Sysdev & BSP: Tying together SSO and OSS

Christian Fernau and Brett Moore

ICT Forum

15 July 2009

This presentation

- What is OSS?
- A live demo (volunteer needed!)
- What is Webauth and Shibboleth?
- The wider picture: UK Federation
- Privacy and the 4 “core” attributes
- Shibboleth in Oxford: the architecture
- Future?
  - SAML, WS-Federation, Geneva, CardSpace
- Questions

What is OSS

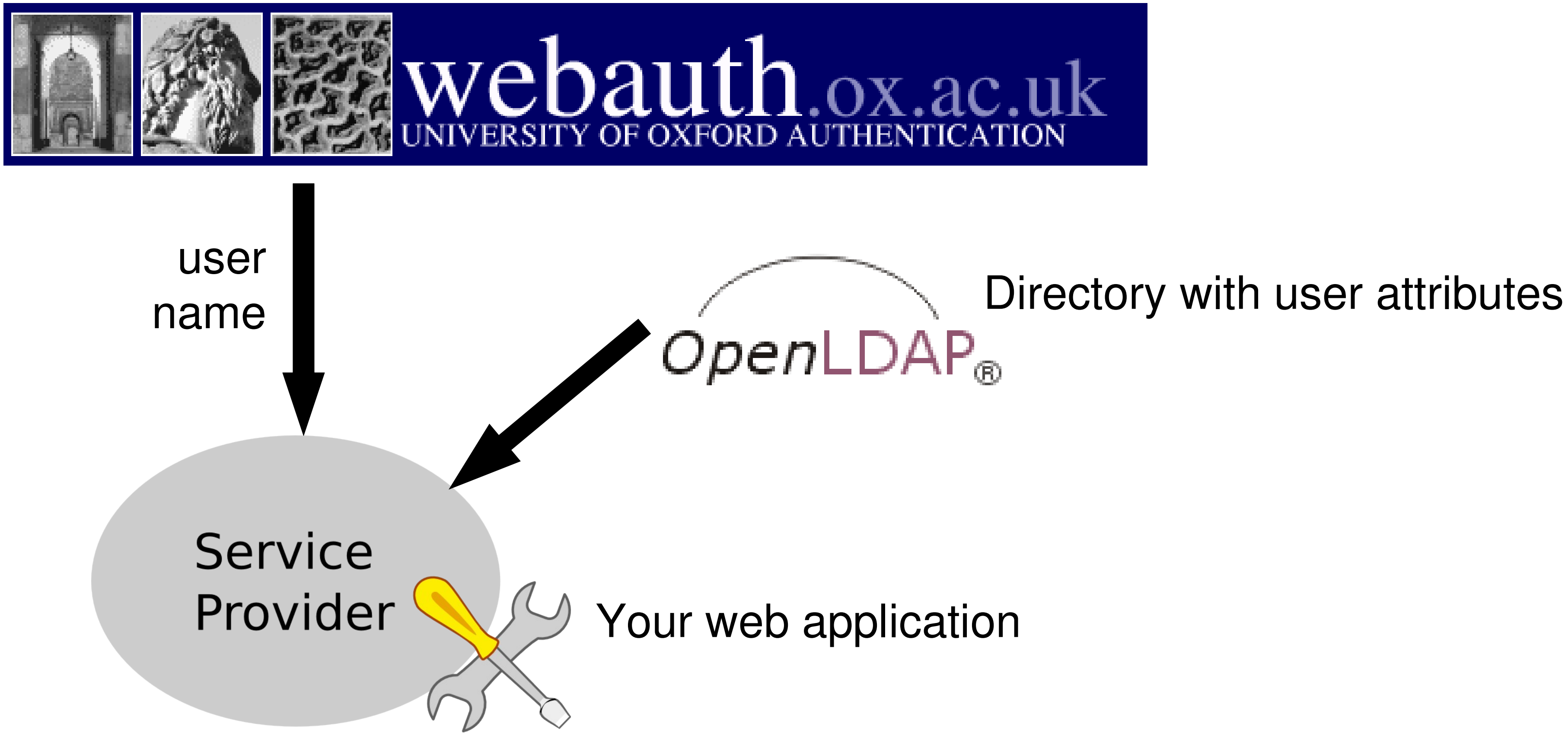
- Oracle's integrated suite for higher education
  - Managing student recruiting, admissions, enrolment, program structure and academic records
  - Apache 1.3, JSP/servlet based webapp, Oracle DB, AIX
- Students log in using their OSSID and password
  - High load on help desk during registration and after exam results are published (password resets)
- https://www.studentsystem.ox.ac.uk/

What is Webauth and Shibboleth?

