



Identity Management

a Toolkit for institutions

John Paschoud, London School of Economics



What are the business drivers for better Identity Management?

- Process efficiency
 - cost-savings on duplicated processes and systems
- Good information governance
 - **knowing** who has access to what!
- Joined-up learning environments
 - with library resources, research data,...
- National standards (UK Access Federation)
- International standards (parallel education federations now in most developed countries)

UK Access Management Federation for Education and Research

Rules of Membership

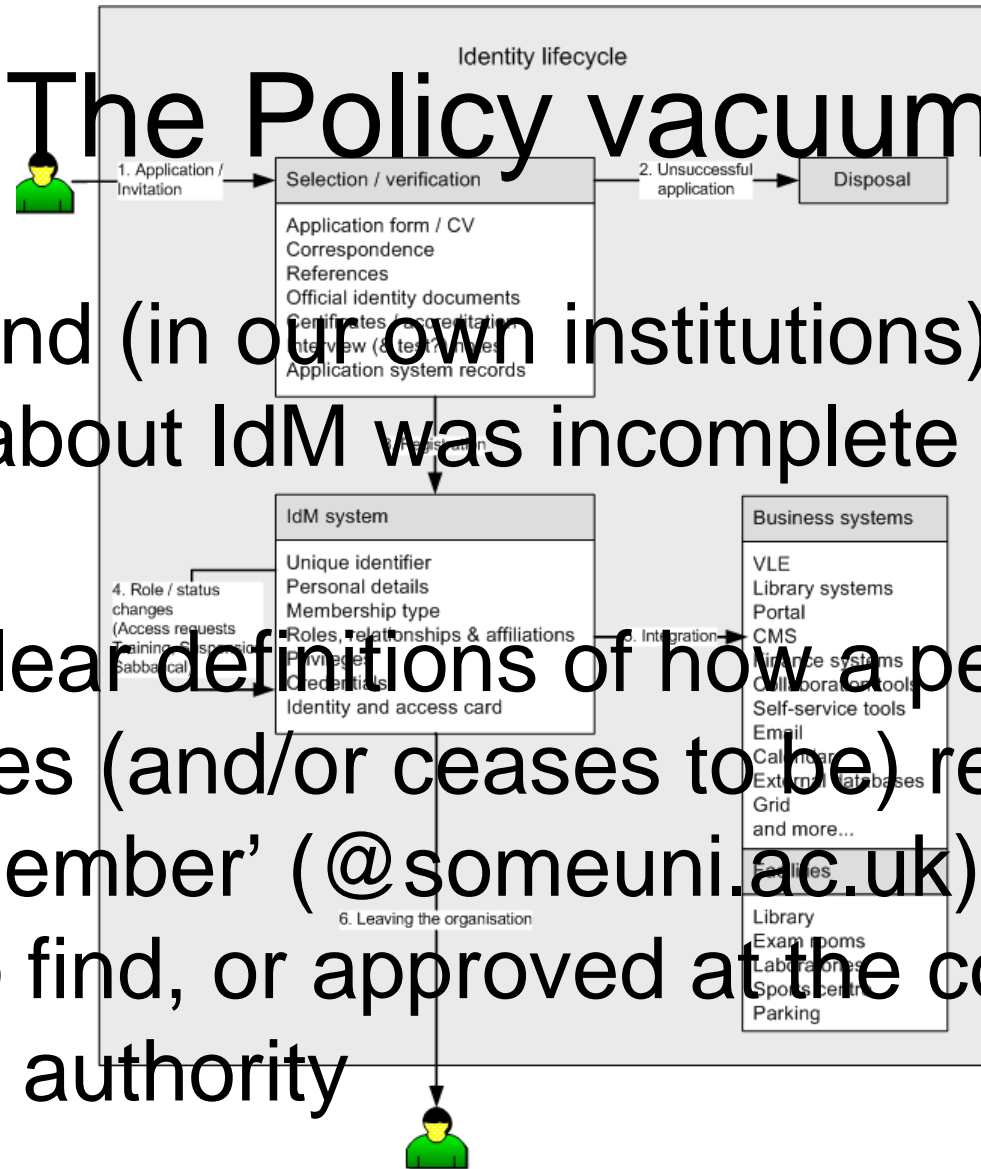
- 6.1. Where End User Organisations have the technical and organisational means to match use of services provided by Service Providers to individual End Users, then the End User Organisation may wish to arrange that at any time thereafter, declare this to the Federation Operator which will then publish this declaration in the Metadata. Once the End User Organisation has made this declaration, it must comply with the provisions of this Section 6 in respect of those Systems and End Users covered by the declaration. The End User Organisation acknowledges that where it is unable or unwilling to make this declaration this may affect access for End Users to Service Providers' services or resources. [note 3]
- 6.2. The End User Organisation must have a documented process for issuing credentials that may give access to Service Providers' services or resources. Information must be made available on request to Service Providers' End Users. End User Organisation is, or is planning to, provide access management information.
- 6.3. The End User Organisation must use reasonable endeavours to provide those End Users in respect of whom the End User Organisation provides appropriate information on how to use their credentials safely and securely.
- 6.4. The End User Organisation must ensure that accurate information is provided about such End Users. In particular:
- 6.4.1. credentials of End Users who are no longer members of the organisation must be asserted for such End Users to the Federation;
 - 6.4.2. where unique persistent Attributes (e.g. eduPersonTargetedID or eduPersonAffiliationClass) are issued to an End User, the End User Organisation must ensure that these Attribute values are not re-issued to another End User for, at least 24 months after the last possible use by the previous End User;
 - 6.4.3. where an End User's status, or any other information described by Attributes, changes, the relevant Attributes must be also changed as soon as possible.

