Contents

What is Identity Management? .................................................................................................................................................. 1

Charge .................................................................................................................................................................................. 2

Approach .................................................................................................................................................................................. 2

   February 2005 ........................................................................................................................................................................ 3

   April 2005 ............................................................................................................................................................................... 4

   May 2005 ................................................................................................................................................................................ 4

   June 2005 ............................................................................................................................................................................... 5

   July 2005 ............................................................................................................................................................................... 6

   August 2005 .......................................................................................................................................................................... 6

Accomplishments to Date .......................................................................................................................................................... 6

   Populations, Affiliations and Service Entitlements (PASE Policies) ..................................................................................... 7

   NetID Assignment for New Hires ........................................................................................................................................... 8

   University Directory Service (UDS) Appropriate Use of Data Policy .................................................................................. 8

   Access to Data (A2D) Guidelines ......................................................................................................................................... 9

   Identifying Next Steps towards a Single ID Card, Clarifying Credentialing .................................................................... 9

Next Steps .............................................................................................................................................................................. 9

Conclusion ............................................................................................................................................................................ 13

Appendix I:  IMLG membership and charter sub-team rosters ....................................................................................... 14

Appendix II: Establishing NetIDs for New Populations .................................................................................................... 16

Appendix III: UDS Appropriate Use Policy and Process for Accessing UDS Data .............................................................. 18
Identity Management Leadership Group
A Progress Report

What is Identity Management?

Identity management allows us to tell if individuals are who they say they are, whether they are affiliated with the University and what entitlements that affiliation allows. It permits data custodians and service providers to control access to information and/or services, according to an individual’s identity, roles and responsibilities. New technology is enabling us to build an integrated network of relationships between data custodians and service providers on campus. Indeed, the University of Wisconsin-Madison (UW-Madison) is building an infrastructure that will allow us to retain our highly decentralized organizational structure while at the same time minimize the many redundancies in how the campus captures and shares the information necessary for effective and efficient customer service. Ideally, this infrastructure will further ensure individual privacy rights, support regulatory compliance, and secure essential university services and applications. It will also enable us to provide services selectively to students, faculty and staff while also extending services to a larger campus community – such as prospects, applicants, alumni, retirees, visiting faculty and consultants.

Underlying identity management at UW-Madison is a complex set of systems, practices, myths and legends that have evolved over the past several decades. In November 2004 Provost Peter Spear and Vice Chancellor Darrell Bazzell charged a group of campus leaders to establish and/or revise policy, clarify current policy and procedures, and essentially demystify identity management on campus (Appendix I - membership roster). UW-Madison is already recognized nationally and internationally as a leader in the identity management arena; the engagement of key campus leaders and stakeholders in identity management governance is considered a significant accomplishment by our peers in the national Internet2 community: “By leading a path towards a coherent, enterprise-wide approach to these critical issues (at a time when end-user complexity overload, audit and accountability, policy drivers, etc. are looming), and at an institution where the estimated degree of difficulty is 9.9, UW-Madison is becoming the totem of our times”

1 Communication from Ken Klingenstein, Internet2 Director of Middleware and Security, October 2005.
**Charge**

The Provost and the Vice Chancellor for Administration charged the Identity Management Leadership Group (IMLG) with the following:

- Define identity management process roles and responsibilities for obtaining access to information and services;
- Establish criteria about how decisions are made;
- Coordinate and negotiate access to information and services;
- Seek efficiencies, especially in the area of eliminating duplicative cards for ID and security purposes.

In addition, the group was charged with answering many of the strategic policy and procedural questions regarding the University Directory Service (UDS) and the new PASE system (Populations, Affiliations, Services and Entitlements).

The IMLG replaced the following campus committees: UDS Steering Team, the Photo ID committee and the ad hoc PASE policy group.

