The Enterprise Authentication Implementation Roadmap

DRAFT August 2006
Open comment period closes October 1, 2006.
Send email to Ann West at awest at educause.edu with comments.

Several new business needs are pushing campuses to rethink their authentication and related identity management infrastructures to enable appropriate interoperability with sister institutions, the Federal Government, industry, and other partners. The Enterprise Authentication Implementation Roadmap describes a recommended approach that campuses can use in building enterprise authentication services in this new environment. It attempts to help campuses develop appropriate processes and architectures, whether you are implementing a small project with an authentication component or retooling your environment in preparation for joining a federation such as InCommon®. This Roadmap also discusses identity management and the relationship between associated concepts as well as specific technology, policy and management issues related to enterprise authentication.

Overview

Authentication (and Identity Management) require close collaboration of the business units, IT, service providers, and users. The security of a particular service or system is only as strong as its weakest link.

If an IT shop runs a great Kerberos authentication server, creates initial credentials for the new students, but doesn't know if the userids and passwords are distributed to the right people in the orientation process, the security of the service could be compromised.

If a service provider deploys an application that screen scrapes the central userid/password and stores it locally, the security of the service could be compromised.

If IT spends time and money deploying a highly secure authentication service for an application that poses little risk to the institution, at least some of the resources could have been better used elsewhere.

If a department deploys an application with its own authentication support and the usage grows enough that the deployer asks to add the service to the enterprise authentication system, campus authentication and thus the resources it protects could be compromised.

Setting overall priorities for the service, prioritizing where the dollars are to be spent, setting appropriate expectations and plans, and effective training and communication are all critical.

The Roadmap Contents

The Authentication Implementation Roadmap has been gleaned from the work and experiences of many campuses and offers the following aids to IT management:

- a model institutions can use to begin aligning their authentication systems to support the emerging trend towards federation in higher-education.
- an approach that encourages readers to consider the broader issues of risk related to operating in this new complex environment.

- a step-by-step process, case studies, and tools that readers can use to determine what should be changed on their campuses.
- a guide for generating the questions and determining the decision-points specific to a campus environment for authentication projects with either small, application-specific or large enterprise scopes.

The Roadmap **does not**:

- include detailed technical information about authentication methodologies
- replace a book on good IT project management approaches

You may review this roadmap with specific questions relating to password reset practices, technologies, and the like; or you may have a small or large scope for your authentication-related project. Whatever your interest, you are strongly encouraged to read through The Need for Change and Develop your Plan for Change sections and begin aligning your practices and infrastructure, even in a small way, to accommodate this new model.

Acknowledgements

This pdf version of the Enterprise Authentication Implementation Roadmap was developed as a convenience for those wanting to read the contents from a printed page. For a complete version of the Roadmap, visit the online version linked from www.nmi-edit.org.

The bulk of this work is derived from the MACE (Middleware Architecture Committee for Education), Internet2 and EDUCAUSE working groups and is the second in a series of Roadmaps providing guidance to higher education about implementing identity management. (See the Enterprise Directory Implementation Roadmap for information on deploying enterprise directories.) For a history of this Roadmap, see the Change Log (see Appendix A).

This document is a compendium of many individuals' experiences and knowledge. Many thanks are offered to Daniel Arrasjid, Tom Barton, Kathleen Barzee, Andrea Beesing, Jessica Bibbee, Mark Bruhn, Gary Chapman, Jacqueline Craig, Jim Dillon, Renee Frost, Scott Fullerton, Andrea Gregg, Keith Hazelton, Karl Heins, Paul Hill, Kevin McGowan, Margaret O'Donnell, Steve Olshansky, Barry Ribbeck, Jack Suess, David Walker, Steve Worona, and the Case Study authors, as well as Mike Stockwell from Cranking Graphics. All errors, misrepresentations, and confusions are solely owned by the persons responsible for the compilation and editing.

NSF Middleware Initiative draft-internet2-mace-authentication-implementation-roadmap-03.html August 2006	Editors: Steven Carmody, Brown University Ann West, EDUCAUSE/Internet2/ Michigan Technological University

This material is based in whole or in part on work supported by the National Science Foundation under the NSF Middleware Initiative - Grant No. OCI-0330626. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).
Comments to: awest at educause.edu

Table of Contents

Executive Summary

Several new business needs are pushing campuses to rethink their authentication and related identity management infrastructures. These include: increasing legislation addressing identity protection and accompanying negative publicity associated with an identity "spill" or breach; the need to provide login credentials to non-traditional groups of users, such as student applicants, alumni, contractors, and friends of the library, and related concerns about how the recipients are managing these credentials and/or when to revoke them; and the work being done by the Federal government to streamline access to their applications that will require participating institutions to meet minimum operational, process, and policy requirements.

Taken together, accommodating these drivers requires:

1. Changing existing common practice to accommodate these trends and migrate toward a model that is more consistent with an evolving federated world.
2. Adopting an IT governance approach that centralizes policy and management responsibilities for authentication and other identity services that underlie campus-wide and high-security services.
3. Understanding of the need for broad ownership of authentication-related business processes.

This approach does not preclude organizational units from managing independent services for specific portions of the community.

Develop Your Plan for Change

The first step to develop a high-level plan to help you move forward by identifying functions, process, policies, and technologies you need to implement to address your specific institution's drivers. Having this plan in hand allows you to address the identified gaps as the opportunity arises, such as coupling a new Web Single Sign-on service with an upgraded portal or establishing a higher level of assurance for higher-risk applications when implementing a new finance system.

To develop the plan:

1. Define your challenge for change, including drivers to help determine where you need to go.
2. Understand your organizations service requirements and accompanying framework to manage authentication on your campus.
3. Develop a set of guiding principles that can be used to guide decision making.
4. Inventory how your campus operates today.
5. Analyze your target online services, who is using them, and what the risk issues are, and develop a list of technical architecture, business process, and policy gaps that need to be addressed to achieve 1 and 2 above.

Implement Change

This section provides a process you can use when working with the constituencies across campus to ensure your policy, business process, and technologies are all in sync with each other. It is important to work on these concurrently to achieve the right balance, since they are so interdependent.

