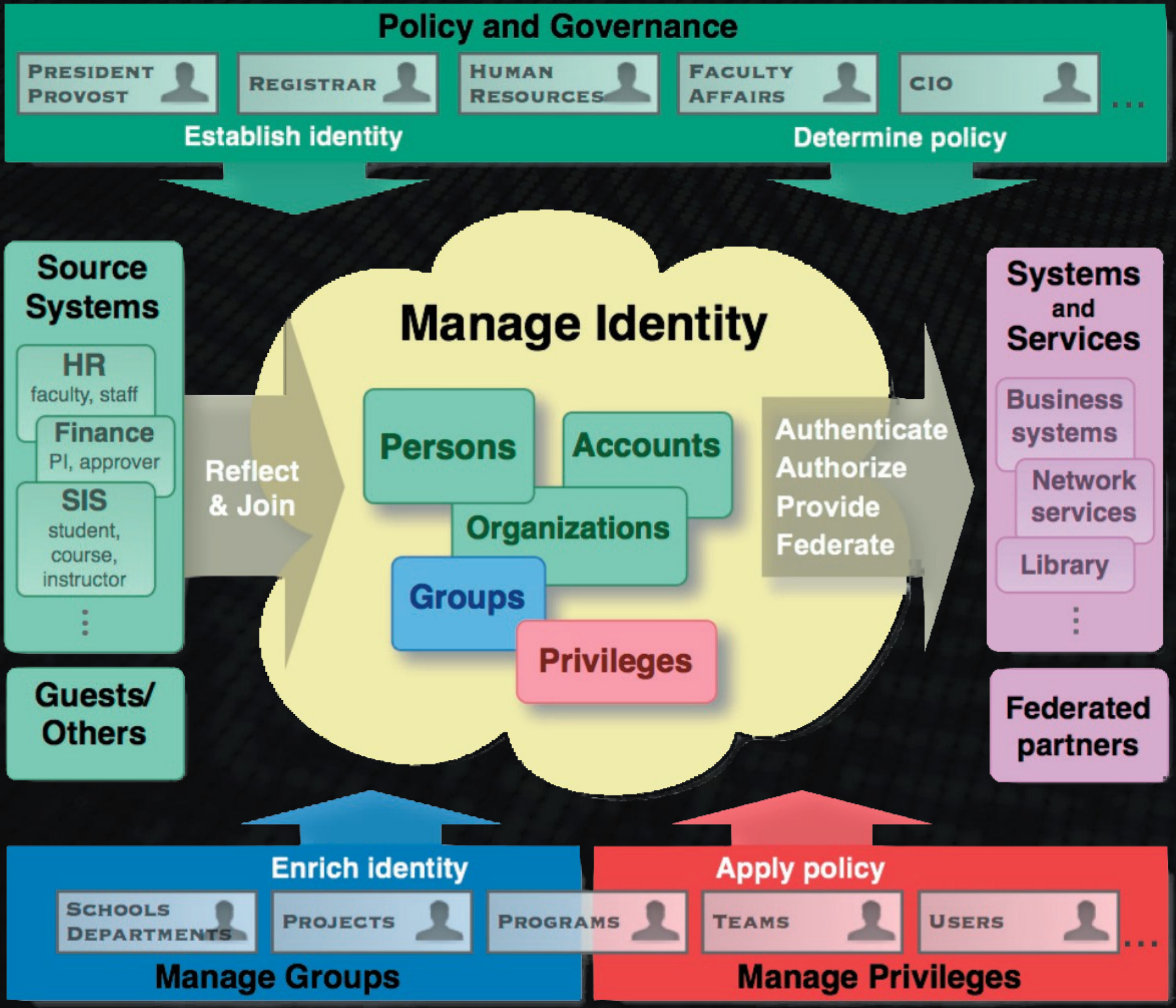
Identity and Access Management Infrastructure for Oxford University

John Ireland
Systems Development and Support Section Manager
Oxford University Computing Services

UNIVERSITY OF OXFORD

Identity and Access Management



Digital Identity

The electronic representation of a real-world entity: a "user"

Authentication

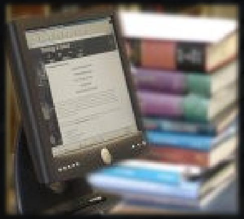
The process by which a user proves their claim to a specific digital identity

Authorisation

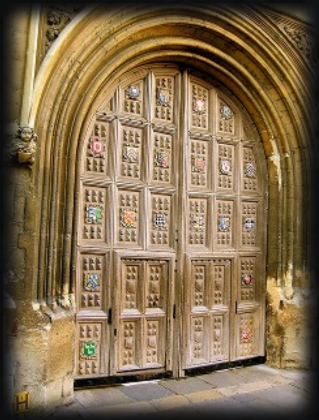
The process of defining who can access what (& enforcing that policy)