**Approach**

Building a strong, secure and efficient identity management system involves sorting through complex technical possibilities that produce an abundance of policy and procedural issues. The IMLG recognizes these complexities and together are developing an efficient process for addressing detailed questions and analyses that are difficult to resolve quickly. This process – the creation of subgroups to articulate, deliberate on and submit recommendations to the IMLG – while potentially time-intensive, has the advantage of being inclusive, brings all the relevant players to the table and ensures that policies are not made unilaterally or in a vacuum. With that in mind, it should be noted that the IMLG is often frustrated by what feels like a lack of progress. Such is the nature, however, of the “discovery phase” of project work.

To date, identity management at UW-Madison has been a fairly ad hoc process because of an absence of policy and/or an absence of standards for how decisions are made. As new systems, applications and services are introduced across campus, procedures to coordinate and manage access also need to be developed. The IMLG agreed that it was appropriate for the group to focus on policy yet recognized the need for technologists and functional staff to “feed” the IMLG with
appropriate and/or “hot button” policy issues that must be resolved before technical work can continue. Thus, the work of the large group proceeds concurrently with that of the subgroups.

What follows is a brief synopsis of how the group has approached identity management since first meeting in February 2005.

February 2005
The first meeting of the group was held in late February 2005 with an aim of setting priorities and a timeline. It was agreed that the group needed to identify the milestones within the lifecycle of the NetID\(^2\) as well as take steps toward reducing the number of ID cards on campus. Further, it was agreed that the group take the time necessary to be educated about how the UDS works, about the NetID lifecycle (e.g., when is a new ID activated, by whom, what identity proofing is required, etc.), and about current entitlements associated with NetIDs.

---

\(^2\) A NetID is a unique identifier, or credential, consisting of a username and password which is used by the UW-Madison community to determine authentication for online resources. It verifies a user's identity, ensures the privacy of personal information, and limits use of campus resources to those who are authorized. The NetID is required for access to such services as My UW-Madison, WiscMail, and WiscCal. Generally, the NetID is the user name that appears to the left of the @ sign in the campus email address (for example, astudent@wisc.edu).
A roundtable discussion produced this list of issues:

- Multiple log-ins
- Licensing resources
- Privacy
- Lifelong access
- Guest access
- Uniformity across user groups
- E-business
- Identification and authentication
- Reduction of the number of ID cards
- NetID and social security numbers
- Barriers to access where we don’t need them
- Physical access and access to data

April 2005

At our April 2005 meeting the group heard from DoIT’s Middleware Systems Technologies\(^3\) staff about how the University Directory Service (UDS) works on campus and began discussions to define appropriate use of UDS. It was decided at this meeting that a “UDS Appropriate Use team” should be created to work with DoIT’s Middleware staff to sort out a process for providing access to UDS. Questions at the meeting included:

- What/who determines “bundle of services?”
- What do people need to know to determine affiliations and who has access to this information?

A presentation was made regarding the services that are currently received by campus community members (e.g., valid ID card holders and corresponding service authorizations). A middleware glossary of terms was distributed – [http://www.doit.wisc.edu/middleware/glossary.asp](http://www.doit.wisc.edu/middleware/glossary.asp).

May 2005

In May the group began processing the larger questions surrounding the lifecycle of the NetID by discussing several realistic scenarios. As a result, the following policy issues were raised:

- How do we define NetID and distinguish it from other identifiers (e.g., student ID, Empl ID, SS#, WiscCard Account #, Web ISO, etc.)?
- What identifier is used to provide the “key” to access services?

---

\(^3\) Middleware is defined as the software layer that lies between the operating system and the applications on each part of a distributed computing environment. The UW-Madison is now building enterprise-wide information systems by integrating previously independent systems, together with new applications. This integration process has to deal with legacy applications and disparate systems, which the Middleware group brings together to form cohesive end-to-end systems.
What is the relationship of this “key” to the ID card(s)?
Should there be an expiration date on the ID card or should there be renewal dates such as that on a drivers’ license? Does the ID card last forever?
What should the relationship be between ID cards and debit/credit cards?

How do we define the changing nature of the populations we are serving?
Applicant to student to alumni
Pre-faculty to post-employment
Pre-staff to post-employment

How do we define services for our primary populations and their affiliations?
Are there fees for service(s) provided?
Are the services electronic services, data related or does the service require physical access?
Are there limits to the service(s) provided?