- Webauth (SSO)
  - Developed by Stanford Uni
  - Webauth protocol
    - Internally uses Kerberos
  - Client for Apache 2
    - (and IIS)
    - ((and Java))

- Shibboleth (middleware)
  - Reference impl. by Internet2
  - Based on SAML standard
    - Also WS-Fed (passive)
  - Open source clients for
    - Apache 1.3, 2.x, IIS, PHP,..
      - Anything that supports SAML
  - Also from Sun, Oracle, Microsoft, Novell, Ping identity, ...

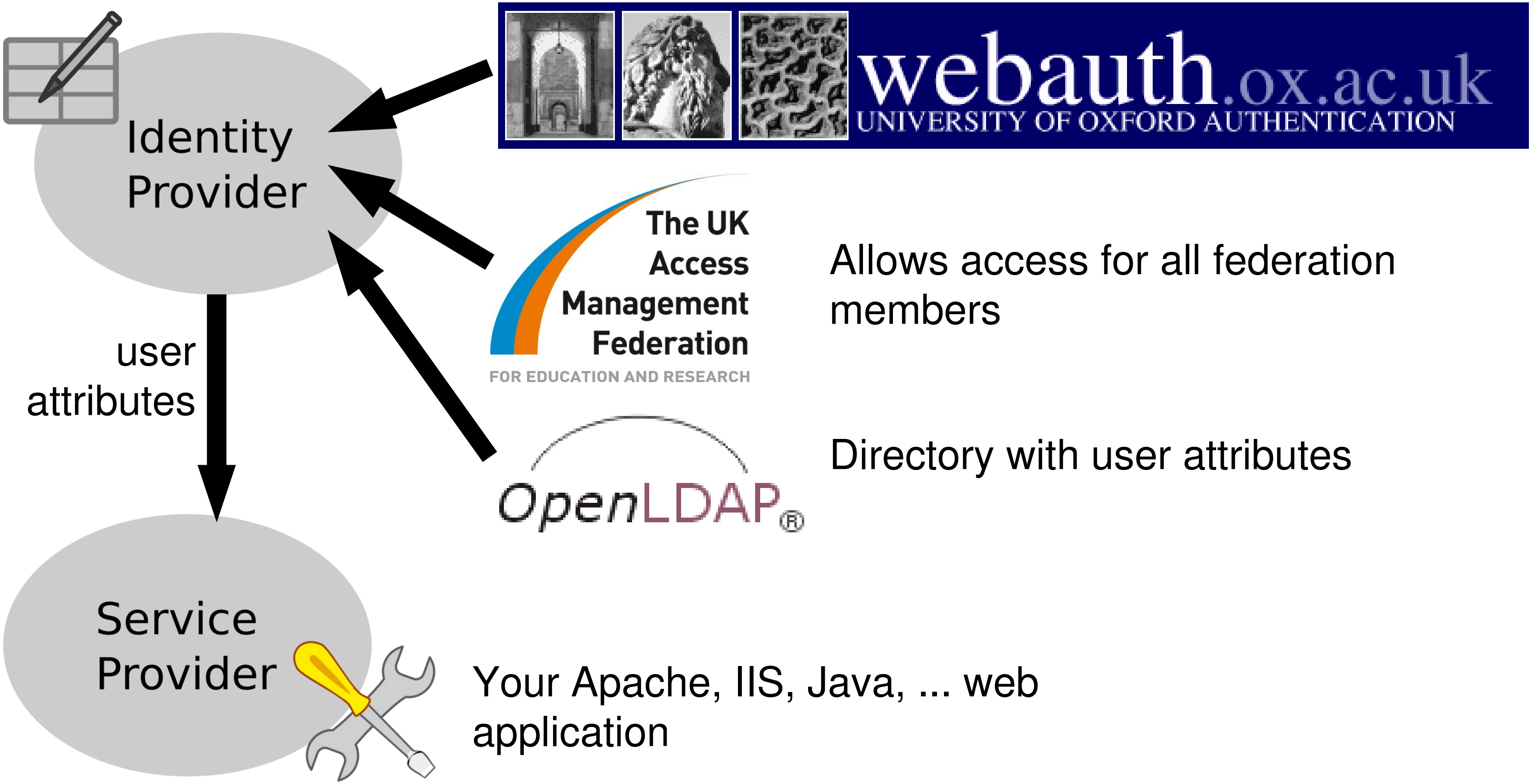
Shibboleth architecture at Oxford



Directory with user attributes

Your web application

Shibboleth® architecture at Oxford



Identity Provider
webauth.ox.ac.uk
UNIVERSITY OF OXFORD AUTHENTICATION
The UK Access Management Federation
FOR EDUCATION AND RESEARCH
OpenLDAP®
user attributes
Service Provider