- **Policy** - Since the authentication service is so tightly bound to identity and access management, you should use your IT governance structure to develop the policy framework for the authentication project and incorporate it into your overall identity management and security policy framework. This should address identification, electronic credentials, registration, and service provider requirements.
- **Business Processes** - Key to business process change is the education of all the affected parties and an on-going review channel for reporting issues and problems with the new procedures. Managers and policy makers need to understand the basics of authentication technology and implementation decision points, and this process also ensures that a variety of viewpoints and sufficient data inform the decisions about authentication. Similar to the policy aspect, the business process effort should consider identification and registration, electronic credentials, account management, support, security and compliance, and staff training. The Federal E-Authentication Initiative's Password Credential Assessment Profile provides overall guidance on the operations, processes, and structures needed to adequately support your authentication system and related identity-management infrastructures.
- **Technology** - A critical goal of the design or architecture of your infrastructure is ensuring that it supports the business and policy requirements to a sufficient degree. If unacceptable gaps exist, the technology leaders must work with their policy and process colleagues to achieve consensus on how to proceed to address the gaps. The first steps are to identify existing constraints, map the business requirements to technology requirements, and finally decide on mechanisms and products. The last step in this stage of the process is to perform the initial system integration in a test environment and test the processes and technology infrastructure.

Migrate to Production

To migrate the new infrastructure to production, pick a staging strategy, which might include selecting relatively low-impact or low-risk services for initial integration in order to prove the functionality and, gradually, the scalability of the new system. Also consider integrating one or two on-campus systems with business owners who are strong partners with whom you can work through political and technical issues early on.

Lastly, the campus authentication requirements will very likely evolve as new end-user groups are identified, and new technologies and services become available. As a result, decide how best to migrate the project governance team to an on-going function. The creation of a new or enhancement of an existing forum where these new issues can be brought to the attention of stakeholders for the ongoing maintenance of the authentication system is critical to the integrity of the integrated service and preserving the risk tolerance level of the institution.

Have a Nice Trip

As with many journeys, the road traveled becomes almost as important as arriving at the destination. The authentication landscape is a dynamic environment. It's time to review and adjust your institution's Roadmap again to determine next steps in your authentication service. Over time there will be new emerging needs and technologies to consider, and you may have to make adjustments with your governance team on the order or priority of items in your Roadmap as you progress.

1. Concepts/Terms

General understanding of the function of authentication, its use, and related concepts are assumed. For readers unfamiliar with these, we recommend referring to the Johns Hopkins University Enterprise Services Glossary.

Key concepts and terms referred to throughout the Roadmap are included below. Many of them have broader meanings and implications but, in the interest of simplicity, are provided with more specific, authentication-related definitions:

Authentication is the process of validating the credentials presented in a particular security context. Proper authentication requires that the identification and registration processes that precede it are not compromised. Authentication should not imply access to resources, which is done with the Authorization step.

Authorization is the process of controlling, based on business rules, an individual's access to resources.

Credential is an object that is verified when presented to the verifier in an authentication transaction. [*OMB M-04-04 E-Authentication Guidance for Federal Agencies*]. Examples include network identifiers (netids), campus unique identifiers, and digital certificates.

Credentialing. See Registration.

Identification is the process by which information about a person is gathered and used to provide some level of assurance that the person is who they claim to be. Generally, this identity verification takes place within the office (e.g. Human Resources or Student Services) that first encounters the individual and creates their record within the institutional system(s) of record. The next step is Registration (see below).

Identity Management is an integrated system of business processes, policies, and technologies that enable organizations to facilitate and control their users' access to online applications and resources — while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access, rights, access restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems.

Identity Proofing. See Identity Vetting.

Identity Vetting is the process used to establish the identity of the individual to whom the credential was issued .[*OMB M-04-04 E-Authentication Guidance for Federal Agencies*] This is typically done at the Registration stage.

Level of Assurance (LoA) describes the degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as:

- the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and
- the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. [Ibid.]

A variety of application factors are examined to determine the minimum strength of the credential provided to an application. This determination is made through a risk assessment of each type of transaction that the application supports, identifying each risk and the likelihood of its occurrence, including:

- identity proofing,
- issuing credentials,
- using the credential in a well-managed and secure application, and
- record keeping and auditing.

As the point in the process with the lowest assurance level can compromise the assurance level of all other steps, each one should be as strong and robust as the others in the process.

Multi-factor Authentication requires the use of two or more approaches from something you know, have, or are. Examples include using a password to unlock a digital certificate store. Typically, multi-factor authentication is associated with a more rigorous vetting process, providing a higher LoA, and therefore a higher security level for more sensitive services or systems.

Registration (*credentialing*) is the process whereby users are given electronic credentials, leveraging the identification process above to ensure that they are coupled with the correct electronic identity information. For example, many campuses use a web-based mechanism to reset an initial password and establish a permanent one, ensuring a correct mapping by requiring the user to enter additional information validated against that which is contained in their record. It is important for institutions to establish rules that govern the processes used by the department or office that assigns and distributes credentials.

Risk-level Assessment is a management technique used to determine the level of exposure associated with unauthorized use of a resource. In the security area, risk-level assessments have a broader use associated with relative priorities and mitigation plans for protecting an institution's information assets.

Single Sign-on Authentication, or SSO, allows users to login once and gain access to multiple applications for a defined time period without having to re-login each time: subsequent authentication takes place without further user interaction or interruption. SSO is most often used to refer to "Web Single Sign-on," however it can also be implemented outside the web with PKI (client certificates) and Kerberos/Active Directory.

2. The Need for Change

Today, additional internal and external factors have created new requirements that are forcing broader campus involvement in discussions of authentication-related policies and procedures.

- **Regulatory Legislation** - In recent years, press coverage of identity theft problems have prompted U.S. Congress and state legislatures to tighten operating requirements for organizations whose computing systems hold personal information. This growing body of legislation and regulation has created increased audit and compliance requirements for many campuses, particularly in the area of security management, such as the California SB 1386 law requiring the reporting of security lapses for certain information. (Refer to the EDUCAUSE Federal Policy page for an overview of existing and pending legislation) The regulatory landscape has also evolved substantially in the areas of financial management practices and management of health-related data. Because of all these increased compliance requirements, campus technologies, and business processes related to identity management, credential distribution, authentication, and management of access control policies are now becoming subjects for auditors – and current processes may not be adequate to meet the new audit criteria.
- **Public Pressure** - The increasing publicity of incidents where personal information has been stolen from commercial entities, or where these entities have "lost" data, have served to heighten public awareness of the risks posed when databases are used to hold large amounts of personal information. Some of these publicized incidents have occurred on higher-education campuses, and have generated significant negative publicity for the institution involved. Often these incidents of unauthorized access are associated with data stored on non-centrally-managed systems on campus, or even on desktop or portable computers. Such incidents are now portrayed in the press as "privacy spills" — an incident where personal information that the institution was ostensibly safeguarding was viewed and retained by one or more unauthorized individuals. For many institutions, even if no laws were broken, the negative publicity may be a significant concern, as the institution may be portrayed as insensitive to personal privacy concerns. Check the Identity Theft Resource Center for information on the 2005 Disclosures of U.S. Data Incidents. Education institutions contributed 73 disclosures or 48% of the total 152 reported incidents. For an excellent discussion of institutional liabilities in this area, see Shakespeare On Cyberliability by Beth Cate, Associate University Counsel for Indiana University.
- **New User Communities** - Campuses are now routinely providing login credentials to non-traditional groups of users, such as student applicants, alumni, contractors, and friends of the library. Because it is common that many users are not required to receive their credentials in person, it may not always be clear who is actually receiving and using these credentials or when to revoke them. For many applications (such as accessing an events calendar), weak identification may not be an issue, but there are central and departmental applications (such as donating money or accessing a site with sensitive research data) where this is a significant concern.
- **Distributed Non-ERP Services** - Over the past several years, the risk level has also been increased by the growth of business departments managing distributed, independent data