How does the negotiation process work – that is, who defines who gets what and how is the service provider involved in this process?

What are the PASE sponsor’s responsibilities for communicating about ID requirements, services, etc?
How do we define PASE sponsor?
How do we define PASE service provider?
Who communicates what to whom along the NetID lifecycle (e.g., if a bundle of services is created, how will the service provider know if/when access is granted)?

June 2005
This meeting engaged the group in reviewing a draft Appropriate Use Policy for UDS, and approved a policy regarding the creation of NetIDs for undergraduate applicants, the first new affiliation submitted through PASE to the UDS. In addition, the group formalized the ad hoc work that was being done by multiple subcommittees by introducing a set of project charters and proposed establishing five IMLG sub-groups:

1) Populations, Affiliations and Service Entitlements (PASE) Policies
2) NetID Assignment for New Hires
3) UW-Madison University Directory Service (UDS) Appropriate Use of Data Policy
4) Access to Data (A2D) Guidelines
5) Identifying next steps toward a Single ID Card and Clarifying the Credentialing Process for IDs at UW-Madison

These charters were created as a way to clarify objectives and deliverables, roles and responsibilities, customers and stakeholders, resources, constraints and boundaries. Moreover, using

---

4 Providing undergraduate applicants with NetIDs allows applicant access to the My UW-Madison portal earlier in the admissions cycle. In addition, it eliminates the need for the Undergraduate Admissions office and/or the Office of the Registrar to issue PIN numbers to applicants.
this set of charters to frame the complex identity management tasks facing us helps to ensure that the projects stay within scope. *(See the section on Accomplishments for an update on each of these charter groups.)*

**July 2005**

The group reviewed a draft policy on the creation of NetID’s for new affiliations *(Appendix II).* This policy was created as a result of the work that was done to get undergraduate applicant information into the UDS. It was agreed that the next new population to review will be new hires (Charter #2 noted above). The group spent the remainder of the meeting reviewing the draft project charters and discussing how the IMLG should be informed of issues and policy implications. It was agreed each of the charter groups would be responsible for submitting updates for the monthly IMLG meetings.

**August 2005**

The August meeting of the IMLG consisted of a series of updates and clarifying questions regarding the various charter groups. It was decided that the charter subcommittees needed to do some work to sort out the myriad technical and procedural details before the IMLG could appropriately focus on policy.

**Accomplishments to Date**

Significant accomplishments have been made toward the creation of a robust identity management infrastructure that supports and enhances the educational, research and outreach missions of the Institution. As noted earlier, this work is complicated and is made more so by the heightened expectations of our campus constituents who require and deserve efficient authorization and authentication services. Further, there are significant environmental and political challenges. Campus budget reductions, staff turnover and a limited amount of human resource time to devote to these issues restricts the IMLG from moving forward as expeditiously as one would hope. The work of the IMLG is broad based and touches every level of campus infrastructure. As policy decisions are discussed it is imperative that there is wide-ranging agreement about functional and technical priorities. To that end, it is imperative that the IMLG take a leadership role in moving to a more collaborative model of providing and leveraging identity management infrastructure at UW-Madison. The work of the IMLG continues to move forward; the accomplishments are outlined here.
<table>
<thead>
<tr>
<th>Charge to IMLG</th>
<th>Accomplishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define identity management process roles and responsibilities for obtaining access to information and services</td>
<td>Chartered five sub-teams (see below) Established UDS appropriate use policy</td>
</tr>
<tr>
<td>Establish criteria about how decisions are made</td>
<td>Ongoing work with charters, and evaluating new processes</td>
</tr>
<tr>
<td>Coordinate and negotiate access to information and services</td>
<td>Established template for assigning NetIDs to new affiliations</td>
</tr>
<tr>
<td>Establish efficiencies (e.g., eliminating duplicate ID cards)</td>
<td>Chartered sub-team to analyze the use of ID cards on campus and clarify credentialing</td>
</tr>
</tbody>
</table>