Allows access for all federation members

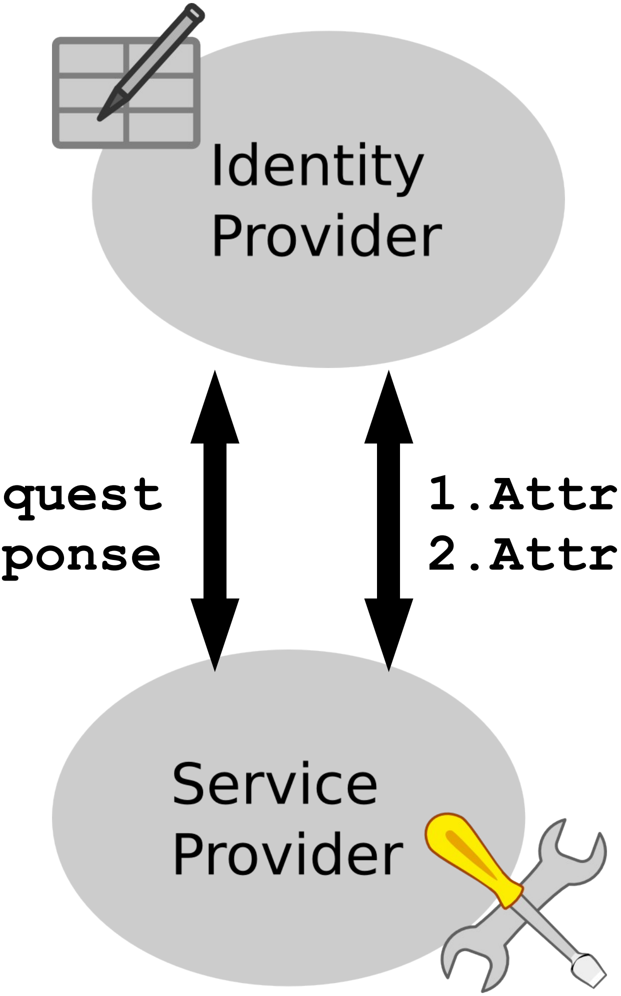
Directory with user attributes

Your Apache, IIS, Java, ... web application

Shibboleth®

Demystifying SAML

Is the user authenticated?



Identity Provider

Get user attributes

1. AuthN Request
2. AuthN Response

1. Attribute Request
2. Attribute Response

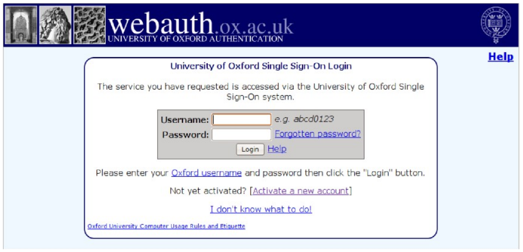
Service Provider

Your Apache, IIS, Java, ... web application

Tying together SSO and OSS

Web KDC

User enters login credentials



University of Oxford Single Sign-On Login

The service you have requested is accessed via the University of Oxford Single Sign-On system.

Username: e.g. abcd0123

Password: Forgotten password?

Please enter your Oxford username and password then click the "Login" button.

Not yet activated? [Activate a new account]

I don't know what to do!

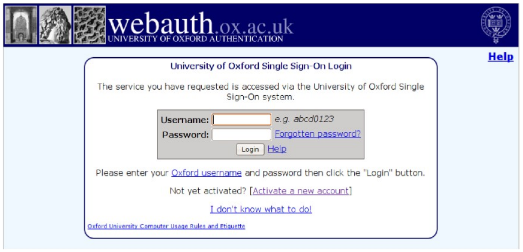
Oxford University Computer Usage Rules and Etiquette

encrypted
WebAuth
Username

Tying together SSO and OSS

Web KDC

User enters login credentials



webauth.ox.ac.uk
UNIVERSITY OF OXFORD AUTHENTICATION

Help

University of Oxford Single Sign-On Login

The service you have requested is accessed via the University of Oxford Single Sign-On system.