centers to support applications beyond Enterprise Resources Planning systems (ERPs). These applications have authentication and authorization security requirements ranging from very low to moderately high, and although they don't operate at the enterprise (or campus-wide) level, many of them contain data that require strong safeguards or interfacing with enterprise systems. Ensuring a consistent level of assurance across all these applications may become a problem.

- **Service Management and User Experience** - Similar to the distributed services above, more and more processes and services are being automated or moved to an electronic self-service model, so the end-user interaction is now online twenty-four hours a day instead face-to-face during office hours. How can we mange the access to all these applications separately in a reliable fashion? How can the end user manage all the credentials involved? Scalability, reliability, and the end-user experience are important considerations, both from a strategic, cost effective, and "customer" service points of view.
- **The Federal E-Authentication Initiative** - This initiative promises a common infrastructure for electronically authenticating the identity of users of E-Government services offered by a broad range of Federal agencies. This infrastructure links institutions as identity suppliers (termed Credential Service Providers or CSPs) and the government agency as identity consumers (termed Agency Applications or AAs). Applications as diverse as NSF's grant submission tool FastLane and the Department of Education's Free Application for Federal Student Aid (FAFSA) will be available through this infrastructure, thus ensuring that all segments of the institutional community will have a strong motivation to participate in the E-Authentication Initiative. However, before campus users can access these applications, the Federal government will require participating institutions to meet minimum operational, process, and policy requirements. As more applications become supported by this initiative, IT shops will receive more and more pressure to ensure access for their campus communities.

These sample drivers for change are pushing institutions as a whole to re-examine what they are doing with respect to authentication and its related identity management processes.

2.1. The Change Itself

Taken together, accommodating these drivers requires the

1. Changing of existing common practice to accommodate these trends and migrate toward a model that is more consistent with an evolving federated world.
2. Adopting an IT governance approach that centralizes policy and management responsibilities for authentication and other identity services that underlie campus-wide and high LoA services.
3. Understanding of the need for broad ownership of authentication-related business processes.

This approach does not preclude organizational units from managing independent services for specific portions of the community.

You might have a campus-wide or more modest scope in mind for your authentication project. Whatever the focus, we encourage you to read this section: even internal IT projects can begin to the lay the groundwork for this approach.

What Are the Critical Components?

- **Thoughtful Consolidation**. Longer term trends point towards increased centralization of authentication as the most capable, cost effective, and risk-adverse solution. Note that centralization is a continuum:
    - differentiated approaches for services managed at department levels may be particularly attractive when an institution maintains different levels of assurance (LoAs) for specific campus populations or for specific types of services, such as accommodating the increased requirements of a health care center.
    - federating technologies can also provide sites with the ability to meet many of their goals without requiring a complete centralization of identity management and authentication. However, introducing unnecessary internal federations can require substantial resources to integrate a large number of applications and limit an organization's choice of applications due to the current lack of federation support by the commercial software sector.
- **Policy and Process**. Any institution-wide approach to authentication services and identity management must include policies and processes consistent with the community's needs and values. Policy states the “what” or “why”; it articulates the long-term institutional position, identifies mandates, scope, roles and responsibilities and requires a shared vision of the:
    - legal and regulatory landscape.
    - business drivers of the institution.
    - values and ethics of the institution, as they apply to the online services that the institution intends to offer.

  Business process is the "how" and can refer to, for example, the way a physical person is verified that he or she is truly represented by the electronic person recorded in the Human Resources system or to internal IT processes of how to support the infrastructure (security procedures, for example).
- **Governance and Stakeholder Involvement**. Planning and policy development can be done using a broad committee structure or, in a smaller stakeholder community, by having lunch with key people. Educating the campus stakeholders takes a lot of effort, and yet can save time and reduce risk in the future when important and critical decisions need to be made. The method is up to you to consider, but the goal is the same. An ongoing managed function:
    - enables effective, transparent, and accountable process and policy development, including decisions on issues of value, risk, related processes, implementation implications, and subsequent tradeoffs.

- comprises an educated forum of technologists, functional leaders, and policy makers.
- recognizes the role of IT as fundamental to the success of the academic institution.
- articulates the guiding principles for the information technology enterprise.

- **Technology**. In general, because of the variability of institutional goals, drivers, skill sets, and resources across the community, there isn't one technology that addresses all needs of all institutions. Therefore, this Authentication Roadmap does not attempt to make a definitive statement about which technology (or technologies) to adopt.

3. Develop your Plan for Change

Now that you understand the reasons for change and the change itself, the next step in this process is to develop a high-level plan to help you move forward by identifying functions, process, policies, and technologies that you need to implement in order to address your institution's drivers.

Having this chart (or Roadmap, as described below) in hand allows you to address the identified gaps as the opportunity arises, such as coupling a new Web ISO service with an upgraded portal or establishing a higher LoA for higher-risk applications when implementing a new finance system.

Authentication Service Requirements

At the end of this Develop your Plan for Change section, you should have a good understanding of your organization's authentication service requirements, including:

1. A definition of your challenge for change, including drivers to help determine where you need to go and an understanding of your organizations service requirements and accompanying framework to manage authentication on your campus.
2. A set of guiding principles that can be used to guide decision making.
3. An inventory of how your campus operates today.
4. An analysis of your online services, who is using them, and what the risk issues are, as well as a list of technical architecture, business process, and policy gaps that need to be addressed to achieve 1 and 2.

