

eduserv



Best Practices in e-resource Access Management

Lyn Norris Eduserv Athens





Identity & Access Management

- Definition:
- An integrated set of policies, processes and systems that allow an enterprise to facilitate and control access to online resources for their users

- No magic bullet or system
- Not about technology itself



I&AM Facts for a typical organisation

- How many passwords do your users have to remember?
 - Over 20 is common
- What % of help desk calls are access related?
 - Password/remote access/username
 - Typical %s are 30-40%
- how many hours does it take to set up online privileges for a new employee?
 - One industry analyst estimates 28 hrs
- Auditing & accounting for how, when and by whom online resources are being accessed is difficult



IP authentication

- Simple to manage
- Simple for the user
- Recognition at enterprise level
 - Enterprise defined by network topology
- All users with access to the network get access to everything
 - No patron attribution
- Limit access to limits of on-site authentication
- Security as good as weakest system on network
 - JSTOR incident



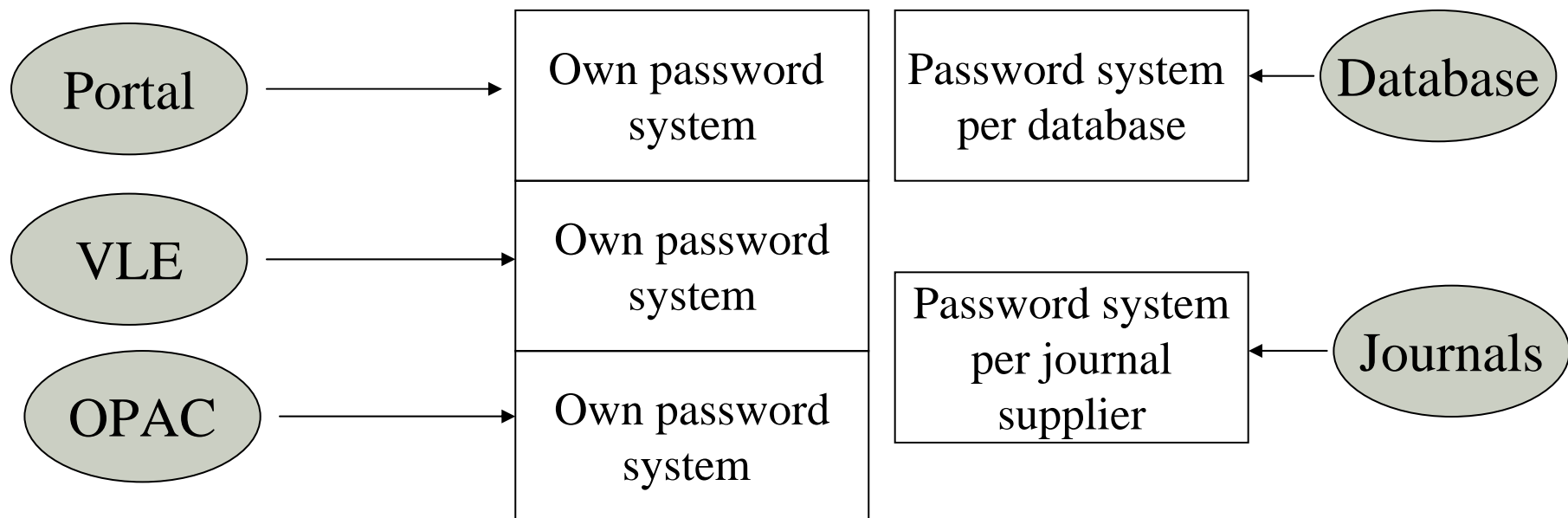
Referring URL & proxy servers

- Both need an authentication system
- Both send users to target resource as member of organisation
- Proxy servers relay every packet of data twice
- Referring URL is inherently insecure (easy to spoof)
- Referring URLs removed by personal password systems & firewalls

Typical organisation today

Local web resources

External web resources



- Each password system probably managed by a different group
- Each probably contains a different set of individuals



So what?

