Identity Management @ UCSB

A functionality and status update serving as a baseline for the ongoing identity discussion at UCSB.

Arlene Allen

November 2009
Enterprise Identity Management (IdM)
1. Creating identity information
2. Storing identity information
3. Maintaining identity information
4. Using identity information

History and design at UCSB
Current goals defined by UCSB password reset event
Futures
Final observations
Enterprise Identity Management

- Creating identity information
  1. Identity proofing
     Proofing is most often balanced against LOA required
     Official documents
     Transitive trust relationships
  2. Provisioning
     Point of entry
     Other data processing systems earlier in the chain
  3. Level of assurance (LOA)
     Formal definitions from NIST provide guidance to orgs
     Most orgs such as InCommon have adopted
Enterprise Identity Management

- **Storing identity information**
  1. Authentication repository
     - Storage for the authentication process(es)
  2. Data repository – typically a DBMS
     - All information contained in the Person object
  3. Data dictionary – defines attributes, CRUD and rights
     - Definitions of attributes in the Person object – source and edits
     - Specific rules for Create, Read, Update, Delete
     - Specific rules for authorization of CRUD actions
Enterprise Identity Management

- Maintaining identity information

1. Strongly bound – doesn’t change other than error correction
   Example: date of birth does not change
2. Bound with review – requires authorization beyond self
   Example: name change with external proof
3. Lightly bound – changed at any time by self with no review
   Phone number, home address, etc.
Enterprise Identity Management

- Using identity information

1. White pages
2. Authentication
   - LDAP, Kerberos, Active Directory, CAS, DCE, etc.
3. Authorization / attribute repository
   - Authorization decisions based on additional stored attributes
4. Business intelligence (BI)
   - Identity information is people information.
   - How many Lecturers with title code xyz this month, etc?
Enterprise Identity Management (IdM)

History and design at UCSB
1. LDAP project ca. 1997
2. LDAP for UID and Password
3. Oblix Netpoint using UID/Password for authn/z (7/2003)
4. Sun JES identity suite

Current goals defined by UCSB password reset event

Futures

Final observations
History and Design at UCSB

- LDAP project ca. 1997

1. Started as building a white pages repository for employees and students.


3. Recognition that an authentication mechanism was needed, but no specifics yet.
History and Design at UCSB

- LDAP for UID and Password

1. Early interfaces were all command line or developer kits
2. UCSB writes C code interface for web screens
3. PPS and student basic attributes integrated on nightly basis
4. Customers voluntarily update their own info
5. UCOP wants nightly extracts - UCNETID
History and Design at UCSB

- Oblix Netpoint using UID/Password for authn/z (7/2003)

1. OIT sponsors committee to evaluate
2. Netpoint as a web authorization method (WAM) is selected
3. Espresso web page created (pseudo portal)
4. UCSB wants to drive printed directory from LDAP
5. Directory Data Editors (DDE) invented to proxy person attributes
6. Oracle swallows Oblix - $60k/year maintenance goes up
7. UCSB budgets well into what will be constant downward trend
8. Software maintenance and upgrade is canceled (FY 05/06)
Sun JES identity suite

1. Sun makes full suite of all identity products available for a single flat rate. About the same as old Oblix maintenance.
2. The only full suites in existence are Sun and IBM
   IBM pricing is “breathtaking”
3. Microsoft is a possibility if using only MS software – unlikely
4. Open source, agnostic approach to identity and low price make Sun the only game in town
5. All development is now done with the Sun tools and services
6. Sun ultimately releases all code to “open”
7. Oracle buys Sun
Enterprise Identity Management (IdM)

History and design at UCSB

Current goals defined by UCSB password reset event
1. Preserve existing data and functionality
2. Increase password strength rules
3. Activation and Password reset processes
4. DDE and self-edit
5. Design around true DBMS as primary repository
6. Maintain and expand contents of data dictionary
7. Status as of November 2009

Futures

Final observations
Current goals defined by UCSB password reset event

- Preserve existing data and functionality

1. Attempt to preserve all people object information both current and inactive. Unique keys and password especially important.
2. SA creates U-reset program so as to provide interim method for activation and password resets. It is labor intensive for both service and customers.
3. DDE and Netpoint functionality need to remain as is possible
4. Nightly data extraction processes need to continue
5. Changes to authentication attributes are synchronously reflected to all authentication repositories
6. Two authentication repositories thus far – OIST and IC LDAPs
Current goals defined by UCSB password reset event