The Identity Management Leadership Group was successful in launching five different working groups and has begun the process of initiating detailed charters for each group. Updates from each of these charter groups are listed here:

**IMLG Charter Sub-Teams**

**Populations, Affiliations and Service Entitlements (PASE) Policies**

UW-Madison is pioneering an integrated system called PASE\(^5\) that will, in effect, revolutionize the way we think about identity management. Having appropriate policies in place will be critical for the timely development and implementation of this phase of the PASE project. The PASE Policies project team will therefore convene on an as-needed basis during PASE Phase II to identify, deliberate on and develop governance, policy and process statements. These will then be brought to the IMLG for approval and ratification. The IMLG also established the PASE User Interface Requirements group (*Appendix I*) to support cooperative development of the web-based interfaces that will be used in a distributed fashion to perform PASE functions such as creating a new affiliation, managing affiliations and mapping affiliations to services. This group was convened in August 2005 and is also documenting PASE policy requirements as they arise (these will be submitted to the PASE Policy Team).

---

\(^5\) PASE is currently entering its second phase – the development of the PASE service entitlement engine and PASE user interfaces. Delegated administration is a fundamental feature in PASE, enabling sponsors and service providers to perform affiliation management (creating new affiliations, assigning individuals or populations to affiliations, etc.) and entitlement management (assigning entitlements to affiliations) functions.
NetID Assignment for New Hires

The purpose of this project is to examine the current practices for providing services to new hires, both staff and student employees at UW-Madison, determine the requirements necessary to enhance those practices and prepare a project plan to implement those enhancements. This group convened in mid-August 2005, has conducted a requirement analysis, and is preparing a final report for the project sponsors with recommendations for next steps.

(UDS) Appropriate Use of Data Policy

The purpose of this effort is to develop, publish and implement an Appropriate Use Policy (AUP) for UW-Madison’s University Directory Service (UDS) data. The UDS AUP, approved by the IMLG in July 2005, has been implemented and publicized. Process and procedures for requesting and gaining access to UDS data have been amended where necessary to be consistent with the AUP (Appendix III).

The process and the AUP are available at [http://www.doit.wisc.edu/middleware/use.asp](http://www.doit.wisc.edu/middleware/use.asp)

Access to Data (A2D) Guidelines

This project would bring together campus representatives to address questions such as:
• What is the officially approved source for gaining access to various categories of institutional information for given classes of requests?
• When should a service-oriented approach be favored?
• What data sources should such generic services use to gain access to the information they need?

The sub-team is chartered to gather campus stakeholder input on these issues and, where appropriate, make recommendations to the IMLG on possible guidelines and principles covering access to data and information.

The sub-team has reviewed the draft charter and the next step will be for representatives of the sub-team to meet jointly with the IMLG to refine and approve the charter, settle on deliverables and timelines and begin work.

**Identifying next steps toward a Single ID Card and Clarifying the Credentialing Process**

There are significant philosophical, technical and fiscal issues involved in moving toward a single ID card. The IMLG discussed some of these issues and agreed that a “smart card” or a single ID card will not work on campus until decisions are reached on other issues. For example, we need to decide who gets a University ID card and who the service providers are, etc. Furthermore, it was agreed that the issues need to include a review of the identity proofing and credentialing processes that would enable a member of the university community to receive an ID card. It was suggested that a thorough review of the credentialing process could, in fact, help to reduce the number of ID cards currently being produced on campus. These issues are to be addressed concurrently. Ken Frazier of University libraries agreed to chair the team.

**Next Steps**

The IMLG needs a strategy for determining what policies must be developed in order to move the technical applications forward while addressing the needs of campus and considering best business processes. Of course, some policies are dependent on other policies being developed, some policies are dependent on what is technically feasible, and most are dependent on whether the campus is willing and/or able to change the way they do their work.