Oxford's IAM Context

Gmail



ExLibris



twitter

Oxford University Computing Services
www.oucs.ox.ac.uk

Organisation

44 colleges/PPH
168 departments
28 libraries
27 others

IT Staff

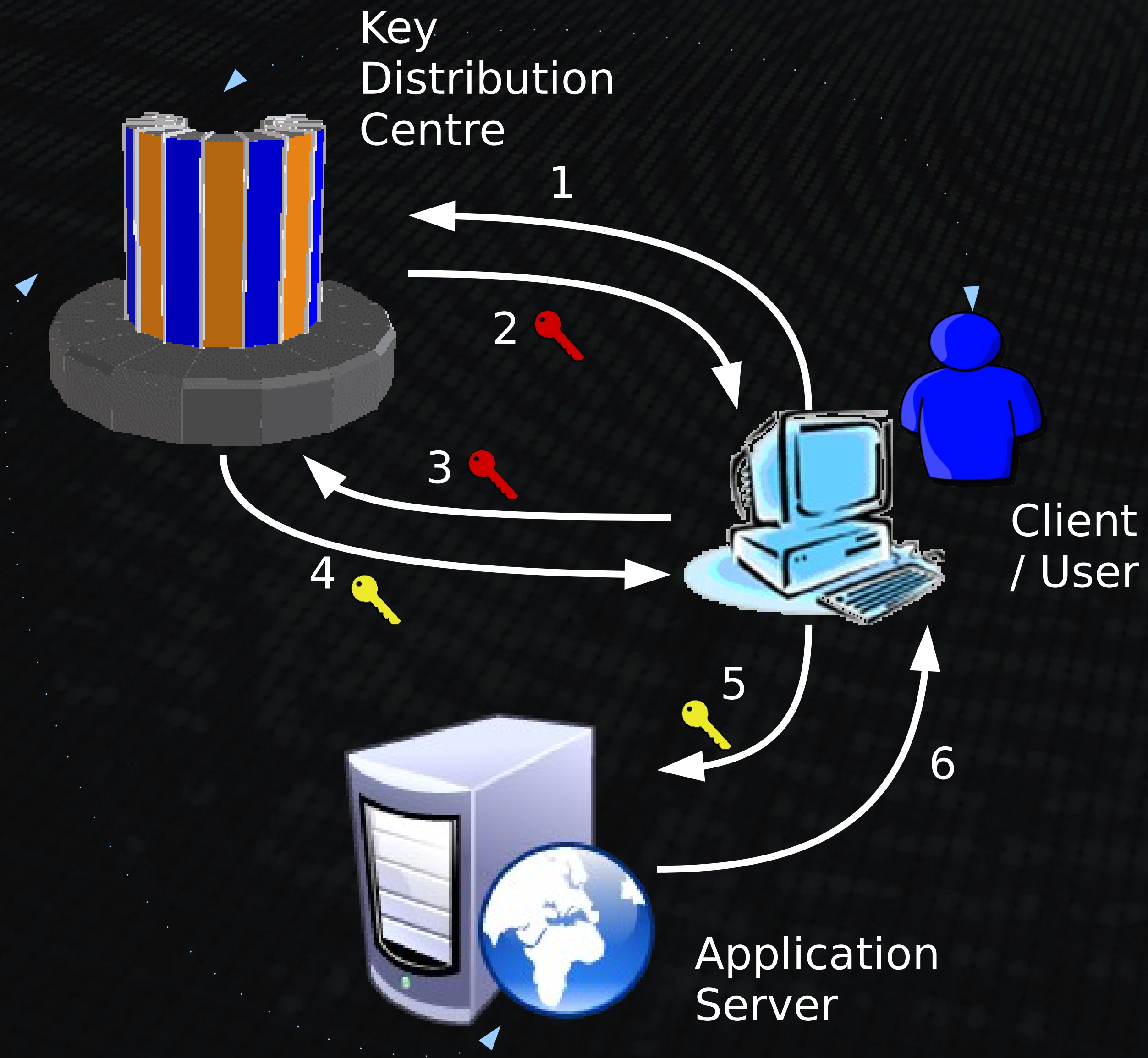
300-400 ITSS

Platforms

Microsoft
IBM/Oracle
Linux
Novell
Apple OS X
Sun

Current Services

Kerberos



Key Points

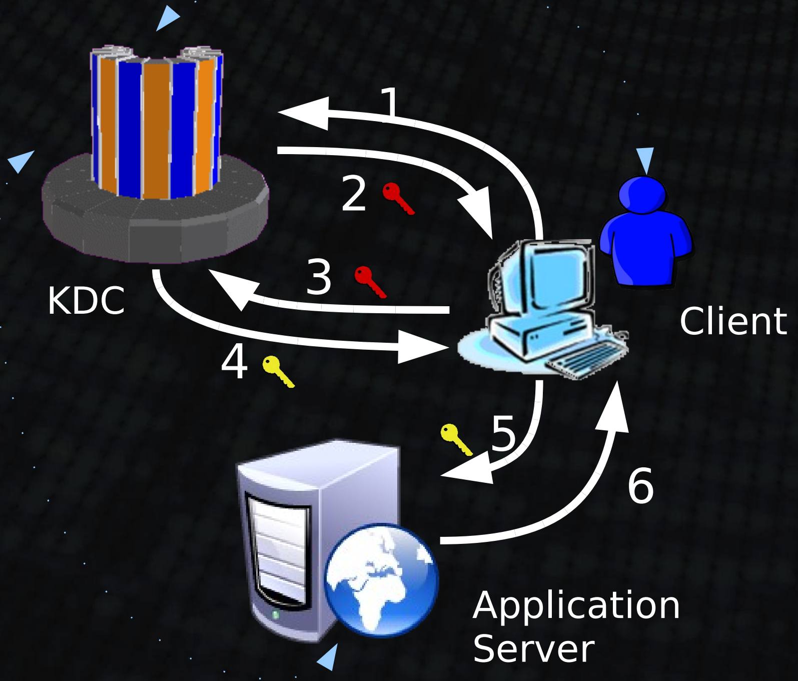
Passwords / hashes are not transmitted during authentication

Different keys for each application server

Single sign-on capability and good resilience model

Kerberos