Username: e.g. abcd0123
Password: Forgotten password?
Login Help

Please enter your Oxford username and password then click the "Login" button.

Not yet activated? [Activate a new account]

I don't know what to do!

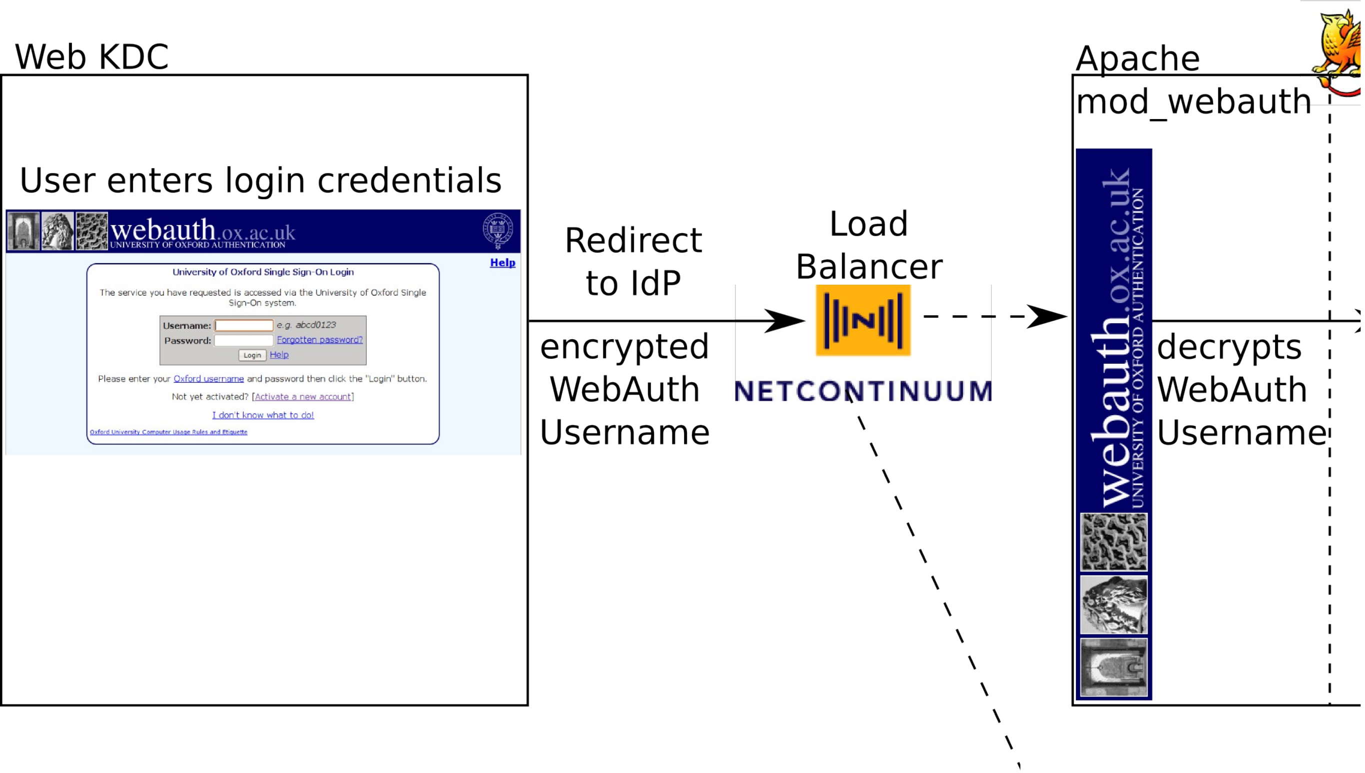
Oxford University Computer Usage Rules and Etiquette

encrypted
WebAuth
Username

Load
Balancer

NETCONTINUUM

Tying together SSO and OSS



Web KDC

User enters login credentials

webauth.ox.ac.uk
UNIVERSITY OF OXFORD AUTHENTICATION

Help

University of Oxford Single Sign-On Login

The service you have requested is accessed via the University of Oxford Single Sign-On system.