Within the next year the IMLG will:
1) Hear regularly from each of the charter sub-teams regarding policy issues/decisions that need to be made.
   - Continue exploring the next steps toward a reduction in the number of ID cards by finalizing the ID card charter and establishing an IMLG subgroup. This group will inventory ID cards currently being used on campus, review the credentialing process on campus, will need to benchmark with peer institutions and will need to obtain documentation from the last time one ID card was discussed at UW-Madison. Recommendations will be brought to the IMLG;
   - Establish a web presence for teams to post agendas and minutes;
   - Ensure that each sub-team establish project milestones so that the IMLG can, in turn, establish a detailed timeline;
   - Revisit the UDS access approval process to determine how well it is working.

2) Determine decision/policy drivers.

3) Establish an identity management philosophy that will produce efficiencies and clarify ambiguous roles and responsibilities. The group is expected to begin this process in December 2005 by establishing answers to the following questions:
   - Is the UDS the “official” repository of identity management information on campus?
     o If yes, will campus service providers that use “person” information be required to use the UDS as the source for this information? (see UDS AUP)
     o Will exceptions be allowed and what is the process for requesting an exception taking into account whether DoIT would be able to address the business needs?
   - Are the services that are created to distribute UDS information the “official” services for identity information?
     o If yes, are campus service providers required to use them?
     o Should the WebISO⁶ service be the only place where the NetID password can be requested?

---

⁶ WebISO (web initial sign-on, sometimes called Single Sign-on) refers to systems designed to allow users to authenticate to web-based services across many web servers using a central authentication service. The user does not have to authenticate (i.e., sign on) multiple times to each different server or service.
o Will exceptions be allowed and what is the process for requesting an exception taking into account whether DoIT would be able to address the business needs?

o Is it required or desired that any campus service that performs user authentication use WebISO unless an exception is granted?

o Is ACT (AuthNZ Coordinating Team)\(^7\) the campus group charged with delivering “official” services for identity management and implementing IMLG policies on a technical level?

---

\(^7\) The Authentication and Authorization (AuthNZ) Coordinating Team (ACT) is a standing committee whose mission is to coordinate the definition and deployment of shared infrastructure services for authentication and authorization (AuthNZ) available to all developers and integrators across UW-Madison. The vision is a single, coherent suite of production-quality AuthNZ services.
**Conclusion**

In the first six months of its existence, the IMLG has accomplished much towards establishing structures to frame and address the numerous and complex identity management policy and process questions that are a necessary part of building a secure and highly functional infrastructure. The work of the IMLG and its sub-teams is most likely to be an iterative process – striking the right balance between policy and business process deliberation and technical development and implementation. As the diagram below illustrates, with these structures in place, work has been initiated in two key functional areas (NetIDs for new hires and ID card credentialing). Each of these initiatives is highly dependent on the work of three key policy areas (UDS, PASE, A2D). As the interdependencies among each of these areas are clarified and the issues are reviewed, policy will more readily be defined.

IMLG members understand that identity management demands more than technical consideration and recognize the strategic significance of our collaboration. That UW-Madison has succeeded in establishing effective governance in this area has already gained attention from our peers and our efforts are considered landmark.
Identity Management Leadership Group

Co-Chairs
Joanne Berg, Enrollment Management
Carla Raatz, Human Resources

Team
Dale Carruthers, Recreational Sports
Alan Fish, Facilities, Planning, Management
Ken Frazier, Libraries
Mark Guthier, Union
Ron Kraemer, DoIT/CIO Office
Howard Martin, Continuing Studies
Susan Riseling, UW Police

ExOfficio
Eden Inoway-Ronnie, Office of the Provost
Bill Richner, Office of the VC for Administration

Charter Team I – Populations, Affiliations and Service Entitlements (PASE) Policies

Coordinators
Karen Hanson, Office of the Registrar
Laura Ingram, Human Resources
Chris Holsman, DoIT

Team
Mairéad Martin, DoIT
Keith Hazelton, DoIT
Stefan Wahe, DoIT
Gary Declute, DoIT
DoIT Middleware Technologists