- Increase password strength rules

1. U-reset program embodied all strength rules + additional 8-32 characters, must be upper/lower with 1 or more numeric. Many special characters also allowed.
   The password cannot contain the UCSBnetID, SSN, email address or first/last name.
2. Compatibility with U-mail also required as is possible
3. Native enforcement of strength rules in LDAP was essential due to UCSB not locking the direct interface to the LDAP. In commercial world, most orgs lock the LDAP.
4. Align with external factors such as UCtrust
Current goals defined by UCSB password reset event

- *Activation* and password reset processes

  1. Activation starts at the UCSB Directory, and from there bifurcates to student and employee
  2. Student design attempts to follow existing Umail process
  3. Employee is tailored appropriately
  4. Knowledge based authentication (KBA) provides basic LOA but is insufficient for UCtrust or InCommon silver (no picture id)
  5. UID (UCSBnetID) and password are selected.
  6. Secret questions (five) and responses are harvested
Current goals defined by UCSB password reset event

- Activation and *password* reset processes

1. Password reset is dependent on UID and secret questions
2. Two questions must be responded to correctly else the account is locked and reset must occur at a front desk (2 tries max)
3. Neither history nor password expiration timing is used
4. The maximum length of the password attribute allows following the current research in use of phrases as password
Current goals defined by UCSB password reset event

- DDE and self-edit

  1. The new system is architected to support these functions
  2. Financial limitations have prevented their development at present
  3. Front desk support will have to be the near term surrogate
Current goals defined by UCSB password reset event

- Design around true DBMS as primary repository

1. First generation used the LDAP as the DBMS and the authentication repository. A poor design.
2. Current effort places all person objects and their attributes in a MySQL DBMS. This allows manipulation of the data using tools designed for such, and increased security since there are no processes from the outside world that will directly contact the DBMS server.
3. Two different versions of the DBMS are possible – the fully authoritative and protected version, and one that only contains a subset of the data (no PII). This increases security for business intelligence (BI) activities.
Current goals defined by UCSB password reset event

- Maintain and expand contents of data dictionary

  1. Data dictionary of globally maintained attributes is key to end point consumers or providers of identity
  3. Considerable work is required to add origination points, CRUD rules, ACI and additional attributes
  4. Over long term DBMS type data dictionary tools could be adopted
Current goals defined by UCSB password reset event

- **Status as of November 2009**

  1. The front-end provisioning processes for students and employees are running nightly in test.
  2. Identity Manager workflow engine is populating the SQL dbms’s and the OIST and IC test ldaps.
  3. Attribute information from the current production system has been pushed into the test system multiple times so as to ascertain the process is working properly.
  4. The user interface for the activation and password reset processes is in testing.
  5. Completed integration testing is likely this calendar year. Customer acceptance testing is still an unknown duration.
Enterprise Identity Management (IdM)
History and design at UCSB
Current goals defined by UCSB password reset event
Futures
1. How do we create additional functionality?
   1. UCtrust (federation)
   2. DDE and self-edit
   3. Espresso retirement or replacement?
   4. Where goes Enterprise IdM at UCSB?
      Identity, Repositories, Authentication, Attributes
5. Non-student, non-employee affiliates
Final observations
Futures

- How do we create additional functionality?

  1. OIST no longer has in house identity programmers
  2. New income (FTE perhaps) allows additional expenditure?
  3. UCSB self-help in the open source contribution sense?
  4. UCSB self-help in a financial coalition of distinct units?
  5. UCSB joins larger UC coalition of identity professionals who are, in some fashion, more effectively underwritten?
  6. ???
UCtrust (federation)

1. Federated identity is what allows us to sign onto a remotely hosted application with our UCSBnetID and password
2. Is most effectively implemented with Sun OpenSSO product
3. Internet2 MACE Shibboleth is next best alternative but more expensive in near and long term maintenance costs
4. Could be outsourced to another identity provider if a third authentication repository is created. UCLA as an example.
5. If the future of UC applications are central service providers (likely), whether insource or outsource, federation is important
6. Federation within the intranet can be used as a different way to solve heterogeneity issues amongst disparate service providers
Futures

- DDE and self-edit

1. The desirability of proxy and self service features is apparent from existing UCSB experience
2. DDE is of moderate complexity and self-edit less so
3. DDE allows a proxy person to change a small set of specific attributes on one’s behalf
4. Self-edit attributes tend to not have any impact on business processes and are usually additional detail for “white pages”
5. Priorities and funding mechanism would be the next discussions
6. Advisory groups can help with the priorities of this and other future goals
Espresso retirement or replacement?

1. Espresso is a single signon point of entry web page to 5 financial applications, CSF, GradNET and Purchase Order Repository. We call it a pseudo-portal.

   https://espresso.ucsb.edu/

2. While Netpoint is still functional, Espresso web page will continue to function. Lifespan is unknown but a few more years is possible. Doug Drury’s people have maintained the code.

