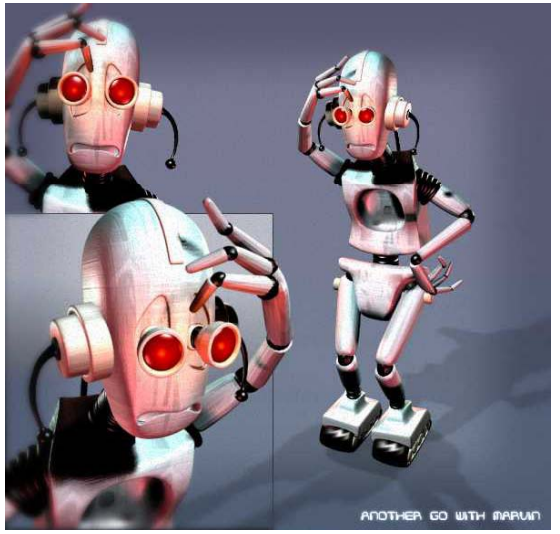
What is a Robot

- A user certificate
  - Whose private key is “unprotected”
  - i.e. not protected with a passphrase
- Identity
  - Not tied to a network identity
  - Tied to a specific user (owner)

Science & Technology Facilities Council

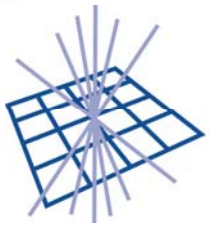
GridPP
UK Computing for Particle Physics

Why Robots



- Solve certain tasks
  - Email encryption
  - Grid monitoring
- Different types (extensions)
- A 1SCP policy defines an additional OID

NGS National Grid Service
core production computational and data grid



UK Implementation

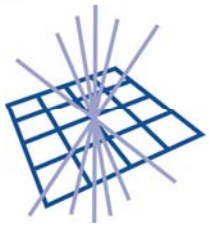
- First one? Now dutchgrid has one too!
- Meant to
  - be accepted by the community
  - gather real life robot experiences
  - become Robot HOWTO for others to use

UK Implementation

- Robots have names
  - Name after what they *are*, not what they *do*
  - "GridClient", "MailCipher",…
- What they do…
  - Depends on use and authorisation
  - GridClient usually does monitoring

Robot Names

- Robot DN *derived* from owner's DN
  - Owner DN + an additional CN
  - /CN=Robot:GridClient
  - ':' can be encoded as printableString
  - ':' does not occur in user or host CNs
  - Simple algo to find name of owner of robot

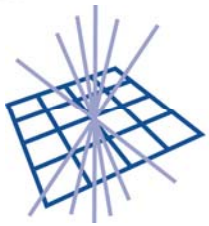


Robot Names

- Why use the DN?
  - DN is used for authorisation
  - DN is logged into log files
  - Can easily find user from Robot's DN
- Allow disambiguation
  - /CN=User Name/CN=Robot:Type (314)
  - No semantics associated to disamb.

Robot extensions

- Must be documented for each type
  - Documentation can be external to CPS
    - Allows for adding more types
- NO SERVER EXTENSIONS
  - MUST NOT be able to act as server
  - Does not contain network identity



How to recognise a robot …from quite a long way away.

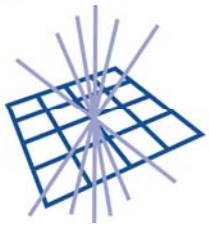
- Check the DN…
  - Does it have an add'l CN with "Robot:"
- Check the policyIdentifier
  - Does it have any Robot 1SCP OID?

Security Issues

- MUST be authorised independently
  - of the user's authorisation
- Private key is "unprotected"
  - i.e., not by passphrase – "always on"
- So UK policy requires:
  - Private key MUST be held on key token
    - Can't steal the key, physically held on machine
  - Proxies MUST NOT be generated from robot

Security Issues

- Robot certificates MUST NOT be shared
  - Single person responsible for use of robot
  - CA decides what it *is*, owner what it *does*
- Each Robot has a unique DN
  - No two Robots share keys
  - A single Robot only has two key sets when rekeyed



Security Issues – RA

- Owner uses existing certificate/key to apply for a Robot
- RA op MUST verify that key is protected on key token
  - Slightly clumsy changes to procedure
  - Also true when rekeying

Open Questions

- Can anyone apply for a robot?
  - If not, how should it depend on the type?
- Distinguish simple from powerful robots
  - Other than by extns
  - How to enforce what it *does* (cf Globus services)
- Bit like object signing extensions
  - How does CA assert this?

Conclusion

- Portals can be a good thing
- But are just one application among many
- Fit in with existing AUC and SSO
  - Portals can do CC to improve usability
  - But this has security issues