Username:		e.g. abcd0123
Password:		Forgotten password?
	Login	Help

Please enter your Oxford username and password then click the "Login" button.

Not yet activated? [Activate a new account]

I don't know what to do!

Oxford University Computer Usage Rules and Etiquette

Redirect to IdP

encrypted WebAuth Username

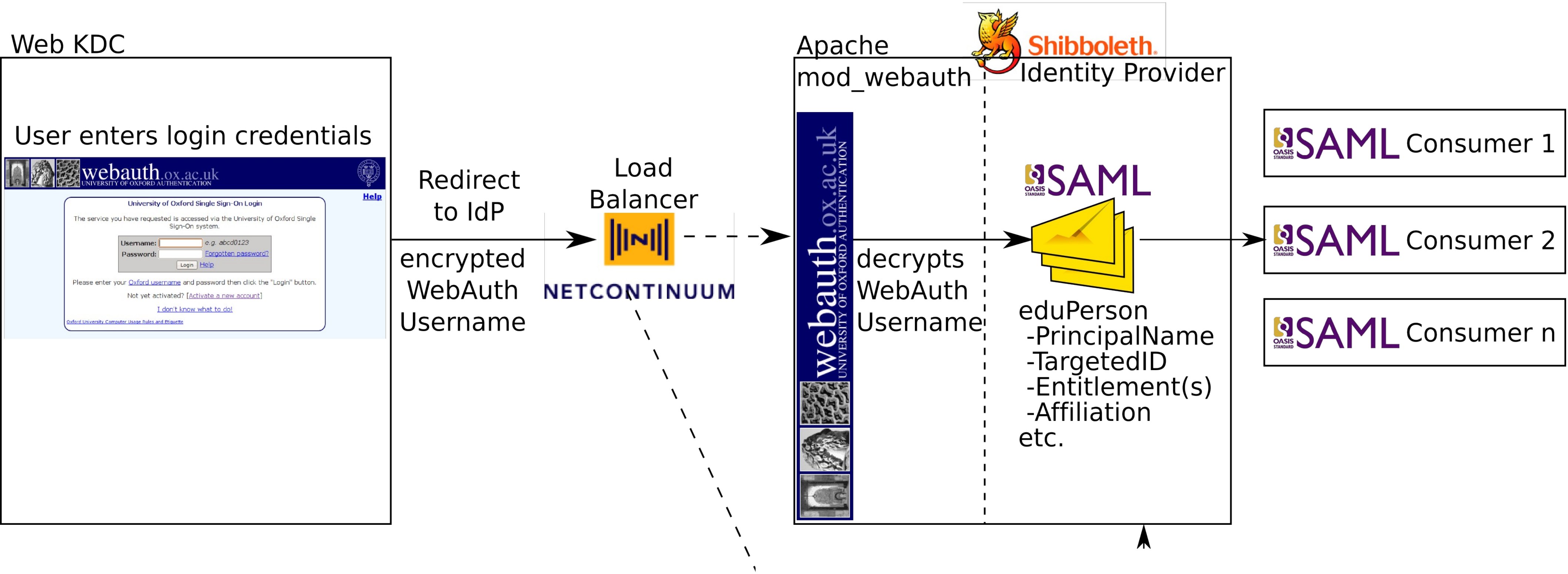
Load Balancer

Apache

mod_webauth

decrypts WebAuth Username

Tying together SSO and OSS



Web KDC

User enters login credentials

webauth.ox.ac.uk
UNIVERSITY OF OXFORD AUTHENTICATION

Help

University of Oxford Single Sign-On Login

The service you have requested is accessed via the University of Oxford Single Sign-On system.

Username: e.g. abcd0123
Password: Forgotten password?

Login Help

Please enter your Oxford username and password then click the "Login" button.

Not yet activated? [Activate a new account]

I don't know what to do!