- Preferred authentication protocol in Active Directory
- Suitable for any Kerberised service, implementations for SMB/CIFS, SSH, IMAP, SMTP, Active Directory
- Resilience through clustering of KDC and client-side failover



Available Since:

2002

Active Users:

33,000

Registered Servers:

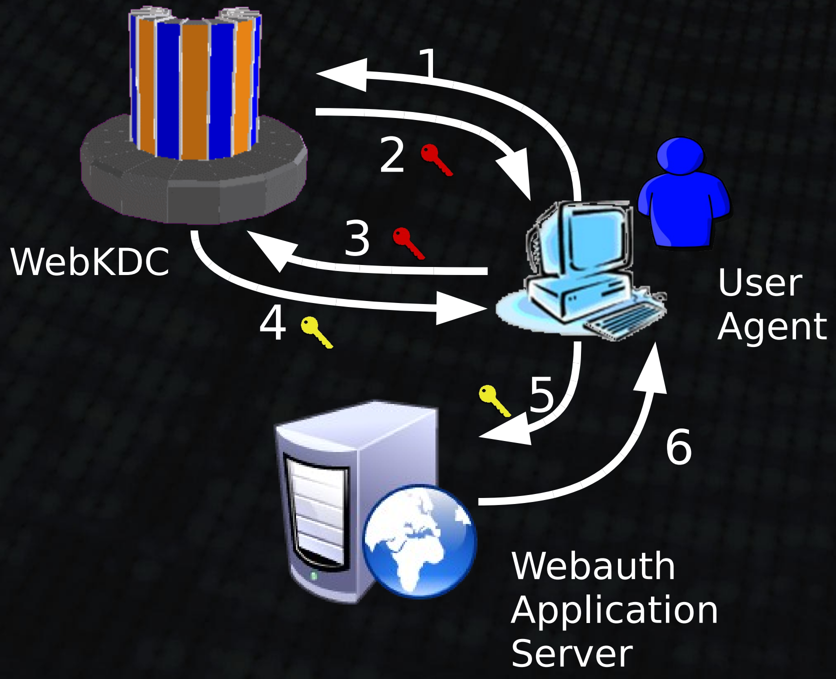
1,200

Logins/Day:

27,000

Webauth

- Wraps Kerberos tickets in web cookies
- Available as Apache module, included in popular Linux distros
- Support for HTTP-Negotiate, WAS-initiated re-auth, …
- Supplementary module to lookup user attributes in LDAP