PASE User Interface Functional Group (no charter)
Pam Bauman, Human Resources
Monica Crawford, DoIT
Mark Foster, Library/DoIT
Karen Hanson, Office of the Registrar
Eden Inoway-Ronnie, Office of the Provost
Mitch Lundquist, Library
Mairéad Martin, DoIT
Brad Schwoerer, DoIT
Judith Strand, Division of Continuing Studies
Mary Quass, Division of Continuing Studies
Charter Team II - Net ID Assignment for New Hires

Coordinators
Pam Bauman, Human Resources
Mairéad Martin, DoIT

Team
Stefan Wahe, DoIT Security
Gary DeClute, DoIT Policy and Planning
Emuye Asfaw, Human Resources
Diane Caucutt, Employee Compensation and Benefit Services
Alice Gustafson, Housing
Marcia Jezwinski, Human Resources
Mike Mojerus, Human Resources
Kathleen O’Rourke-Benjamin, Employee Compensation and Benefit Services
Kay Schoenherr, Medical School Deans’ Office Human Resources
MST Technologist, DoIT
DoIT Architect

Support Staff
Darlene Retallick, Human Resources

Charter Team III – UDS Appropriate Use Policy

Coordinator
Mairéad Martin, DoIT

Team
Pam Bauman, Human Resources
Karen Hanson, Office of the Registrar
Karen Lutz, DoIT Security
Chuck Miller, DoIT Middleware
Julia Nelson, DoIT Security
Larry Schiebel, DoIT Middleware
Stefan Wahe, DoIT Security

Charter Team IV – Access to Data (A2D) Guidelines

Coordinators
Keith Hazelton, DoIT Architect
IMLG representative TBD

Team
Carol Block, DoIT
Bobby Burrow, Facilities, Planning and Management
Gary DeClute, DoIT
Doug Flee, DoIT
Karen Hanson, Office of the Registrar
Scott Manley, DoIT
Mairéad Martin, DoIT
Jim Phelps, DoIT Architect
Barb Vogel, DoIT

Other membership to include representatives from Academic Planning and Human Resources
Charter Team V – Identifying Next Steps Toward a Single ID Card and Clarifying the Credentialing Process

Coordinator
Ken Frazier, Libraries

Team
Pam Bauman, Human Resources
Joanne Berg, Enrollment Management
Karen Hanson, Office of the Registrar
Carla Raatz, Human Resources
Susan Riseling, UW Police
Jim Wysocky, Unions

Other team members to include representatives from FPM, Housing, Human Resources, DoIT, Health Services and Recreational Sports
In October 2004, the Information Technology Committee (ITC) — UW-Madison’s shared governance committee charged with advising the Provost on IT matters — confirmed the identification of the CIO Office as the data custodian for NetID issues and policies. At this time, the ITC also approved a new and inclusive process designed to provide the CIO Office with broad and deep input from the campus community. Please see the attached list of members of the NetID Policy Committee and ACT (the AuthNZ [Authentication and Authorization] Coordinating Team).

Ideally, the assignment of a NetID would offer a university “identity” — not services. With this goal in mind, the CIO Office has recently accepted the recommendations of the NetID Policy Committee and ACT concerning policies to support the assignment of NetIDs to a sponsored New Population. These recommendations include:

1. Individuals in the New Population should receive a NetID.
2. New Population individuals’ NetID should become their permanent NetID should they be granted permanent status.
3. In the case of New Population individuals who do not become permanent:
   a. Their NetID will remain active for a period of time agreed upon by the sponsor and the CIO Office;
   b. The NetID will be tied to the New Population individual even after deactivation, for a period of time agreed upon by the Sponsor and CIO Office;
   c. After deactivation, these NetIDs can be recycled after a period of time agreed upon by the Sponsor and CIO Office.

Note that these recommendations only apply to New Population individuals who do not currently have a permanent NetID.
Appendix III
UDS Appropriate Use Policy and Process for Accessing UDS Data

Appropriate Use of University Directory Service (UDS) Data Policy
The University of Wisconsin-Madison
July 7, 2005

The UDS provides applications and services at the University of Wisconsin-Madison with demographic, role and contact data to support identity management, authentication and authorization.8 The following guidelines are designed to ensure judicious and compliant use of that information, protecting the security and privacy of that data where necessary.