You will use this information to decide the first implementation step of your overall plan, a process as described in Implement Change.

Developing a Roadmap for Your Institution

A useful way to think about the result of this high-level planning activity is to develop a rough implementation sequence (or Roadmap) of the identified technology functions, processes, and policies. This is described in Develop your Direction.

3.1. Define the Problem

The first step in developing your high-level plan for change is defining the problem and articulating a definition of your challenge for change, including drivers to help determine where you need to go. This process is typically very short-term (a few days to a few weeks) and

- lays out a description of the issues or vignettes describing current problems, potential benefits, and desired functionality, and
- garners stakeholder commitment to move forward with a more detailed project study.

You should be able to succinctly articulate the problem definition by the end of this step, otherwise the project will be much more difficult.

Who Should Be Involved?

Once an authentication problem definition is agreed upon, the next stage is to determine who will write the guiding principles, perform the inventory, and develop the high-level direction. You will need to gather broad input for

- determining the economic costs and benefits of the alternative approaches,
- ensuring the solutions are feasible,
- increasing the likelihood of buy-in to the final plan, and
- changing established business processes as gaps become identified.

Consider including the following roles in your discussions:

- Data stewards - Human Resources, Registrars, Finance, Library
- Policy stewards - Provost, COO, EVP
- Process stewards - CFO/COO and related business offices
- Application and service stewards - alumni, registrars, admissions, financial aid office, distributed developers (if any)
- Infrastructure stewards - IT, facilities (building access)
- Users - faculty, students, staff, friends

At smaller schools, this planning step may be accomplished by one or two people who spend time talking to key stakeholders. For a case study of how a large institution addressed participation in a similar campus-wide project, refer to the Enterprise Directory Implementation Roadmap section on project structure.

The group assembled for this planning stage may also become the core group for the implementation stage. It all depends on the scope of your project and institutional environment.

3.2. Define the Guiding Principles

Once you have your problem definition in hand and know who should be involved in the planning stages, the next step is to work with them to define a set of guiding principles or working assumptions for the authentication service to help people make decisions, understand the environment, and determine relative priorities.

A set of principles is typically written from a high-level perspective and with very few details. The intent is that they should apply for many years to come and are intended to guide policy development and enterprise and departmental application deployments and reflect the needs of major groups across campus. They may also highlight aspects of your more encompassing identity management assumptions.

Case Study (PDF) – Paul Hill provides information on MIT's guiding principles.

Example Guiding Principles for Authentication

Below are a few example guiding principles to get you started:

- Centralized authentication is preferred over distributed authentication.
- Authentication-related policies will be based on the following existing policies or existing policy framework at our institution: [you can indicate those here].
- In the interest of optimizing security, information confidentiality, and preservation of individual privacy, a minimum necessary standard will be observed with respect to the collection, handling, and use of identity information.
- Applications or systems purchased after January 2007 must be capable of utilizing the campus authentication service natively.
- The network should be considered public and unprotected.
    - An attacker has the ability to attach a machine to the network and monitor traffic.
    - The burden of securing an application or service is shared among the developers, contractors, system administrators, and the department that provides the basic network infrastructure.

3.3. Inventory your Campus

Now that you have a set of guiding principles in hand, you should now develop an inventory of information about the current policies, processes, and technology practices and requirements, both on campus and in the wider higher-education community. The questions encompass identity management issues relating to authentication and are intended to frame your future discussions and raise awareness of existing issues. Recommended areas for your inventory include:

- **Policy Framework** - This section helps you to understand the broad policy landscape (or the currently stated "what" and "why") on your campus, navigate the policy-making process (or advocate the establishment of one), and identify the gaps and possible approaches when the time comes.
- **Current Approaches** - This section provides guidance for taking a snapshot of how policy is implemented, including the architecture and related processes, such as identity vetting and credentialing. Information gleaned in this section will illuminate what LoA your credentials have at present.
- **Context** - This section offers a set of issues to review to determine what drivers and context information can help guide your planning. It includes a more detailed inventory of drivers and feedback about the services and constituents of the future.

Policy Framework

- **Policy Frameworks** - Do you have institutional, information technology, identity, or security policy frameworks that already contain authentication- related policies, or into which, newly developed policies can fit?
- **Principles and Policies** - What broad governing principles or policies do you currently have which may relate to managing authentication and access to electronic resources in

general, e.g., policies on responsible or acceptable use, computer account eligibility, change management, log review, and audit?

- **Existing Authentication Policies** - What specific policies, guidelines, or other documentation does your organization have on authentication-related elements, such as identity proofing, identifier assignment, account eligibility, password, or other credential issuance and re-issuance?
- **Governance** - What is your policy governance approach, e.g., with respect to policy development, review, approval, and interpretation?
- **Audit and Regulations** - Do you perceive current, or future, audit and regulatory requirements that may affect the approach you take to managing access to electronic resources?

Current Approaches

- **Degree of Centralization** - Is all of your authentication currently being performed on a per-application or per-system basis, or are integrating or centralized approaches (e.g., LDAP, Kerberos, Single Sign-On) in use, and if so to what extent?
- **Identifiers** - How do you assign identifiers (usernames) to members of your community? How early in the admissions or hiring process are identifiers assigned? Do you have a unified institutional approach to identifier assignment, or are their many identifiers assigned to individuals by different authorities?
- **Credentials** - How do you assign passwords or other credentials to members of your community? Do you have a self-service capability in place for initial password setting and for password re-set? Do you use any authentication techniques or credentials other than username/password? What evidence of identity do you require to be presented by users in order for credentials to be issued? Are your passwords sufficiently protected in transit by the use of encryption?
- **Authentication Level** - Do you categorize different applications, services, or communities as requiring different levels or types of authentication?
- **Management** - Organizationally, who is responsible for the management of any shared or centralized authentication services? Do you have the internal resources and expertise to evolve your authentication approach if you so choose? How do you tend to balance the authentication mechanisms of commercial, open-source, and internally developed solutions?
- **Issues** - What problems do you perceive with your current authentication approaches? What are your architectural or technical requirements (see Appendix B)?

Context

- **Peers** - What are your peer institutions doing with respect to managing authentication and other identity management services? What can your organization learn from them to apply to your own environment?

- **Partners** - What external service partners do you have and how do you address access to resources you don't directly manage?
- **External Drivers** - To what extent do you perceive pressures for changes to your authentication approaches along the lines outlined above in the "Drivers for Change" section?
- **Leverage** - Do you have information technology projects now beginning or underway that you can leverage or coordinate with closely as you evolve your management of authentication?
- **Return on Investment** - What application or systems do you have which would most benefit from improvement in their use of authentication, either in the interest of enhancing security or improving end-user experience?
- **Communities** - To what groups of people beyond on-campus faculty, staff, and students do you provide services? Are additional groups being considered?