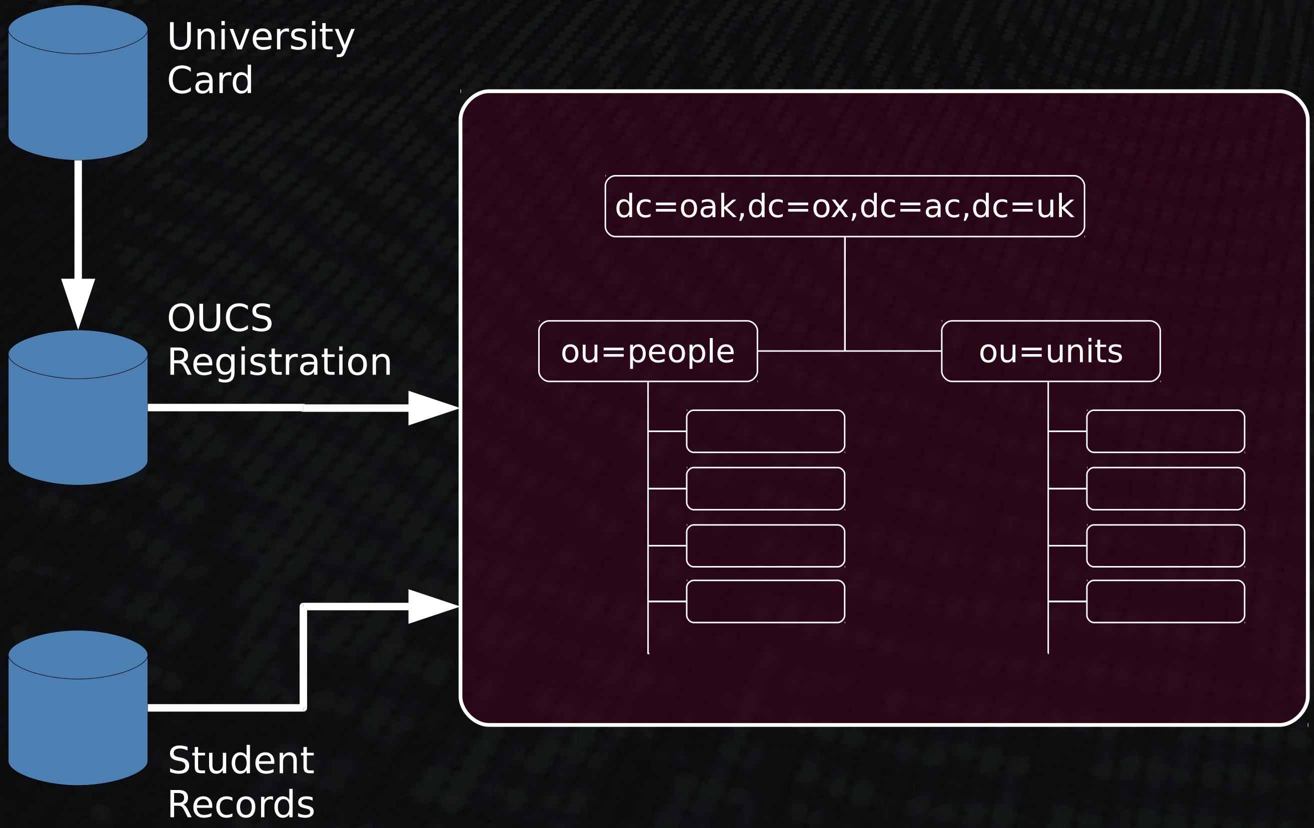
Available Since:
2002

Active Users:
33,000

Registered Servers:
385

Logins/Day:
6970

Oak LDAP



Available Since:

2008

Active Users:

n/a

Registered Servers:

189

Queries/Day:

180,000

Oak LDAP

```
dn:                     oakPrimaryPersonID=8455,ou=people,...
cn:                     Nate Pobridge
o:                      University of Oxford
ou:                     Department of Computer Science
displayName:            Nate Pobridge
sn:                     Pobridge
givenName:              Nate
mail:                   nate.pobridge@cs.ox.ac.uk
eduPersonOrgDN:         dc=ox,dc=ac,dc=uk
eduPersonAffiliation:   member
eduPersonOrgUnitDN:     oakUnitCode=cs,ou=units,dc=oak,...
eduPersonPrimaryOrgUnitDN: oakUnitCode=cs,ou=units,dc=oak,...
oakAlternativeMail:     nate.pobridge@cs.ox.ac.uk
oakPersonID:            8455
oakUniversityBarcode:   2201423
oakUniversityCardID:    10037759
oakCardExpiry:          20120101000Z
oakOSSID:               52683314
oakStatus:              senmem
oakOxfordSSOUsername:   alic3000
oakITSSFor:             oakGN=ITSS,oakUnitCode=cs,ou=units,...
memberOf:               oakGN=ITSS,oakUnitCode=cs,ou=units,...
memberOf:               oakUnitCode=cs,ou=units,dc=oak,dc=ox,...
objectClass:            oakPerson
objectClass:            eduPerson
```

Available Since:

2008

Active Users:

n/a

Registered Servers:

189

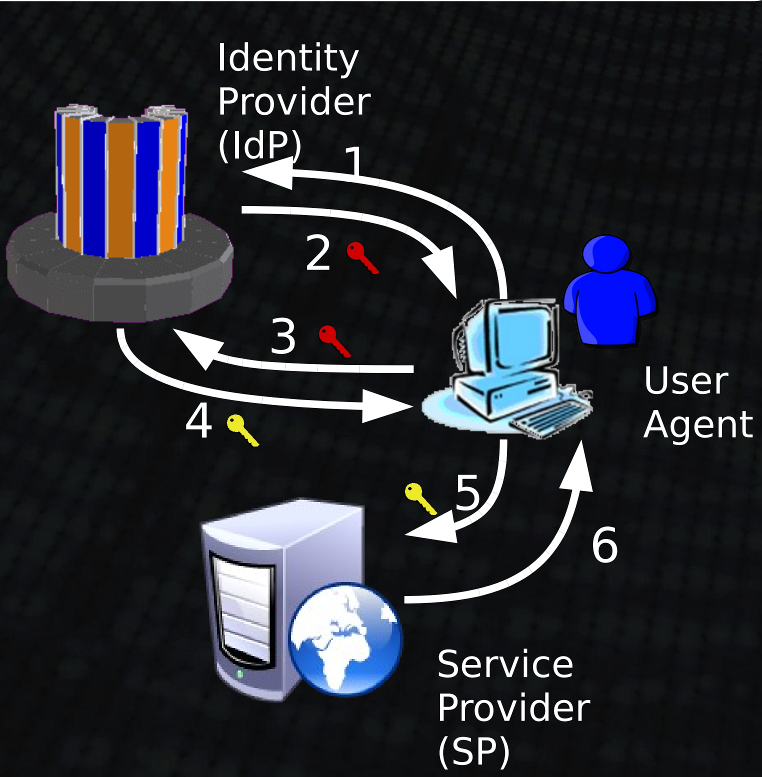
Queries/Day:

180,000

Shibboleth

Windows

- Software implementation of SAML Web Browser Profile
- Available as Apache module, included in popular Linux distros
- Available as **ISAPI filter for IIS (5,6,7) on Windows 2003**
- User attributes requested / returned in initial sign-on



Available Since:

2007

Active Users:

22,500

Registered Servers:

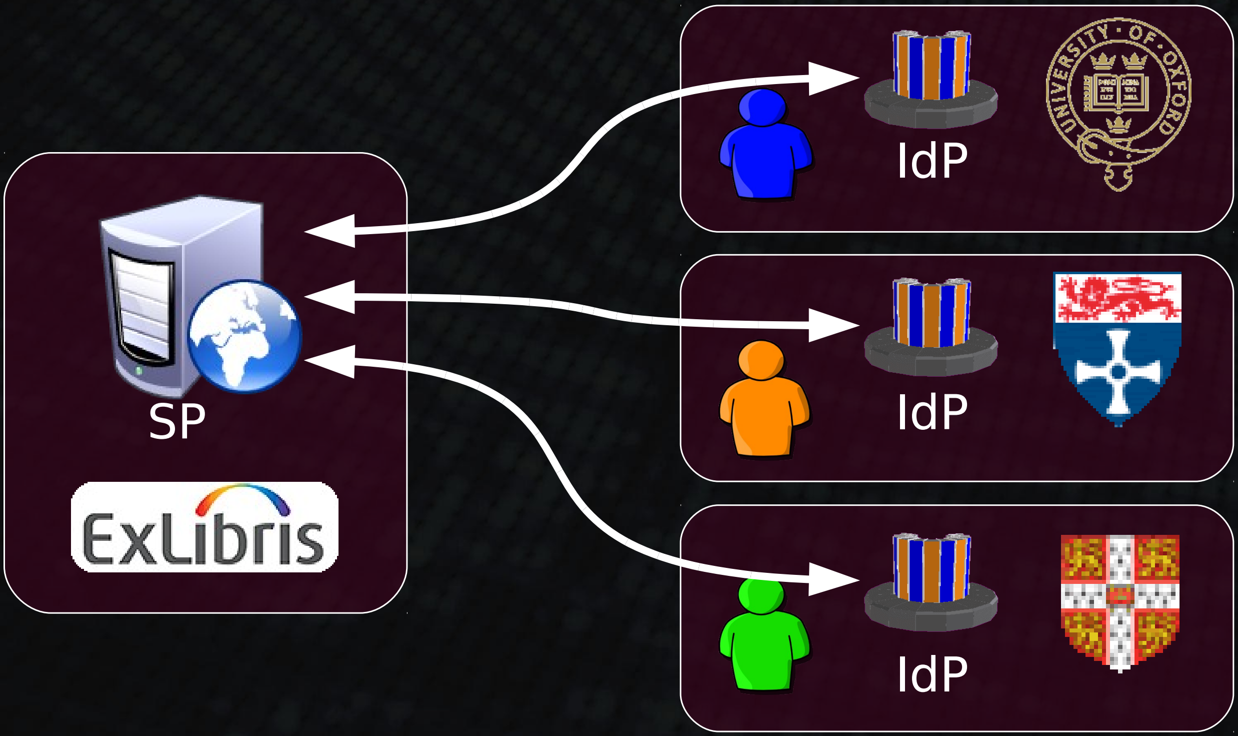
31

Logins/Day:

6742

Shibboleth

- Supports federated access management
- Enables 3rd parties to rely on our authentication of our users
- Enables us to rely on 3rd parties
- Enables us to federate internally



Available Since:

2007

Active Users:

22,500

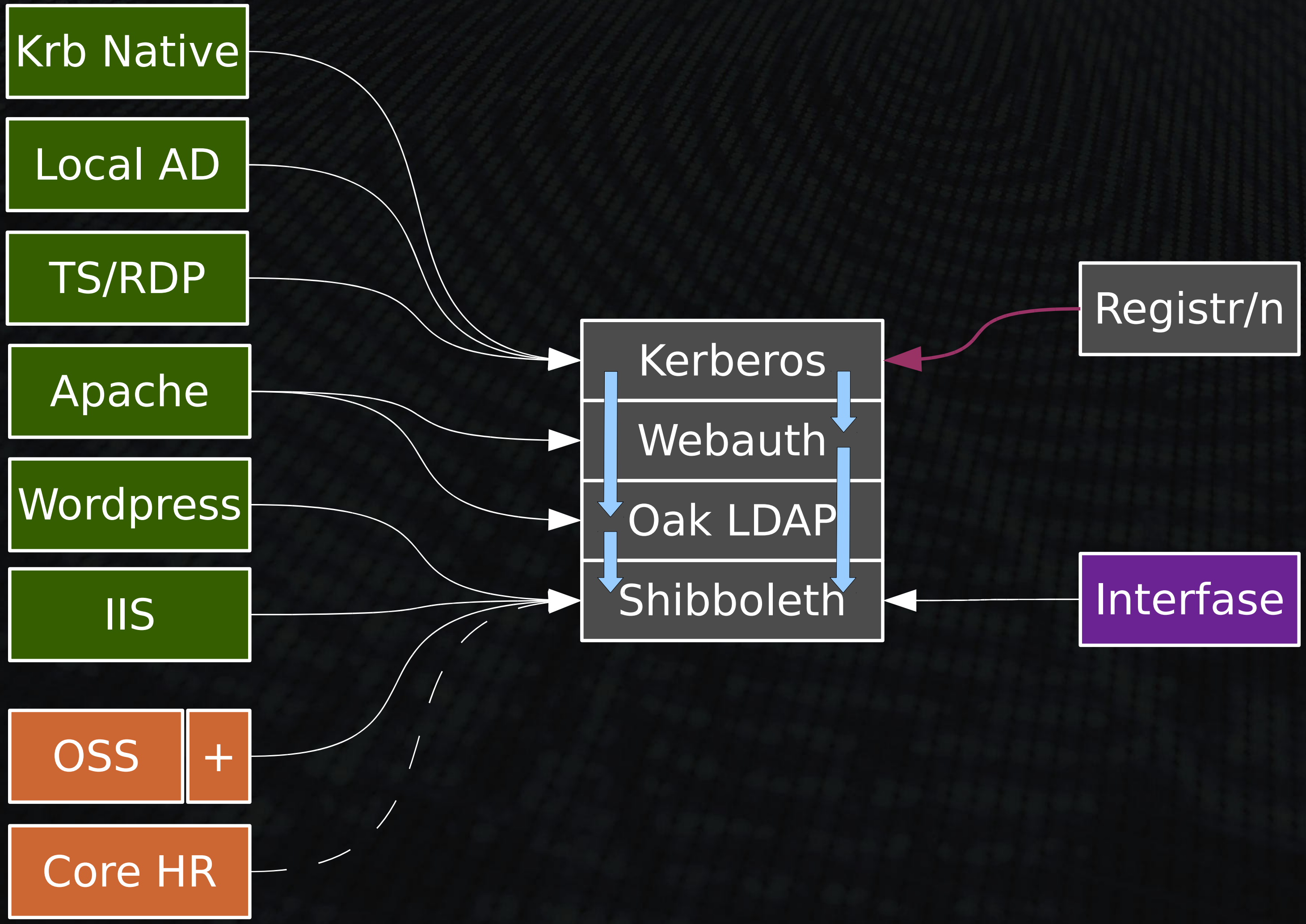
Registered Servers:

31

Logins/Day:

6742

IAM Suite


Krb Native
Local AD
TS/RDP
Apache
Wordpress
IIS
OSS
+
Core HR
Kerberos
Webauth
Oak LDAP
Shibboleth
Registr/n
Interfase

Current Projects

Core User Directory

- Provide a comprehensive central directory of people
- Consolidate and match person records from many sources
- Include foreign keys to assist drilling into primary data sources

Start Date:

2011-01

Finish Date:

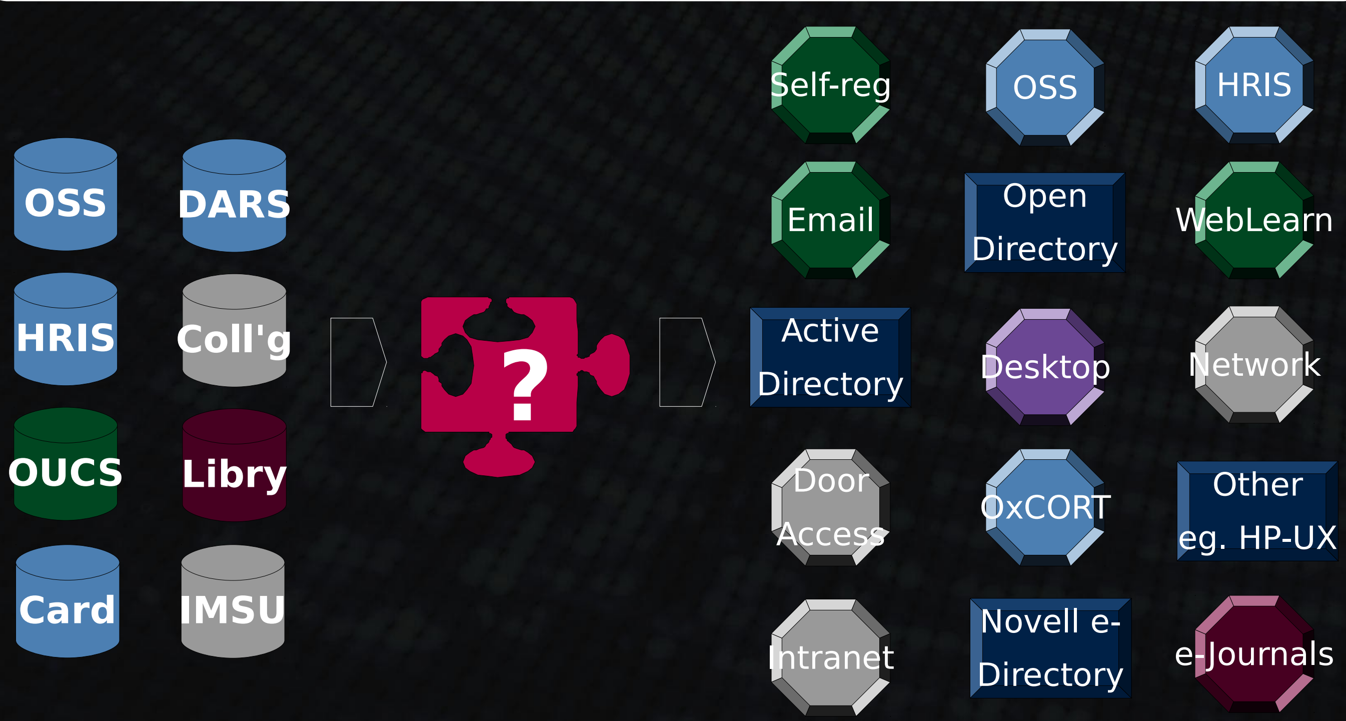
2012-06

Sponsor:

UAS IS Board

Staff:

2



Group Store

- Provide a central store for “managed” and “ad hoc” groups of people
- Currently running a development system based on Internet2 Grouper
- Project will be tied in against CUD as the services complement each other

Start Date:

2011-01

Finish Date:

Delayed

Sponsor:

OUCS

Staff:

1

UNIVERSITY OF
OXFORD

Oxford Active Directory

- SSO for AD using a cross-realm trust with Kerberos is available and works well for workstations in a domain, but…
- …there are doubts about support for this model from Microsoft and application vendors
- Our plan is to carry out rigorous testing of a typical Microsoft AD deployment for an organisation like Oxford…
- …and deploy an Oxford Active Directory domain if this looks beneficial

Windows Server®
Active Directory

Start Date:
2011-07

Finish Date:
2011-10

Sponsor:
OUCS

Staff:
2

Multi-factor Authentication

- Joint OUCS & Student Administration project
- Provide “enhanced authentication” for access to draft examination papers in VLE (WebLearn)
- Pilot solution based on SAML2 with one-time password delivered via SMS
- Infrastructure modifications suitable for general use

