

CARDIFF
UNIVERSITY

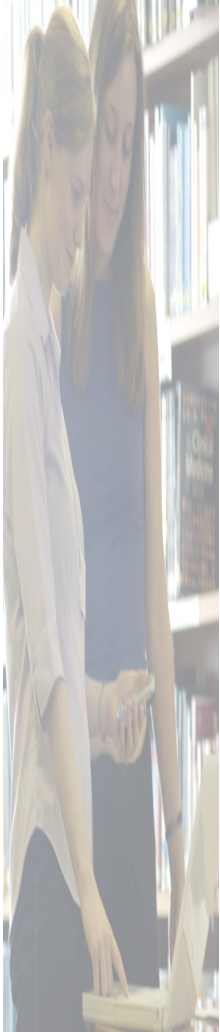
PRIFYSGOL
CAERDYDD

information services
gwasanaethau gwybodaeth

Federation and Identity Management in the UK

Rhys Smith, Paul Rock
Cardiff University

insrv



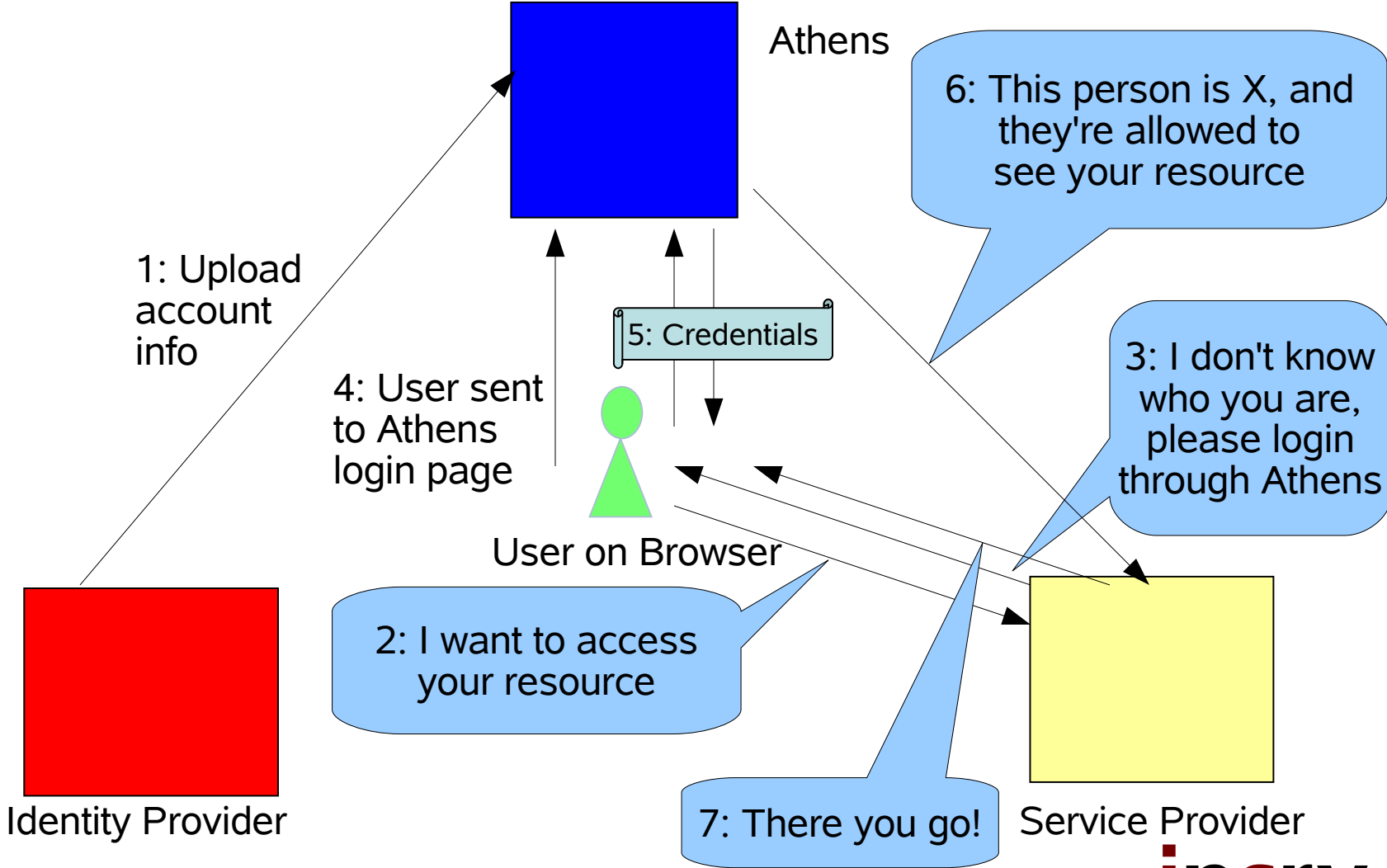
outline

- a bit of background
- the problem – the solution
- shibboleth – the stage show!
- access management in the UK
- AM -> FAM -> IDM
- IDM in the UK
- The Identity Project
- Help!

a bit of background

- athens:
 - an Access Management System for controlling secure access to web based services.
 - offers single sign-on access to multiple web-based services
 - usernames and password held at Athens but administered at a local level

classic athenis



oh dear...

- “ a big database table with about 4.5 million rows and 300 columns”
- but it works, so...

what's the problem?