3.4. Develop your Direction

Having the information about your campus authentication service and future needs, you can now develop the detailed plan. In this stage, you will:

- Create a matrix of the populations of people you intend to serve (students, faculty, staff, contractors, alumni, etc.) and the services the stakeholders want to offer to them (email, library, learning management, online giving, and recruiting services, for example).
- Use this matrix to develop overall requirements for your processes and technology infrastructure by considering the risk, drivers, and related requirements.
- Compare these requirements with your inventory to determine the gaps and develop your own institutional or application Roadmap and target LoAs.

Create your Matrix

Depending on whether your project scope includes the entire authentication service or just authentication for a specific application, create a matrix of the populations of users that your campus intends to serve and the services the stakeholders want to offer to them. This will help you to analyze your risk factors and LoAs later. For example, offering a course to a distance education student who will never set foot on campus poses very different identity vetting implications than a student standing next to you, holding a state-issued drivers license. Having a strong identification and registration processes to achieve a high LoA is far more difficult in the first case than the second.

Different than the inventory which included information gleaned at a management level, this matrix helps you understand the specific implementation issues. To get a rough idea of how you can proceed, review two worksheet examples in the linked spreadsheet:

- Example 1: Web-based Self-service Password Change Application (XLS).
- Example 2: Web-based Banner Financial Application (XLS).

Use either one of the applications included in this spreadsheet as an example to walk through this part of developing your direction. At this point, for a chosen application determine:

1. Broad populations in columns A, B, and C.
2. Their current LoA in column D as defined by the E-Authentication levels on page 7 of the Password Credential Assessment Profile for levels 1 and 2. (If you're using PKI, check out page 2 of the Certificate Credential Assessment Profile for levels 3 and 4 as well)

This step can be as detailed or high-level as needed.

Consider Risk and Assign LoA

With your population and inventory data in hand, you should now work on determining the risk level for the applications and using that to develop the LoA for the credentials.

1. Read and use the approach outlined in Section 2 of the Federal E-Authentication Guidance for Federal Agencies for relatively lightweight risk assessment for applications. In this part of the process, you are taking the role as a service provider and determining the relative value of the information resource.
2. Using the information from step 1, indicate the access (or application function in the spreadsheet) that each role would have and add that to column E. The spreadsheet uses the common CRUD (Create, Read, Update, and Delete) data manipulation functions to help classify the access rights.
3. Determine the Application Risk Assessment Value (either high, medium or low in the case of the spreadsheet examples) and the corresponding minimum LoA of the credential required to access the application. Insert these two values to column F and G respectively. Refer to E-Authentication Guidance for Federal Agencies for information on mapping application risk level to required credential LoA.
4. Column H then compares the required minimum LoA (from column G) with your current campus LoA by role (in column D) and determines whether you have a LoA gap. If you do, you may need to beef up the technology or processes to get the specific credentials up to the required LoA level.

For a more detailed risk assessment refer to the Electronic Risk and Requirements Assessment. It is a database-driven tool available from the Federal E-Authentication Initiative and helps you assess your institution's applications and related authentication risks. EDUCAUSE/Internet2 Computer and Network Security Task Force has a Risk Assessment Framework that may be of help as well.

Don't worry if you end up with more than one LoA for all your applications. More and more campuses are finding that they need more than one to ensure that the security rigor is appropriate for the wide range of applications they support.

Case Study (PDF) – University of Maryland, Baltimore County

Jack Suess discusses Levels of Assurance at the University of Maryland-Baltimore County.

Determine Gaps

You can now use your application's required LoA and accompanying credential strength requirements to determine what you need to do to address the gaps you may have identified in step 4 above.

- To help you with this, the NIST Publication 800-63 Electronic Authentication Guideline discusses the specific components that affect LoA, how they differ across the levels, and what you need to implement to achieve each of the four Federal LoA levels. Levels 1 and 2 are password-based and 3 and 4 are PKI-based levels. For a summary of the requirements, refer to the Credential Assessment Suite:
- For levels 1 and 2 refer to the Password Credential Assessment Profile. Most campuses will start by working towards level 1, which includes guidance for assessing organizational maturity, authentication protocol, token strength, and status management. See page 7 of the Profile for a summary of requirements.
- For levels 3 and 4 refer to the Certificate Credential Assessment Profile. These are appropriate for higher-level security requirements.
- For a tool to help determine the password (and certificate) practices for all four levels, refer to the Entropy Spreadsheet.

Note: The E-Authentication Initiative provides an excellent body of work to help schools determine appropriate approaches, but keep in mind that this effort it is still evolving. Campuses should track the Initiative's progress to ensure compliance once they decide to leverage their identity infrastructure to access Federal applications.

Case Study (DOC) – E-Authentication Credential Assessment for InCommon Federation Sampling of Three Universities

Three universities were assessed on assurance levels 1 and 2 using the E-Authentication Assessment Framework. The linked doc is the gap analysis of those assessments done.

Develop your Direction and Roadmap

One way to think about the result of this high-level planning activity is to develop a rough implementation sequence (or Roadmap) of the identified technology functions, processes, and policies. It can help to organize and communicate your plans for the authentication infrastructure and determine which of your upcoming projects you can leverage to make progress.

A Roadmap can also assist non-IT stakeholders to visualize the interplay of these components and the dependencies involved with the process of implementing any one of them. Take the gaps identified above and develop a rough implementation sequence. You can use this as your own institutional or applications Roadmap. For examples, see

- University of Wisconsin-Madison Roadmap - Graphical Example
- Cornell University - Written Example
- University of Texas System - Graphical Example (Click on *How do we get there?* and look for UT System Identity Management Roadmap.)

4. Implement Change

Now that you have your high-level plan (or your own Roadmap) in hand, the next step is to consider how to implement it in the larger institutional context.

The Implement Change section will provide a process you can use when working with the constituencies across campus to ensure your policies, business processes, and technologies are all in sync with each other. In addition, this section provides case studies of deployment approaches and how other campuses are managing this change.

From your own Roadmap, consider upcoming projects and choose the items that fit well. For example, if implementing a new finance system requiring different levels of access, use this application to discuss LoA and related business processes and technologies. With your chosen items in hand, read on about the interplay of policy, business process, and technology.