Oxford University Computer Usage Rules and Etiquette

Redirect to IdP

encrypted WebAuth Username

Load Balancer

NETCONTINUUM

Apache mod_webauth

webauth.ox.ac.uk
UNIVERSITY OF OXFORD AUTHENTICATION

decrypts WebAuth Username

Shibboleth. Identity Provider

SAML

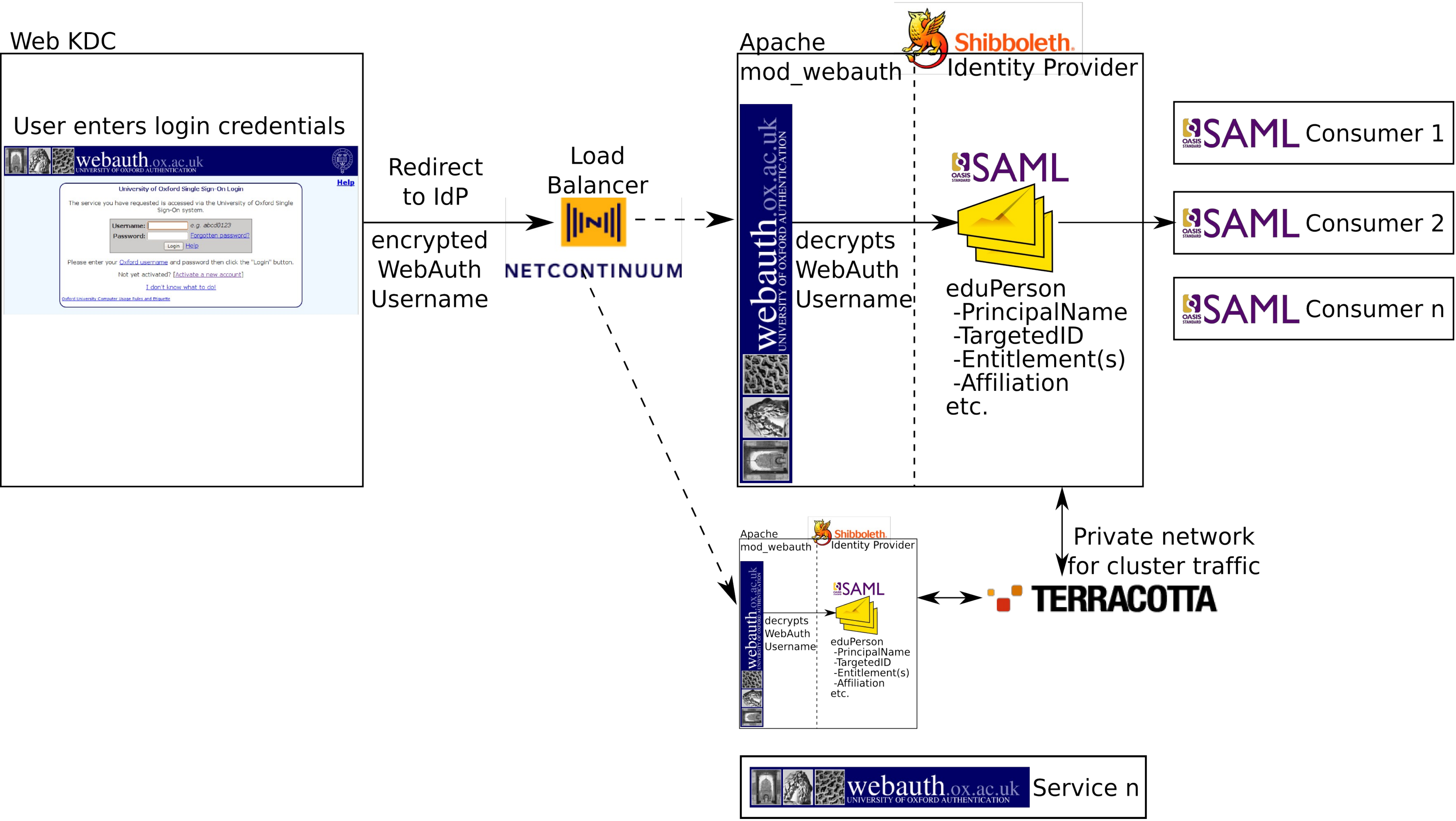
eduPerson
-PrincipalName
-TargetedID
-Entitlement(s)
-Affiliation
etc.

SAML Consumer 1

SAML Consumer 2

SAML Consumer n

Tying together SSO and OSS



webauth.ox.ac.uk
UNIVERSITY OF OXFORD AUTHENTICATION

Help

University of Oxford Single Sign-On Login

The service you have requested is accessed via the University of Oxford Single Sign-On system.

Username: e.g. abcd0123
Password: Forgotten password?
Login Help

Please enter your Oxford username and password then click the "Login" button.