3. OpenSSO is the Sun software vehicle for any replacement.

4. Advisory groups get to debate ROI of doing over vs. retirement.
Futures

- Where goes Enterprise IdM at UCSB? (Identity)

1. A single identity can correlate to a single authentication mechanism, such as a password or token, and simplifies use
2. Multiple authentication mechanisms can correlate to a single identity, but then (usually) sacrifice common password
3. A single IdM requires the multiple consumers of identity (services) to agree on many definitions and processes
4. Federation is a finesse to 2 and 3 in that there can be multiple independent provisionings, authentication mechanisms, and derived meanings alongside (potentially) a single password. The common language of federation provides the bridge.
5. The recent evolution of identity management (IdM) has seen federation as a substitute for enterprise identity
Where goes Enterprise IdM at UCSB? (Repositories)

1. Enterprise identity repositories were invented so as to have a single attribute storage mechanism. Referential integrity issues are thus eliminated. Authorization activities are based on a single instance of the data, and thus consistent.

2. Problems tend to revolve around multiple front end provisioning processes that all believe they are authoritative.

3. Second level problems revolve around disparate definitions and reactions for the same attribute depending on its source.


5. The Bad: These are seldom ever dealt with beyond high expense solutions within identity management.
Where goes Enterprise IdM at UCSB? (Authentication)

1. Enterprise authentication potentially leverages a single middleware technology. Examples would be CAS, Kerberos, Active Directory, LDAP, NIS, DCE etc.

2. The Good: Economy of scale

3. The Bad: Count the times this has happened on one hand

4. Enterprise authentication is a prerequisite to single signon (SSO). Single signon has mutated to mean common signon and adds greater complexity to enterprise authentication.

5. SSO is frequently finessed by requiring access to the complete set of services through a portal

6. Portal solution is then hard due to requiring all services to be compatible with the portal being used
Where goes Enterprise IdM at UCSB? (Attributes)

1. Attributes can be coarse or fine grained.
   Coarse example: Employee
   Fine example: Start date of 9 month secondary appointment
2. Role Based Access Control (RBAC) is all about fine grained attributes. The services capable of solely relying on coarse attributes are easy to enumerate and not growing in number.
3. The Internet2 Eduperson object defined most of the coarse attributes and has seen little enhancement in recent years.
4. Inevitably, services (applications) all have their own attribute repository
5. A centrally maintained data dictionary is essential in coordinating the coarse and fine grained attributes
Non-student, non-employee affiliates

1. Examples abound – Library card, contractor, pre-employee, wireless, post-employee, emeriti, guest, post-student, etc. We refer to them as “miscellaneous demographics”.

2. The services normally authorizing these individuals in any particular category are few.

3. As previously discussed, every demographic stream must have the complete CRUD lifecycle defined and implemented – a significant capital expense.

4. Governance needs to carefully assess the ROI of both the increased capital and ongoing operational expenses.

5. Technology has yet to demonstrate an ability to offload increased operational work to distributed organizations
Final observations

- Basic authentication and white pages

  A single userid and password fulfills the largest portion of an institution’s authentication needs.

  Adding a small set of attributes is sufficient for federation. Beyond Eduperson, UCTrust currently uses: Ucnetid and Assurance.

  Additional attributes such as email, phone numbers and address are sufficient to maintaining a useful white pages.

  Benefits of white pages are many, however, there is a constant evolution in policy as regards what can be made public.
Final observations

- **Identity providers (IdP) and service providers (SP)**

  Identity providers are effective in direct proportion to their authority in the lifecycle of the person object and its embodied attributes. The more that external forces affect an identity, the more that identity will be inaccurate.

  Service providers achieve greatest success in the identity interface if no particular function within the service requires any attribute to change within the identity provider’s repository, and the attributes of identity are sufficient to that service’s authorization.

  IdP’s are best when authoritative in the coarse grained attributes. SP’s must maintain the fine grained attributes for which that SP is authoritative.
Final observations

- **Identity providers (IdP) and service providers (SP) contd.**

  An SP may optionally be an IdP.

  The SP might have a requirement for a local but non-authoritative identity repository. The person object comes from an authoritative identity repository and CRUD processes are in place for synchronization.

  The SP may add authoritative attributes to the person object where such attributes are not present in the authoritative IdP for that person.