4.1. Policy, Business Process, and Technology

Even though the Implement Change section discusses the development of the policies, business processes and technologies separately, it is important to work on them concurrently to achieve the right balance, since they are so interdependent. As a reminder:

- **Policy** is the statement of an organization's intent or decision on an issue. It describes the "what" or "why." This can be done at a high-level such as determining who may receive credentials and what the user can access with them. Components of a policy framework can be written and communicated in many different ways.
- **Business process** describes "how" to implement this intent. Using the credentials policy above, a related business process could entail working with the offices that first interact with particular constituents and determining how they should verify users' identities. In addition, the credentials must be generated and securely somehow distributed to the individuals. Later, if the institution would like to offer services to another group (contractors, local high-school seniors, etc.), the policy may need to be amended to include them and new business processes set up and technology changed accordingly.
- **Technology** also describes "how" to implement the intent and goes hand-in-hand with the business processes. Using the above example, the technologist implements the appropriate password practices and configures the appropriate system (s) to generate the credentials that will be distributed by the business offices. Users then log into an application or a network, using a well-designed technology architecture that meets the security requirements and can scale to accommodate the user groups identified in the policy statement.

Ensuring the security of an application relies on the appropriate implementation of an institution's values (policy) in the business policy, technology, and end-user realms. For an example of how these can be interdependent, see the discussion of Single Sign-on Considerations (see Appendix C).

Who Should Be Involved?

Refer to the Define the Problem section for the list of stakeholders to consider. You can have one team for each of the three areas with overlapping membership or one large group consider these issues.

Depending on your scope, you should have representatives from each area meet regularly to discuss the overlaps, gaps, and issues when the plans from the three teams are integrated. For example, it may be concluded that the technical team can't implement a technical enforcement method for a policy, and therefore a business process and related policy-enforcement methodologies must be changed.

Key to this part of the process is effective and on-going communication to keep everyone informed and reduce the surprises. Doing this builds trust into this part of the project and enhances the likelihood of arriving at the most appropriate solution.

The Importance of Communication and Education

Remember to include campus outreach efforts and training in your plans to educate and inform the user community about the goals and deliverables of the project and to prepare them for a change that will probably affect the way they interact with the institution's systems.

Managers and policy makers, in particular, need to understand the basics of the authentication service and its implications for their respective department. End users should understand their responsibilities, role, and importance in maintaining secure credentials, for instance. Education and awareness methods could be in the form of presentations from key stakeholders or project staff, informational web sites, online Q&A forums, blogs, or email mailing lists.

4.2. Develop Policy Framework

Since the authentication service is so tightly bound to identity and access management, you should use your IT governance structure to cast the policy framework for the authentication project and incorporate it into your overall identity management and security policy framework.

Specifically, authentication policy should include the following:

- **Identification** – What requirements will be imposed to ensure sufficient proof that the person is who they say they are? What credentials are required to confirm their employment, student status, or other affiliation relationship to the institution? If identity data is derived from existing directory or user account databases, how will legacy information be verified? What are the requirements to support the chosen LoAs?
- **Electronic credentials** – What rules determine the form of the credential? How will requirements or standards affecting this be identified? How will legacy architectures be able to make use of the electronic credential? What encryption standard will be required? What does the anticipated lifecycle of credentials look like? Can they be changed, retired or reused? What are the LoA requirements for the credentials?
- **Registration** – How is information about the individual obtained? Does it come from payroll or student databases? How are affiliates, such as applicants, alumni, and contractors added? How will electronic credential information be linked to information

about the individual? What relationships or dependencies are required for the enterprise directory, patron directories, or other similar services? Are appropriate protections in place to ensure the privacy of information about individuals? What are the LoA requirements for registration?

- **Service providers** – What requirements will be imposed on service providers to ensure the privacy of identity information whether on your premises or offsite? What standards are required to ensure protection of the credential during transmission? What level of assurance of the authentication credential is necessary for access to which service? Is multi-factor authentication required for some services?

Case Study (PDF) – University of Wisconsin-Madison

Steve Devoti and Mairéad Martin describe authentication at the University of Wisconsin-Madison. Of note is a recent password policy.

Case Study (PDF) – New York University

Gary Chapman describes the context for and provides New York University's approach to authentication and identity policy.

For further examples, see Cornell University's Authentication of Information Technologies Resources Interim Policy, the SANS Security Policy Project, or Rodney Petersen's A Framework for IT Policy Development, EDUCAUSE Review, March/April 2004 for examples. For additional institutional examples, visit the Association of College and University Policy Administrators (ACUPA).

Policy Development Tips

Below are a few policy development tips:

- Identify the short term, interim policies that you can develop and implement while the longer-term versions are being developed. You can publish them as interim and include a link to the draft permanent versions. This helps to ensure that critical issues, whether technological or process-based, are addressed as early as possible as the project proceeds. Examples include the Guiding Principles you developed earlier and Cornell's Authentication of Information Technology Resources Interim Policy above.
- Ensure that the technical- and process-oriented individuals are passing along the policy issues they discover in their work and that a feedback loop is established. For example, as a password reset mechanism is being being developed, a typical question includes "how many secrets should we require users to establish to reset their password"? The answer to this question relates back to the identified requirements, LoA, and identity proofing and may be in effect more of an interpretation of policy than a technical question.
- If you don't have one, start laying the groundwork to establish a governance structure and assemble an ongoing oversight/management group to help guide policy development in the future. You may be able to ask those involved at these initial stages to serve a bit

longer to get a process up and running and provide continuity. For information on starting a formal governance structure, visit the IT Governance Institute.

- E-Authentication Initiative's Password Credential Assessment Profile provides overall guidance on the operations, processes, and structures needed to adequately support your authentication system and related identity-management infrastructures. If you intend to have your constituencies use electronic services provided by the Federal Government, it would be prudent to be consistent with these processes and practices as you develop your policy framework as outlined in the Drivers for Change section.

4.3. Develop Business Processes

In conjunction with the policy and technology development, the business process work must support the policies that govern your authentication service. Key to successful and efficient business process change is the education of all the affected parties and an ongoing review channel for reporting issues and problems with the new procedures. Managers and policy makers need to understand the basics of authentication technology and implementation decision points, and this process also ensures that a variety of viewpoints and sufficient data inform the decisions about authentication.

