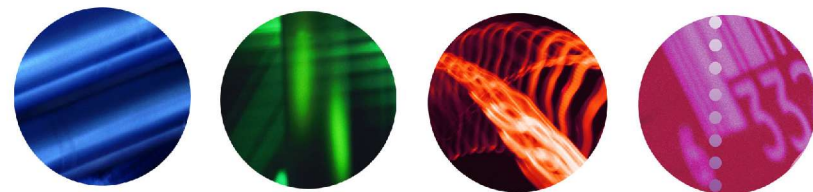


Introduction to Identity Management Systems

Alan Robiette, JISC (UK)

[<a.robiette@jisc.ac.uk>](mailto:a.robiette@jisc.ac.uk)



Overview

- What is meant by identity management?
 - What are identifiers (IDs) for?
 - How are they assigned and managed?
 - To which categories of people?
 - What properties of identifiers are important?
 - Comments on practical systems
 - ID management at national level
 - And finally a little about personal net IDs
-



History

- For a long time every system had its own IDs and login credentials
 - Poor user image – users have to maintain multiple identities and passwords
 - Leads to confusion and inconsistency – not all parts of the organisation working from the same data
 - Much duplication and waste of effort
 - Identity management aims to bring some order into all this
-



What are IDs for?

- All entities in IT systems need machine-readable names
 - A name which machines can process is a prerequisite for building systems to provide people with services etc.
 - Assigning IDs is a process of mapping real-world identities to machine-readable ones
 - Ideally done once at institution level
 - Promotes consistency and data quality
-



Registering people

- Who qualifies for services?
 - Students
 - Are there special categories: part-time, distance-learning, or others?
 - Do data from different sources need to be reconciled?
 - Staff
 - Full-time, part-time, visiting?
 - Alumni?
 - Others
 - These can be problematic: e.g. visiting academics/researchers, library affiliates etc.
-

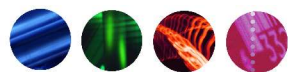
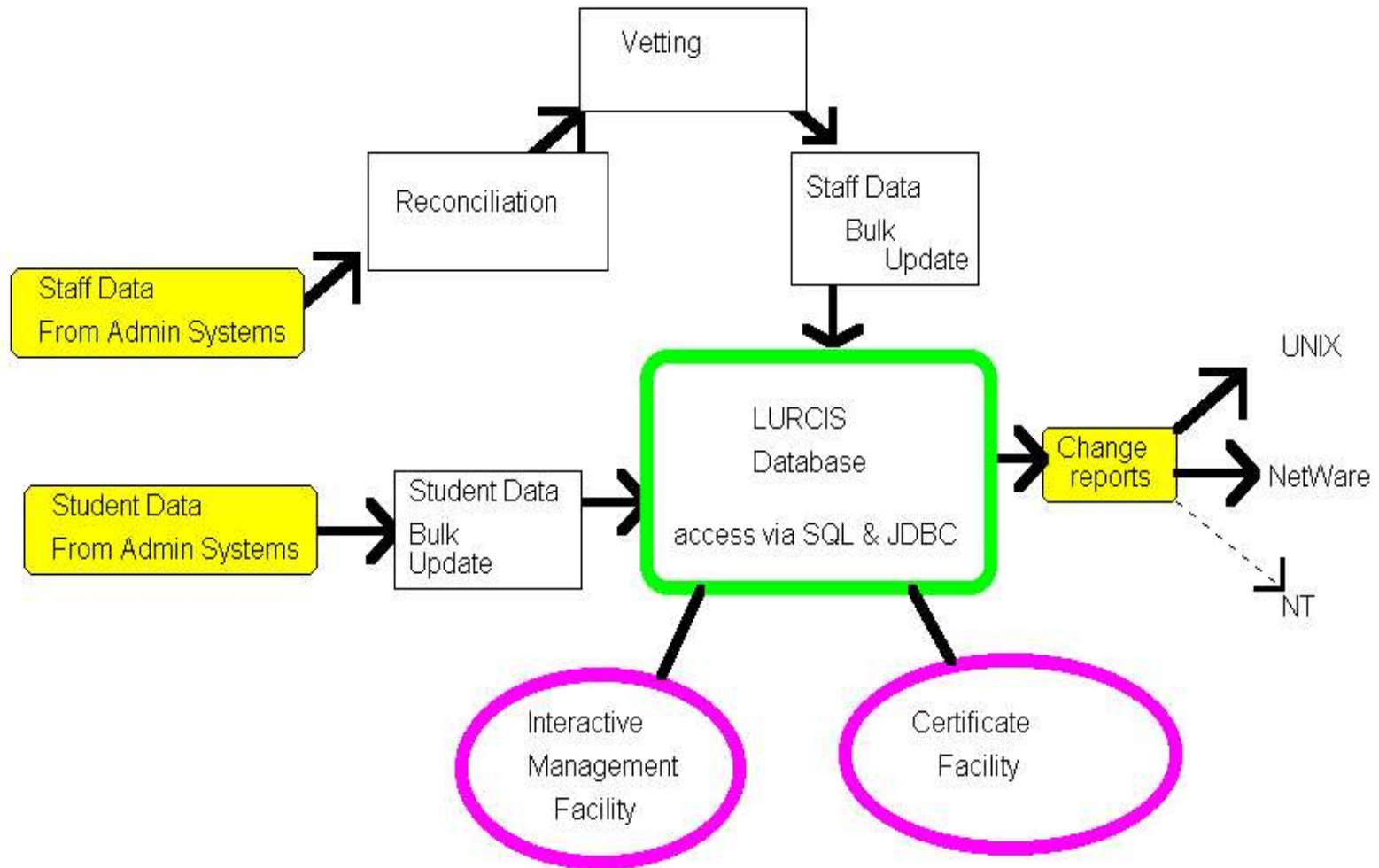