- users work in increasingly global environment, demand increased mobility;
- desire for increased security, privacy;
- more resources – more credentials:
 - for user: lots of usernames/passwords!
 - for resource: manage own AMS (account administration overhead, forgotten passwords, etc), or a central AMS (e.g. Athens)
 - for both: security & integrity compromised (e.g. “abc123”), Proprietary authentication systems

the solution?

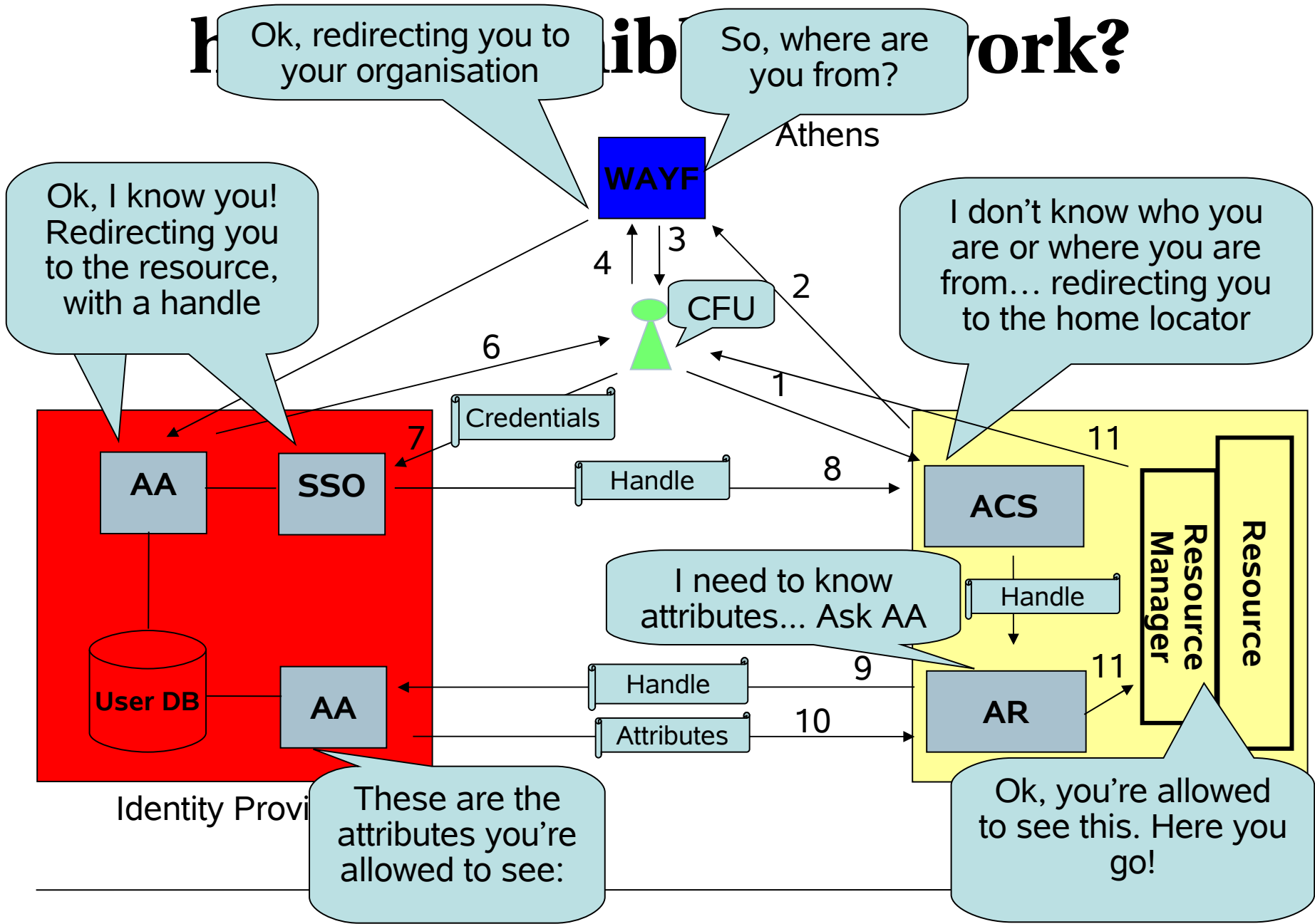
- *federated (devolved) access management:*
 - *role based (not identity based)*
 - i.e. (staff @ cardiff university) not (rhys @ CU)
 - *still allow personalisation*
 - 1 way hash of user id (@ resource - further priv')
 - *single sign-on to resources*
- organisations responsible for identity management;
- trust between resource providers and identity providers