  The SP may add additional person objects not known to the globally authoritative IdP. Note that this variation becomes similar to an IdP that is a federated peer. One would choose to federate if there were other SP’s needing to consume these additional identities.
Final observations

- **UCTrust requires the UCSB authoritative IdP to be federated**

  The processes of federation run autonomously. The authoritative IdP processes may be down and the federation might still be up.

  For both process management and technical reasons, the federation process refers to its own identity repository that is provisioned by the identity workflow engine based upon the business rules of which person object may be legitimately shared. Typically, this is another LDAP.

  The authoritative IdP must have the CRUD processes in place for the unique attributes associated with federation.
Final observations

- High end functionality such as SSO, Portal, RBAC, VD, etc. (single sign on, web portal, role based access control, virtual directory)

Such functions come at a steeply increased cost of creation and maintenance. It is important that the consumption of such functionality is orchestrated at the institutional level and approaches general adoption, else the degree of leverage required to obtain a positive ROI is not achieved.

Enterprise IdM can easily become a partially stranded investment due to the disconnect between its repertoire of features, and those features that are in wide use. Put differently – it is easy to overspecify an IdM.
Final observations

- Complex service providers

The complexity of some systems, such as ERPs, is so high that they must have an internal identity repository.

From the identity workflow engine perspective, these do not look any different than the authentication repository of an identity provider (IdP).

In such instances, the rules of authorization to that service will tend to be the determining factor in any initial “push” provisioning into that service’s repository. Email is a possible example.

Since the tools of authorization are within the service provider (SP), the creation of a local identity will generally be a form of “pull” provisioning. The example here is most, if not all ERPs.
Final observations

- Finance of Identity at UCSB

  Every fiscal year from 2004 onward has seen less money allocated to IdM than the previous year.

  IdM income is now (optimistically) at $155,671. Worst case $145,056. IdM expenses after all recent cuts are now $262,966.

  Sun software support might be canceled at the end of this FY, saving approximately $72,000. IdM will still be in yearly deficit.

  UCSB future needs first require us to catch up with supporting present expenses.
Appendix
Fault tolerance is achieved by duplexing each hardware component. Disks are mirrored.
Log In to UCSB Identity Manager

UCSBnetID
Password

Login  Forgot Password?

Need to activate your UCSBnetID account?
Look Up UCSBnetID
(Temporary link - please add it to the gateway page.) First-Time Login For Students
(Temporary link - please add it to the gateway page.) First-Time Login For Employees
Account Activation - Set New UCSBnetID and Password

Please select your desired new UCSBnetID and enter a new password below.

UCSBnetID: benwilson01

Your password must adhere to the following policies:

- Your password must have a minimum of 8 characters and a maximum of 32 characters.
- Your password must have a minimum of 1 numeric character, 1 upper-case letter and 1 lower-case letter.
- In addition to letters and numerals, the following special characters are allowed: ~!@#$%^&*()_+=- {}[];:'"\,\&<\>.?/
- Your password cannot contain your UCSBnetID, social security number, name or email address.

Password: *

Confirm Password: *

Please enter an email address below if you would like a confirmation of your account activation sent to you. You can also save the email address as an optional email address in your account by checking the box below.

Email Address: *

Check this box to save this email address: 

* indicates a required field
Account Activation - Set New UCSBnetID and Password

Please select your desired new UCSBnetID and enter a new password below.

UCSBnetID: ben_wilson*

Your password must meet the following criteria:
- Your password must contain at least 9 characters and a maximum of 32 characters.
- Your password must contain at least 1 numeric character, 1 upper-case letter and 1 lower-case letter.
- Special characters are allowed: ~!@#$%^&*()_+-=\{{}\}|:;",'\&<>/D, social security number, name or email address.

Password: ben_wilson03
Confirm Password: ben_wilson03

Please enter an email address below if you would like a confirmation of your account activation sent to you. You can also save the email address as an optional email address in your account by checking the box below.

Email Address: [

Check this box to save this email address: []

* indicates a required field

Continue Cancel
# Account Activation - Authentication Questions

Please provide answers to each of the following questions. This information will only be used to authenticate you in the event that you forget your password.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is/was your favorite sport or activity?</td>
<td></td>
</tr>
<tr>
<td>What is/was the name of your favorite person in the world?</td>
<td></td>
</tr>
<tr>
<td>What is/was the name of the street you grew up on?</td>
<td></td>
</tr>
<tr>
<td>What is/was your major?</td>
<td></td>
</tr>
<tr>
<td>What is/was the name of your pet?</td>
<td></td>
</tr>
<tr>
<td>What is your favorite color?</td>
<td></td>
</tr>
<tr>
<td>What was your mother's maiden name?</td>
<td></td>
</tr>
</tbody>
</table>

[Continue] [Cancel]