Registering people (2)

- Business processes often vary
 - Normally well established and robust for full-time students and staff on payroll
 - Real-world identities checked against national ID number (if this exists), bank details, tax reference etc.
 - But may differ for other categories, e.g. part-time students, library walk-ins
 - Typically leads to multiple sources of data which may need “cleaning” and reconciliation
 - Roland Hedberg will expand on this
-



A simple example



Assigning IDs

- At institution level IDs must be unique to the individual
 - E.g. need to resolve cases where two individuals have the same or overlapping names; the “John Smith” problem
 - Some other important properties
 - Persistence: can an identifier ever be reassigned? If so, when?
 - Human-understandable or opaque?
 - May need both for different purposes
 - Associated attributes (metadata)
-



The central IDM system

- Result of processes just described
 - Alternative names include IDM system; “person registry”; metadirectory
- Often implemented as a relational database
 - Commercial products exist, but many institutions build their own
 - RDBMS tools well adapted to building management interfaces, update procedures etc.



Provisioning systems

- Central ID database can then feed other systems
 - IT sub-systems e.g. desktop network, email directory, library management system, RADIUS server
 - Physical card systems, security
 - Etc.
 - Legacy systems may require their own ID formats
 - Mapping between identifiers is important
-

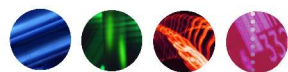
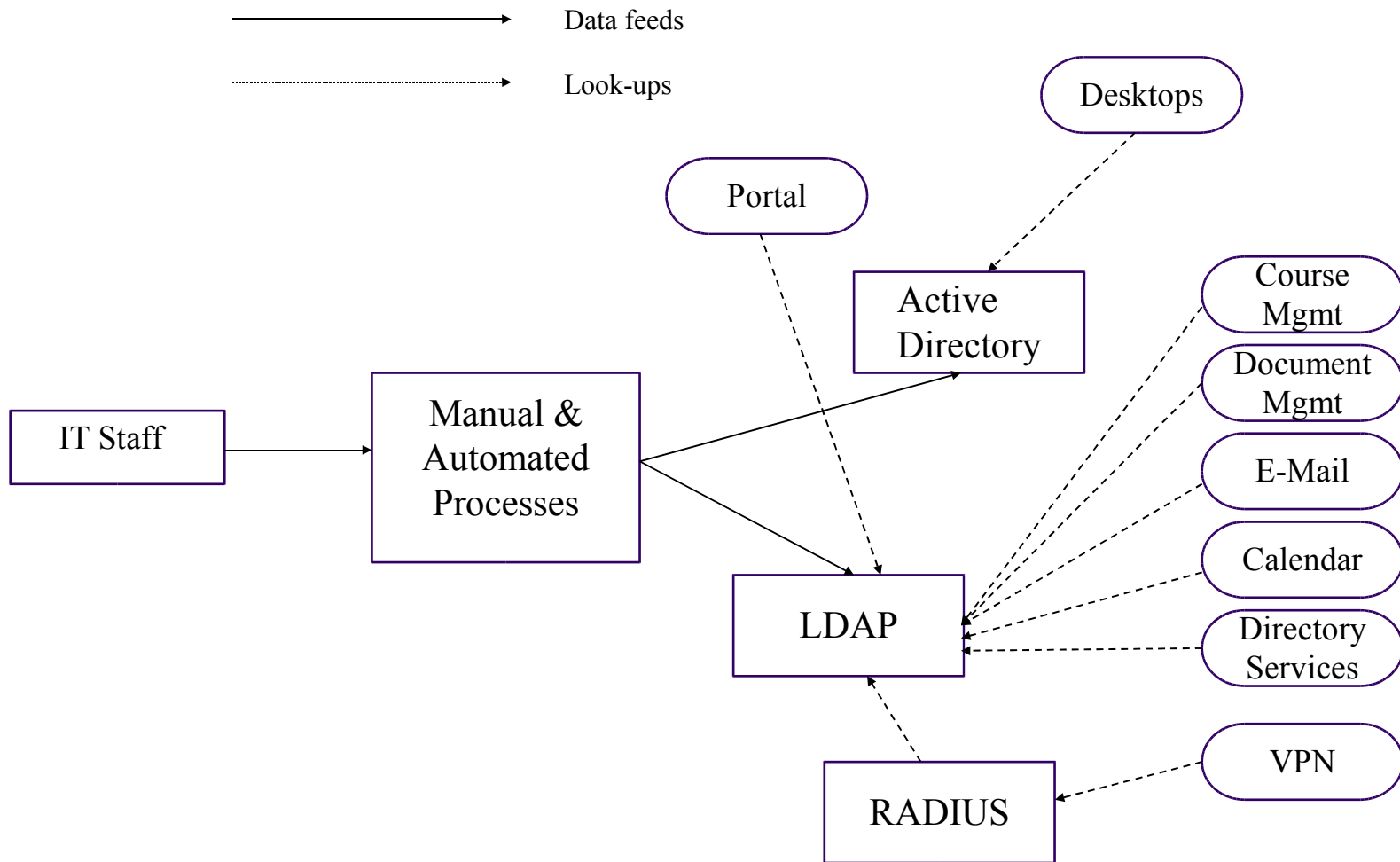