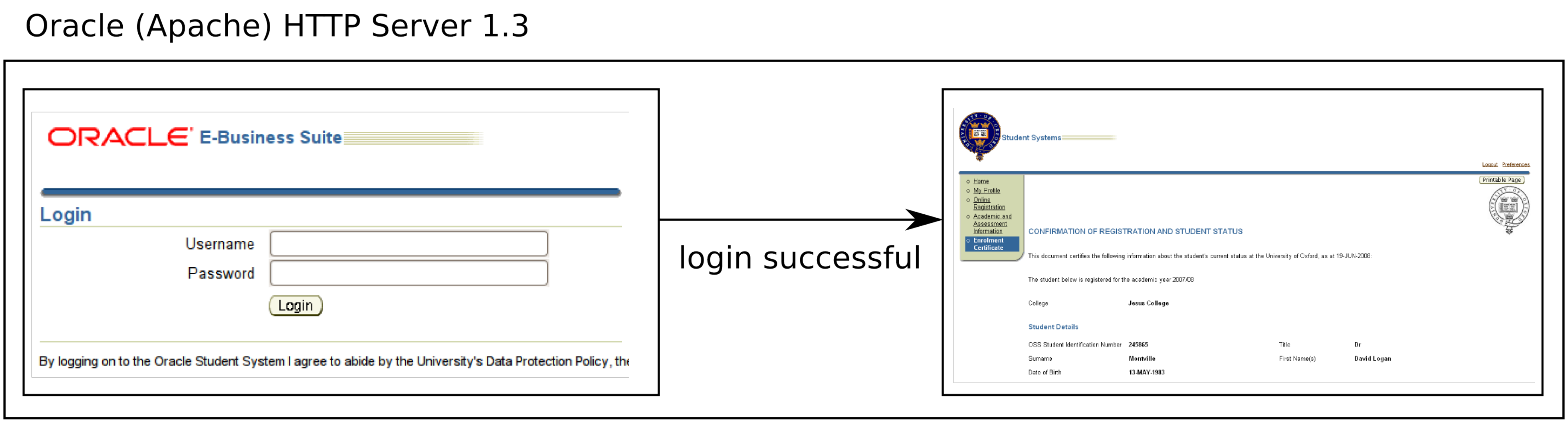
Not yet activated? [Activate a new account]

I don't know what to do!

Oxford University Computer Usage Rules and Etiquette

Tying together SSO and OSS

Before:



Oracle (Apache) HTTP Server 1.3

ORACLE E-Business Suite

Login

Username

Password

Login

By logging on to the Oracle Student System I agree to abide by the University's Data Protection Policy, the

login successful

Student Systems

Logout Preferences

- Home
- My Profile
- Online Registration
- Academic and Assessment Information
- Enrolment Certificate

Printable Page

CONFIRMATION OF REGISTRATION AND STUDENT STATUS

This document certifies the following information about the student's current status at the University of Oxford, as at 19-JUN-2008:

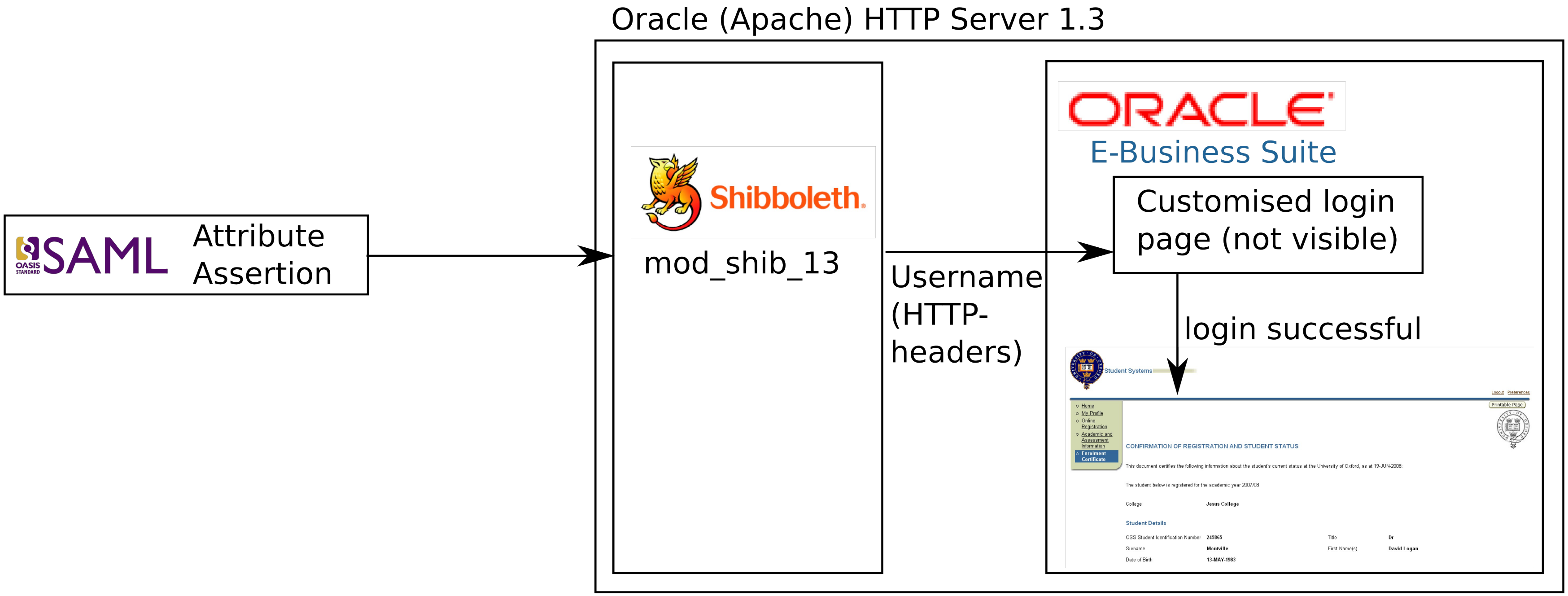
The student below is registered for the academic year 2007/08