Start Date:

2011-01

Finish Date:

2011-09

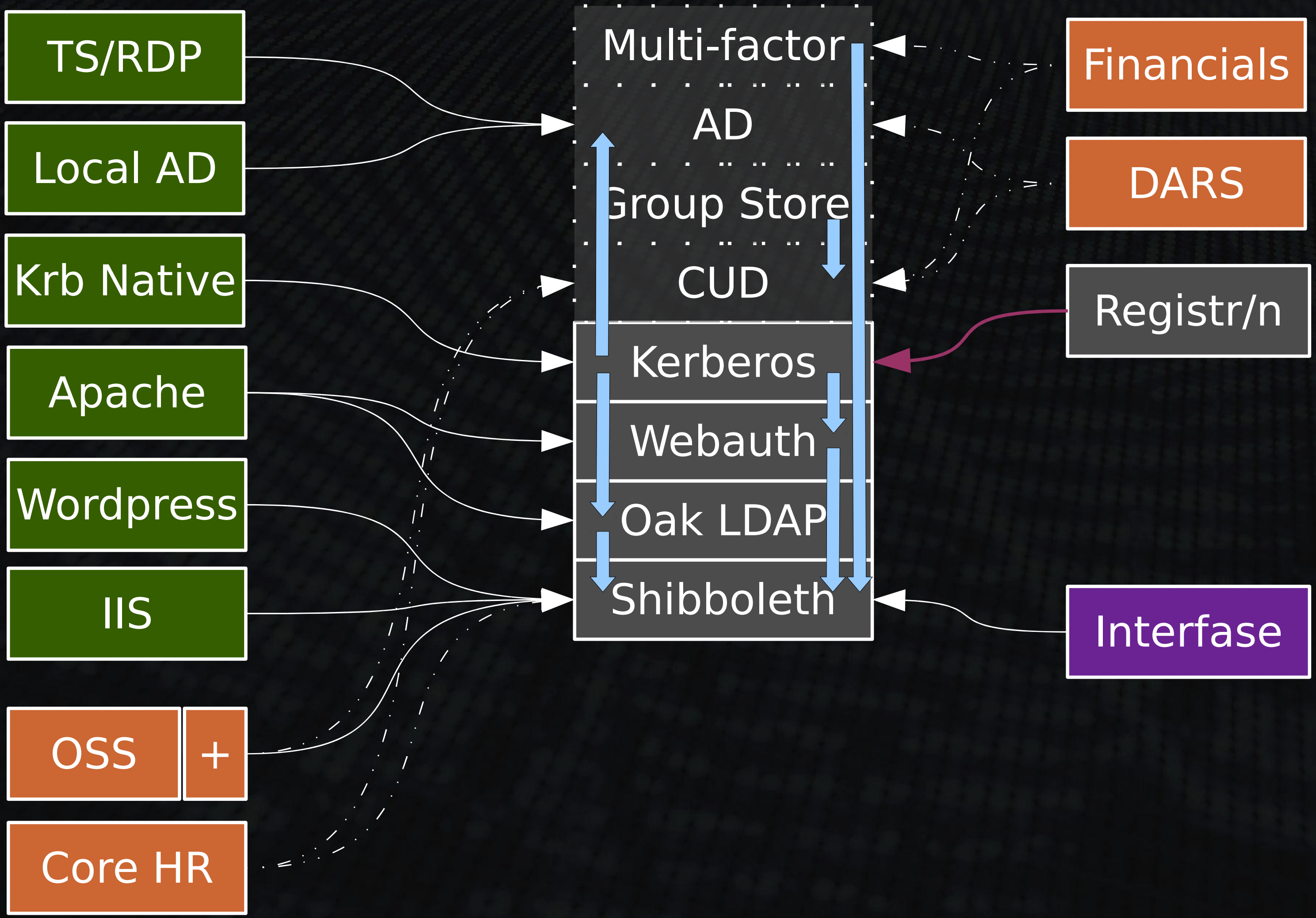
Sponsor:

UAS IS Board

Staff:

3

Enhanced IAM Suite



Future Projects?

Further Work

- There are still use cases that are not well supported
  - Commercial products which only support proprietary authentication
  - Products which "authenticate against LDAP"
- There is something awkward about Alumni needing to get a new login to access DARS
- Issuing credentials to new users is inefficient and not particularly secure
- There is a growing demand to be able to support non-members
  - Potential applicants (student & staff)
  - 40,000 library readers

Some Ideas

Middleware solutions to handle IAM suite integration for difficult applications

SSO "for life" - we don't reuse usernames anyway

SSO "for all" with online self-registration

Questions

Please do use the feedback forms to request workshops covering any aspects in more detail

john.ireland@oucs.ox.ac.uk