Specific Processes to Consider

Below are the specific processes and requirements relating to the identification, credentialing and re-credentialing, as well as account management processes that you should have in place:

- **Identification and registration** includes on- and off-campus identity vetting and other processes that may have to be considered if parts of the population cannot comply with vetting policies, such as exception procedures for dealing with constituencies who need access, but fall outside the identified local populations (e.g., "guests" or remote users).
- **Electronic credentials** includes creation of self-service or other password change mechanisms; password-reset exception processes; and procedures involving password sharing or compromise. Use the NIST Password Entropy tool to determine policy and LoA compliance.
- **Account management** includes provisioning and de-provisioning accounts, how these are done and when, and status and affiliation change management.
- **Support** includes help desk and related support personnel's responsibilities. Matt Smith from the University of Connecticut did an informal survey on help desk and password reset issues.
- **Security and compliance** includes auditing and process debugging and security monitoring and compliance. Refer to Log Management for the University of California: Issues and Recommendations for an example of some of the issues associated with security and compliance.
- **Staff training** includes educating staff about new processes and responsibilities and changes in those already existing.

Below are additional points which you should consider, but are not necessarily germane to an initial implementation:

- **Alternative plans and procedures** when normal operations cannot be followed, such as when the system is not working properly or is functioning at an alternate location during a disaster or abnormal conditions.
- **Flexibility to allow a variety of services to leverage the authentication system**, without compromising the intent of the policies and intent. Also consider any processes that need to be ADA compliant.
- **Identification and documentation of how changes are made** in a longer-term, shorter-term, and emergency contexts.

Remember, your processes must be documented and auditable This is critical if your institution decides to leverage the authentication (and identity management) infrastructure to use an external on-line service or participate in external partnerships. A central document repository is useful for both review of the service provider to establish trust and for auditing to verify it.

Using the Password Credential Assessment Profile

The next step is to consider the expected information flow for creation, provisioning, and de-provisioning of user credentials for the communities you identified in the Develop the Plan section. (You may or may not have done this in your gap analysis.)

The E-Authentication Initiative's Password Credential Assessment Profile provides overall guidance on the operations, processes, and structures needed to adequately support your authentication system and related identity-management infrastructures.

Assurance Level 1 outlined on page 8 lists requirements for proving formal incorporation of the organization, managing and transmitting authentication credentials, and maintaining a record of their status and ensuring their timely revocation when appropriate.

While reviewing Assurance Level 1 is important, it is recommended that those working on the business processes go on to review Assurance Level 2 and, in particular, the Organization Maturity, Registration and Identity Proofing, and Delivery Confirmation sections. These offer guidance regarding specific processes to address and implement on your campus.

Case Study (PDF) – University of California Password Resets

Karl Heins, the UC Director of Information Technology Audit Services, explains why mandatory password changes may not be effective.

Case Study (PDF) – Penn State's Password Practices

Renee Shuey provides an overview of Penn State's password practices.

Case Study (PDF) – Rice University

Barry Ribbeck discusses authentication at Rice University with an emphasis on their password practices and levels of assurance.

4.4. Develop Technology Infrastructure

A critical part of the design or architecture of your infrastructure is ensuring that it supports the business and policy requirements to a sufficient degree. If unacceptable gaps exist, the technology leads must work with the policy and process colleagues to achieve consensus on how to proceed. For example, the authentication technology requirements of a library providing access to resources for all state residents will tend to be very different from the authentication requirements necessary to secure an organization's payroll and accounts payable operations.

At this stage, there are several basics tasks to be completed. (A more complete description of each of these tasks can be found in the design phase of the Enterprise Directory Implementation Roadmap).

Case Study (PDF) —Tom Barton from the University of Chicago discusses their authentication architecture.

The central authentication service will most likely consist of or be dependent on a set of central services, such as:

- LDAP directory,
- central web sign-on service,
- password activation and re-set site, and/or
- person registry tracking affiliation status of community members.

These in turn will be used by the applications integrated in the course of the overall project.

Assemble Existing Constraints and Map Business Requirements to Technology Requirements

In addition to identifying the components required, whether existing or new, consider any technology and staffing or organizational constraints and determine what you can and can't easily change. At this point, it's best to understand the spectrum of the business requirements and how they impact your available authentication (and identity management) technology choices before you wade off into making specific product decisions. Consider walking through the following issues:

- **Applications** - Determine what authentication mechanisms/protocols are supported by your target applications and environments (such as network operating system, if that is one of the items.) Do they support multiple authentication technologies? What do your legacy applications require?
- **Authentication Service** - What does your existing authentication architecture support and how secure and flexible is it now? Are you passing credentials in the clear — if so, for which applications and what are the associated risks ? What are the operational and development issues? If you are considering implementing a web single sign-on system, which applications will be easy to connect in and which won't be? Identify the authentication service operational and management requirements, such as service uptimes.

- **Source Systems** - How often is the authentication system updated and from where? Is the information associated with all the identified populations available in the current source systems? Do the new requirements have time targets or constraints?
- **Credential Management** - Review existing credential strength, assignment and reassignment processes, as well as passing, management, and reset methods.
- **Identity and Account Management** - Review the types of identifiers, role and affiliation attributes, and where they are stored. Determine the range of accounts, such as guest, contractor etc. that were identified as supported users. Determine the creation, change, and deletion requirements for identity and subsequent account management. Are there constraints or changes to note? What are the time requirements for account creation and deletion? How will the service be provisioned and what is the anticipated frequency or requests? How will the credential be linked to the information in the identity management system?
- **Security Management** - Identify the security-related requirements and their impact on the architecture and current strategies. What is the LoA(s) to be supported? You should be able to map these to the technical requirements as listed in the NIST Electronic Authentication Guideline Special Publication 800-63. Are multiple authentication systems required because of the specific needs of your legacy systems and/or security? Will you be implementing a single sign-on or reduced sign-on system? How strong do your passwords need to be?
- **Personnel and Resources** - What are your existing staff skills? Does your staff have the expertise and time to support more than one authentication methodology? Will you require outside consultants, and if so, for what specific tasks? Can you solve an existing operations problem by consolidating services and thus free up sufficient staff time?

Decide on Mechanisms and Products

Given the technical requirements identified above, there are a number of vendor and open-source solutions to consider. At this stage, you are deciding on your protocols and products to support. Common mechanisms include:

- **Kerberos** - Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well (e.g., Microsoft's Active Directory).
- **LDAP Authentication** - Lightweight Directory Access protocol is used to communicate with directory servers and defines how a client can authenticate to the directory server. Many web-based applications include a form where the user enters a userid and password; the application then attempts to "bind" to a local LDAP server with the user's credentials. The success or failure of the bind operation determines the success or failure of the user's authentication to the application. The basic implementation of this approach requires storing the user's password as an attribute of the user object, which is usually stored in a hashed form rather than plaintext. Plug-ins exist for several LDAP servers that can bypass password attribute search and instead attempt a login to an external service

(usually Kerberos). This plug-in approach allows sites to deploy applications that only support LDAP-style authentication and to still avoid storing user passwords in the LDAP directory.