1. UDS data use must be authorized by the appropriate data custodians for student, employee or other data using the UDS authorization request form. This form specifies what data elements are needed for what purpose. UDS consumers9 will be notified annually to reapply for authorization. The data obtained must be used only for the specific purpose identified on the request form and not for any other purpose, and must not be supplied to other applications.

2. UDS data use must comply with the applicable State of Wisconsin and Federal laws and regulations concerning privacy and security as well as complying with University policy. UDS data use is specifically bound by the University FERPA Policy (http://registrar.wisc.edu/ferpa/faculty/) and University Appropriate Use Guidelines (http://www.doit.wisc.edu/security/policies/appropriate_use.asp).

3. UDS data may be used for purposes of providing identity management, which includes, for example, directory authentication and authorization services, and contact information.

4. UDS consumers must provide details on what UDS data they store locally.

5. UDS consumers must take all necessary precautions to secure UDS data in transmission and in storage. This includes utilizing security best practices as posted at http://www.doit.wisc.edu/security.

6. Consumers of UDS data will be held responsible for any security breach traceable to their use or specific authorization and will be held liable for any willful misuse or deliberate system damage traceable to their use and specific authorization.

7. Periodic and random audits will be performed on use of UDS data by DoIT Security.

8. Consumers of UDS data must provide access logs and access to systems containing UDS data upon request to DoIT Security.

---

8 Identity management refers to the policies, processes and technologies by which the identities of persons are proofed, registered and maintained. Authentication is the process of validating that identity. Authorization is providing access rights and privileges based on that identity.

9 UDS consumers refers to applications or services that use data from the UDS.
1. Person submits email for access to UDS data to udsrequests@doit.wisc.edu

2. Requests are reviewed Monday-Friday at 10:00am by the primary reviewer or the backup reviewer if the primary is not available. This email group automatically cc’s Mairead Martin.

3. A log of requests is maintained by Middleware. The reviewer performs a daily check of all requests whose status is not set to “CLOSED”.

4. The reviewer also looks at all “CLOSED” requests that are up for annual review. In this case the reviewer contacts the original requestor to confirm that the data access request is still valid.

5. The reviewer dates and sequentially numbers each request and sets the status to “RECEIVED”.

6. An acknowledgement email is sent to the requestor by 3:00 pm of the day the request is received.

7. The acknowledgement email includes the following: Request number, the Access to University Directory Service (UDS) Information form and the UDS Questions document.

8. The status is set to “FORM SENT”.

   Reviewer schedules a meeting with the requestor to go over and assists with the completion of the forms.

   The requestor is to return the form within 5 business days.

   The status is set to “FORM REVIEW SCHEDULED”.

9. Requestor sends completed form and UDS Questions document to udsrequests@doit.wisc.edu

10. Acknowledgement is send to the requestor stating that the forms have been received and a cost estimate will be sent within two business days. The status is set to “FORM RECEIVED”.

11. Reviewer discusses data access request with the UDS project manager and asks for cost estimate. The status is set to “REQUEST COST ESTIMATE”.

12. Reviewer forwards the cost estimate to the requestor. The status is set to “COST ESTIMATE SENT TO REQUESTOR”.

13. All material is forwarded to security for their review and signature. The status is set to “SECURITY REVIEW”.

14. Security forwards the request to the appropriate data custodian.

15. Data custodian reviews the request and forwards their decision to the reviewer.

16. The status is set to “DATA CUSTODIAN - APPROVED” or “DATA CUSTODIAN - DENIED”.

17. Approved request are sent to the UDS project manager. The status is set to “SENT TO PM”.

18. Project specification and time line is created and a revised cost estimate is sent to the requestor.

19. Requestor approves or rejects the cost estimate. If approved, the requestor provides with a PR number indicating where time is to be charged. The project manager provides the reviewer with an updated status. The status is set to either “REQUESTER - APPROVED” or “REQUESTER - DENIED”.

20. The project manager informs the reviewer when the project is completed. The status is set to “CLOSED”.