Dependent directories

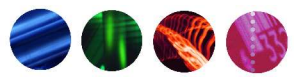
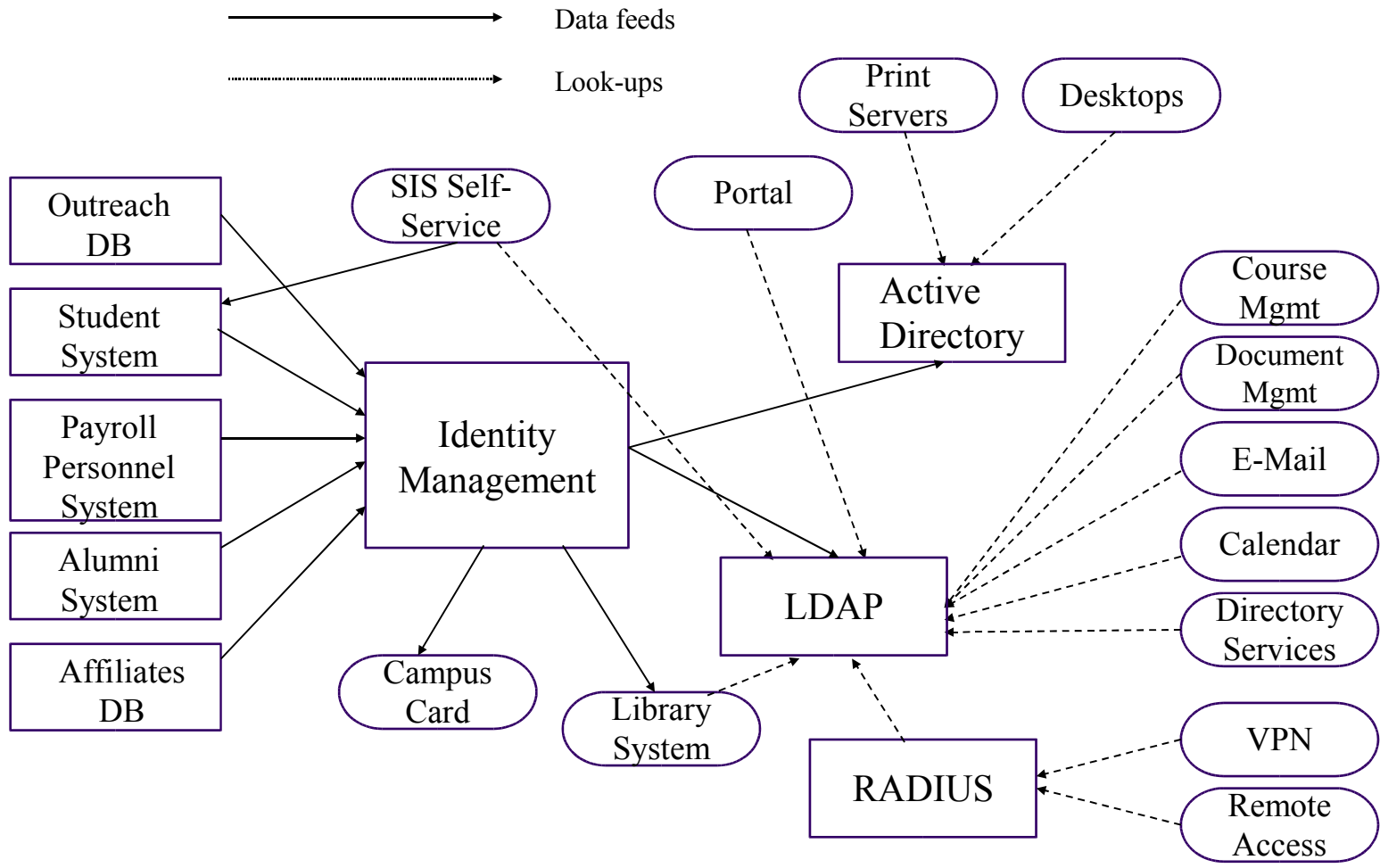
- Registries for IT sub-systems more often implemented as directories
 - For performance reasons, to support high volume of look-ups
 - Directory systems exist as both proprietary products ...
 - E.g. SunONE directory server, Microsoft Active Directory, Novell e-Directory
 - John Paschoud's talk will explore AD
 - ... and open source alternatives
 - E.g. OpenLDAP