technology for FAM?


- shibboleth:
 - enables FAM
 - an access management system for controlling secure access to web based (and beyond?) services;
 - offers single sign-on access
 - usernames and password at **organisation** end – standard network username/password

shibboleth – the stage show

libork?



JISC UK access management

- previously (well, currently) – centralised
 - e.g. athens – central repository of accounts/cred's
 - funding for athens ends july 2008. 50p per user (or thereabouts) after that...
 - next generation:
 - federated, devolved authentication (DA)
 - UK Access Management Federation for Education and Research
 - for he, fe and Schools (JISC and BECTA)
 - went live November 30th 2006.
 - (became self aware 2:14am EDT August 29th 20... (!))
-
- 

project progress and future

- whole of Cardiff University shib enabled now
- all new staff/students using it exclusively
- existing athens users migrating easter+
- approx 7,000 unique users (of 30,000)
(only ~1,500 first years!)
- what has this taught project taught us?

AM -> FAM -> IDM

- to connect people to resources:
 - Access Management (AM) - allows us to say who can access what (based on information such as personal affiliations, status, licensing, etc.)
- to connect people to remote resources, and enable effective inter-institutional collaboration:
 - Federated Access Management (FAM) - same as above, but passing info' between institutions
- to “do” effective FAM:
 - “good” IDM! - to make assertions to other organisations about your members, you need to know the information!

“good” IDM in UK academia?

- very varied
 - “good” / “bad”, simple/complex, proprietary, COTS
- different goals / different methods
 - different institutions have different ideas about IDM, so implementing in different ways
- a voyage into the unknown
 - have an idea but no conclusive facts & figures on where everyone is, and if they're compatible through FAM
- so, JISC funded...

“The Identity Project”

- funded by the Joint Information Systems Committee
 - 10 partner institutions
 - 8 main areas of work (next slides)
 - 5 key bodies on steering committee (Partners/RUGIT/UCISA/JISC/UKERNA)
 - 1 year project

what we're doing

- eight main work areas
 - 1) broad survey of current IDM practice
 - 2) in-depth case studies of IDM practice
 - 3) investigate practise/policy around membership
 - 4) investigate how NHS links affects IDM
 - 5) investigate how grid infrastructure affects IDM
 - 6) identify common problems/solutions
 - 7) examine current tools for IDM
 - 8) identify best practice & future developments

how you can help

- if you're from an UK academic institution...
 - please get in touch with me (later or via email)
 - working with us during this project ensures your institution's point of view will be included
 - community consensus ensures the project is useful
- non UK academic
 - any input, out of scope but help align policy
- if you're from a vendor with IDM tools
 - please get in touch with me (later or via email)
 - we want to investigate a wide range of tools
- Any suggestions are welcomed!

urls

- <http://www.identity-project.org/> (soon)
- <http://www.jisc.ac.uk/>
- <http://www.ukfederation.org.uk/>

the end

- for:
 - more info
 - a copy of these slides
 - clarification of any points
 - meaningful discussion about IDM/FAM
 - meaningless discussion about anything else...
- email: smith@cardiff.ac.uk
rock@cardiff.ac.uk