- Support effort
- Redundancy
- Inaccuracy
- Leads to insecurity

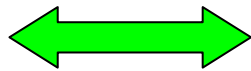
- Difficult for remote users
- Low take-up of e-resources

- Stick with IP or referring URL

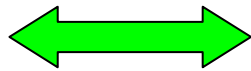
Organisational Single sign-on – the future

Local web resources

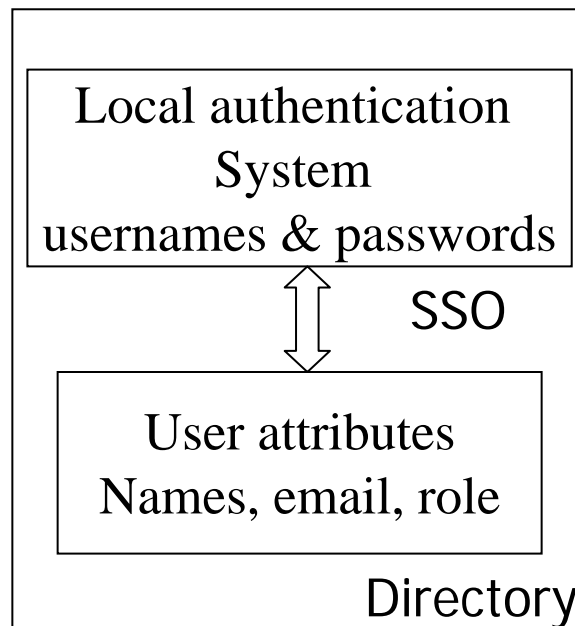
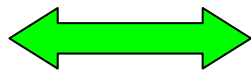
Portal



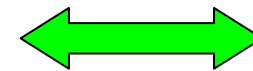
VLE



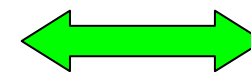
OPAC



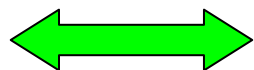
External web resources



Database



Journals



Authentication transfer protocol e.g SAML, Shibboleth, AthensDA



Benefits of individual username repository

- Single copy of user information
 - More accurate
 - More secure
- Audit control
- Ability to group users
 - Ability to allocate different e-resources to different user groups
 - Statistics at group level
- Personalisation linked to a single username



Obstacles

- Identifying all the users
- Categorising the users
- Maintenance processes
- Legacy systems
- Power games within the enterprise
- Privacy concerns



Privacy concerns

- Personally identifiable data
 - Names, email addresses, status
- Necessary to manage the user base
- Necessary to provide audit control
- Persistent identifiers necessary for personalisation



Mitigation

- Use pseudonymous identifiers
 - persistent for personalisation
- Don't duplicate information
- Try not to base usernames on names
- Balance against user memory

- Control what attributes are released to whom

Attribute release in action

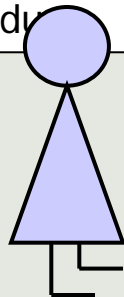
My Identity

Organisation: University of Tennessee

Role: student, post-graduate

Department: physics

Email: joe.s@tennesse.edu



My policy

This resource wants this information about you:

- Email**
- Role**
- Department**

1. Access resource

Physics resource

2. I need information about you

Access policy

- Email (registration)
- Students only
- Personalisation

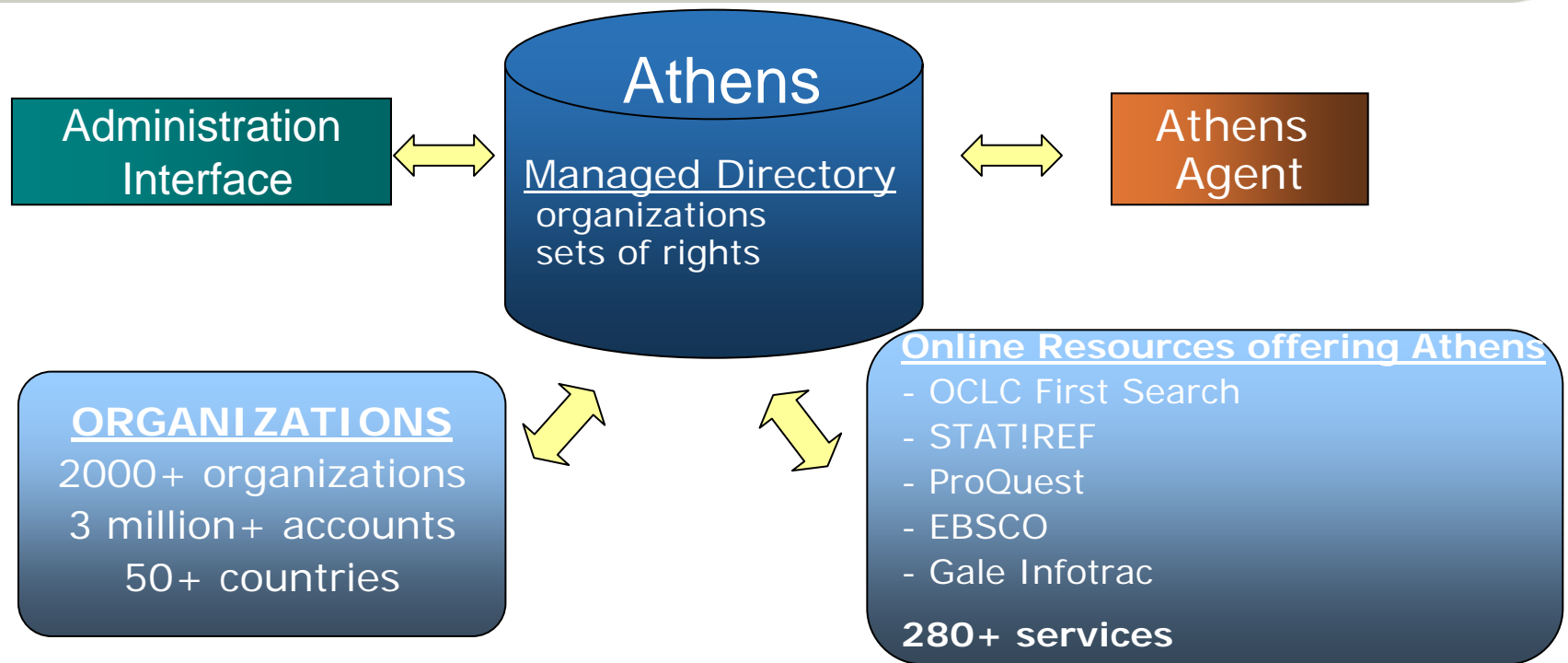
3. OK



Is organisational SSO possible?

- Yes – Athens has been doing it since 1996
- For all UK HE and FE institutions
- Devolved administration since launch
 - Essentially a managed directory service
- Devolved authentication since Oct 2002
- Total 5m users currently supported
 - 3.5m Classic Athens users
 - c1.5m AthensDA users
- Over 300 resources use it
 - Scopus, Lexis Nexis, NEJM, ProQuest

How Athens works...



- Athens hosts a managed directory, populated by librarians or library systems
- User management tools and statistics designed for librarians
- Users are authorized by checking against the contents of the registry when they request access to a service



Devolved or federated authentication

- has been a huge success
 - Operational since 2002
 - platform for federated IdM services
 - groundwork for SAML or Shib now available in 50-80 institutions

DA lessons learnt

- Institutions less prepared for DA than initially believed
- Significant levels of support required during project development and first year of operations
- Support tools needed to be developed
- Institutions have implemented using a very wide range of technologies



Individual credentials – the publisher view

- Opportunity to sell different types of licence
 - by attribute, eg department, faculty, or by role e.g doctors but not nurses
- Personalisation simpler
- Better auditing
- Potential for increased support
 - Publisher has to deal with every institution's directory separately
 - Unless in a managed federation like Athens



Credentials by individual not institution

- Coming
 - Not here yet
 - Privacy concerns to be allayed
- Standard attributes
 - Will take time to develop
 - E.g Athens student attribute
- Offer significant benefits to publishers
 - More control of users
 - Different licences by attribute type



Questions?

- For more information on Athens
- See www.athensams.net