[<http://www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf>]

Why is it hard to make the IdM business case?

- “People are our core business asset” is usually easy enough..... But
- IdM is hard to explain; the language of ‘identity’ can get too philosophical!
- Solutions (costs) are largely middleware (not up-front applications)
 - the Middleware Engineer’s Dilemma

The Policy vacuum



- We found (in our own institutions) that policy about IdM was incomplete (and worse)
- Even clear definitions of how a person becomes (and/or ceases to be) recognised as a 'member' (@someuni.ac.uk) were not easy to find, or approved at the correct level of authority

An institutional toolkit for Identity Management

- ...was recommended by JISC's *Identity Project* led by Cardiff and LSE, Nov 2006 to Oct 2007
- Work was funded by JISC and started in Jan 2009
- A partnership of Bristol, Cardiff, Kidderminster and LSE
 - all with some practical experience of doing IdM
- Oversight involves UCISA, RUGIT, ISAF, JISC, RSCs and independent evaluator

...and it's first published **today** at the
UCISA Conference

Who is the IdM Toolkit for?

Answer A:

- University & college ICT directors, CIOs etc
 - ...who would go to jail for *really bad* IdM
 - ...or at least have to explain to someone why they've been kicked out of the UK Federation

Answer B:

- Their staff who are either:
 - Already quite good at the technicalities – but could do with some guidance on what's expected; *OR*
 - Suddenly tasked with becoming the local expert in IdM - and a bit scared

How we developed the Toolkit

- A first stab - based on material from the *Identity Project* and past experience of partners and project team
- Road-testing the Draft Toolkit on IdM improvement projects at Kidderminster and Bristol
- Access to the pre-publication Toolkit for Oxford and Newcastle who also provided feedback
- Tidying-up the end result - with some further consultation
- Production in 'traditional' document and online interactive versions (different routes for different needs)
- Design and promotion working with JISC Communications

What's in the Toolkit? [1]

- **Introduction to Identity Management**
 - Defines basic terms and concepts of Identity Management used or assumed elsewhere. Should be read by anyone using the Toolkit.
- **Identity Management governance and policies**
 - Describes the roles, structures and policies required for Identity Management and how they relate to Identity Management systems and processes. Useful for Chief Information Officers or Directors responsible for IT, and staff who need to draft or apply institutional policies.
- **Identity Management systems, components and functions**
 - The technical components and functions of Identity Management systems in an academic institution. Good background reading for IT service managers and staff, and anyone discussing Identity Management with potential system suppliers.
- **Defining institutional requirements**
 - Functional requirements for each component of an Identity Management system, which may be useful in defining the objectives of an in-house implementation project or in detailed specifications to suppliers.
- **Discovering and Auditing current institutional Identity Management**
 - A detailed guide to finding out the state of Identity Management in an institution with a comprehensive audit (based on work of the JISC Identity Project which developed and tested IdM audits in several universities).

What's in the Toolkit? [2]

- **Gap analysis**
 - Explains how to establish the current and desired states of affairs for Identity Management, gives a list of common gaps in FHE institutions, and suggests ways for developing a strategy.
- **Institutional Roadmap**
 - Producing an overall roadmap or programme plan. Prioritising major deliverables and milestones by achievability, cost and institutional impact.
- **Designing and Managing an Identity Management project**
 - Project management issues particular to implementing Identity Management, including key institutional benefits of improved Identity Management for use in an institutional business case.
- **Selecting supplier solutions**
 - Where commercial procurement of systems or components is required, this section aims to help understand the IdM system solutions available, produce procurement criteria, and construct tender documents.

Other useful things you'll find at the bottom of the box

- Identity Management Glossary
- Providing network access for 'walk-in' users
- Identity Management Policy checklist
- Measuring user security be
 - How to run the “Password



Where to get it?

www.Identity-Project.org