College Jesus College

Student Details

OSS Student Identification Number	245865	Title	Dr
Surname	Montville	First Name(s)	David Logan
Date of Birth	13-MAY-1983		

After:



Oracle (Apache) HTTP Server 1.3

SAML Attribute Assertion

Shibboleth. mod_shib_13

Username (HTTP-headers)

ORACLE E-Business Suite

Customised login page (not visible)

login successful

Student Systems

Logout Preferences

- Home
- My Profile
- Online Registration
- Academic and Assessment Information
- Enrolment Certificate

Printable Page

CONFIRMATION OF REGISTRATION AND STUDENT STATUS

This document certifies the following information about the student's current status at the University of Oxford, as at 19-JUN-2008:

The student below is registered for the academic year 2007/08

College Jesus College

Student Details

OSS Student Identification Number 245865 Title Dr

Surname Montville First Name(s) David Logan

Date of Birth 13-MAY-1983

The wider picture: UK Federation

- A group of member organisations who sign up to a set of rules (see next slides)
- Is an independent body funded by Becta and JISC
- Manages the trust relationships between members
- Oxford joined in 2006 (SDSS)

The UK Federation Rules for IdPs

- Provide data that is accurate and up-to-date
- Comply to technical specifications
- Observe good practice for
  - configuration, operation, and security of service, exchange of data, private keys, ...
- Must hold all licences and permissions required
- Must not damage reputation of Federation
- Give 'reasonable assistance' to investigate misuse

The UK Federation Rules for SPs

- Must not disclose attributes to 3rd parties
- Use attributes only for access control decisions or presentation (and only for the service that the user requested)...
- ...or for generating aggregated anonymised usage statistics
- SP is responsible for management of access rights: federation has no liability

- eduPersonScopedAffiliation
  - e.g. student@ox.ac.uk, staff@college.ox.ac.uk
  - or even student@**cam**.ac.uk
- eduPersonTargedID
  - e.g. lafP89Jfla2faKf=@ox.ac.uk
  - different for every SP, but permanent
- eduPersonEntitlement
  - e.g. filmandsound:medic (Film & Sound online)
- EduPersonPrincipalName
  - corp9999@ox.ac.uk (“herald” username)

UK Federation examples

- ScienceDirect (Shibboleth has replaced Athens)
  - http://www.sciencedirect.com/
- University of Newcastle (within UK)
  - https://gabriel.lse.ac.uk/twiki/bin/view/Main/WebHome
- Internet2 wiki (outside UK)
  - https://spaces.internet2.edu/display/SHIB2

Future

- Microsoft Geneva
  - Replaces AD FS (Active Directory Federation Services)
  - Supports SAML, WS-*, Live ID
  - Allows integration with .NET applications
- Sun's project “Tango”
- CardSpace
  - Significantly improved user experience
  - through better integration with desktop apps (also browser)

Questions?