Basic IDM approach



More complex IDM system



IDM at national level

- Several countries now committed to doing IDM at national level
 - Example: the UK Athens service
 - Built to manage access uniformly to licensed resources (e.g. e-journals)
 - Currently serves around 3 million users
 - Several hundred participating institutions
 - Virtually total coverage of academic publishers
 - Works by devolving ID management back to individual institutions



National level issues

- Scale goes up by 1-2 orders of magnitude
 - So resolving name clashes etc. becomes much harder: the devolved model leaves this to be done locally
 - So the unique ID is the *combination* of locally assigned ID + institution name
 - Cf. also eduPersonPrincipalName (uses syntax *userID@domainname*) as in Shibboleth
 - And eduRoam works essentially the same way
 - The alternative is a true national level registry, as in FEIDE project in Norway
-



National level problems

- Some people genuinely have multiple identities!
 - For instance someone who takes up a staff post in University A, while still a registered student at University B
 - In the devolved institutionally-managed model, the IDs will be quite separate
 - Because of this, not all resources are visible at the same time
 - Problems are intensified with life-long learning, student mobility etc.
-



Person-centric IDMs?

- Think more about life-long learning
 - People study at different points in their lives
 - At different institutions, and for different qualifications
 - Sometimes doing more than one type of study at once
 - A person-centric IDM system would handle this much more naturally
 - And with appropriate safeguards might cope with other personal needs also
-



But who might provide one?

- The two requirements are scale and long-term stability
 - Really only governments have successfully done this up till now
 - So for education, a national-level scheme (such as FEIDE) is a possible answer
 - Otherwise some options include
 - Banks?
 - Telcos and/or larger ISPs?
 - Maybe in future, not-for-profit trusts???
-



Conclusions

- Institutional-level identity management is the starting point for all core middleware
 - Relatively straightforward technically: most of the problems are to do with cultural issues, ownership, territory
 - National-level IDM schemes are on the increase
 - Most follow the devolved model, though this has some negative consequences
-



Finally

- Robust, long-lived personal electronic identities are an interesting prospect
 - With many advantages, provided security and user control could be guaranteed
 - But equally with corresponding dangers if compromised
 - If or when we get these, we'll have to worry about linking them back into our institutional systems
-

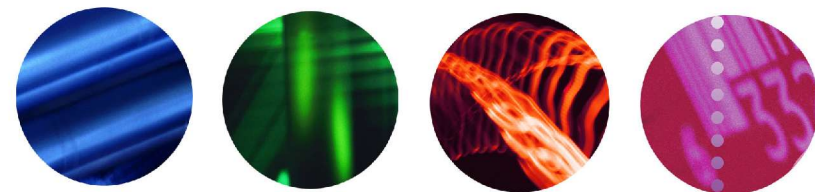


More information

- Identifiers, authentication, and directories: best practices for higher education
 - Internet2 middleware pages,
<http://middleware.internet2.edu/internet2-mi-best-practices-00.html>



Discussion ...



Supporting education and research