- **Passwords over SSL/TLS** - Current expected practice (it's no longer merely best practice) is for web-based applications to create an SSL/TLS tunnel to the browser user whenever a user is asked to enter a password into a web form.
- **Public Key Infrastructure (PKI)** - PKI is based on the exchange of electronic credentials called certificates. With public key cryptography, institutions can provide the following:
    - highly reliable digital credentials supporting authentication and leading to scalable and flexible authorization;
    - strong encryption supporting data security in transit and storage;
    - true digital signatures supporting auditable transaction validation;
    - document integrity through the use of digital signature mechanisms.

For more information on these and other methodologies and common practices, refer to the further resources below.

- Check the EDUCAUSE Identity Management Working Group list for threads on this and other related topics.
- The IETF (Internet Engineering Task Force) is a standards organization responsible for many of the most widely used protocols on the Internet. The Security Area working groups have responsibility for Kerberos and many protocols related to public key technologies. Information about working groups in the security area is available here.
- The National Institute of Standards and Technology's Computer Security Division publishes a number of Practices, Checklists and Implementation Guides.
- The SANS (SysAdmin, Audit, Network, Security) Institute is a cooperative research and education organization. It maintains a large archive of relevant documents.
- Kerberos information
  MIT
  Microsoft
  IETF: RFC 1510
  KX.509 information - University of Michigan's distribution site for their Kerberos-to-PKI credential conversion software.
  PKINIT - University of Michigan's PKINIT site, the Kerberos Version 5 extension that provides for the use of public key cryptography.
- PKI Information
  Higher Education PKI Technical Activities Group (HEPKI-TAG)
  EDUCAUSE Identity Management Services Program

A Request for Information (RFI) from vendors of interest could be done at this stage for either a broader identity management package or authentication system. However, while purchasing an

integrated vendor solution will impact the technical work, it does not reduce the identity-related policy and business process work associated with the identification and credentialing functions.

Case Study (PDF) – University of California Riverside

Andrew Tristan explains the authentication approach at UC-Riverside.

Case Study (PDF) – Brandeis University

William Goedicke discusses Brandeis University's identifier practices.

Perform Initial System Integration(s) in the Test Environment

Consider any dependencies that have emerged, which must first be acquired or upgraded before another implementation step can occur. These may include:

- Hardware acquisition
- Software acquisition
- Service acquisition
- Internal software development or upgrade
- Technical staff training
- End-user, support staff, and staff training (help desk, users {self service})
- Scheduling of on-site vendor participation

Run the initial implementation as a limited non-production pilot long enough to fully exercise all initial system capabilities and uncover unexpected wrinkles. Do extensive scaling and load testing. Modify system configuration and documentation as necessary. Make sure logs and related analysis tools are useful and events can truly be parsed, tracked, and audited. And finally, review the utility of documentation and the handling of unusual cases such as de-provisioning those users who, through malfeasance, lose the privilege to access services.

4.5. Migrate to Production

After coming this far, these final steps describe how you move from the planning and implementation in test environments to going live with your changes and focuses on considering the order of the overall system integration, interdependencies, and migration to production.

Migrate to the New Infrastructure

To migrate to the new infrastructure, pick a staging strategy, which might include picking relatively low-impact or low-risk services for initial integration in order to prove the functionality and, gradually, the scalability of the new system. Also consider integrating one or two on-campus systems or business owners who are strong partners with whom you can work

through political and technical issues early on. Below are possible steps a campus could take at this stage:

- **Develop phased migration strategies** for moving from the existing infrastructure to the new one. This includes updating or creating the data feeds, code changes, linking in the applications, and deciding the phases of the migration. Schedule the process of "going live" carefully, accounting for time-of-year or other anticipated factors affecting demand on the systems and staff resources. Remember to develop contingency plans for backing out of the new system if things prove problematic.
- **Start working through your communications and education plan**; hold get-ready meetings with project members (including stakeholders, help desk, etc) as developed by the business process team above. Be sure you discuss expectations of those involved in the project as well as critical campus players so the project isn't over sold.
- **Migrate systems and users**

Create a Forum for Making Informed Decisions

Lastly, the campus authentication requirements will change as new end-user groups are identified, and new technologies and services become available. As a result, decide how to migrate the initial project governance team to an on-going function. The creation of a new or enhancement of an existing forum, where these new issues can be brought to the attention of stakeholders for the ongoing maintenance of the authentication system, is critical to the integrity of the integrated service and preserving the risk tolerance level of the institution. Issues referred to in this on-going group should include:

- Changes to the infrastructure that may be needed resulting from new regulations, new user communities added, or new or updated services.
- Major organizational changes that may disrupt established business processes.
- New technologies that become available that could enhance the business process and/or policy framework in place and introduce new resource requirements or changes to existing services.
- New services that are scheduled to be incorporated into the new infrastructure. What is the process for deciding what to integrate, in what order, and how?

Participants could include many of the same representatives who participated in the initial governance structure. In many cases, authentication is coupled with an identity management or overall IT governance body.

Have a Nice Trip

As with many journeys, the road traveled becomes almost as important as arriving at the destination. The authentication landscape is a dynamic environment. It is time to review and adjust your institution's Roadmap again to determine next steps in your authentication service. Over time there will be new emerging drivers to consider, and you may have to make adjustments with your governance team on the order or priority of items in your Roadmap, as you progress.

Finally, you should end this part of the journey with an overall plan, the finished implementation of the first stage of your plan, and a process for continuing through the next iterations. Congratulations and good luck!

5. Resources

Below is a list of references included in this Roadmap.

A Framework for IT Policy Development (PDF) written by Rodney Petersen in EDUCAUSE Review, March/April 2004.

Association of College and University Policy Administrators (ACUPA) provides further examples of institutional policy.

Authentication of Information Technologies Resources Interim Policy provides readers with a policy example, courtesy of Cornell University.

Case Studies

Brandeis University Case Study (PDF) William Goedicke highlights the University's identifier practices in the context of authentication.

MIT's Guiding Principles (PDF)is an example provided by Paul Hill of MIT's.

New York University's Policy (PDF) includes Gary Chapman's description of New York University's approach to authentication and identity policy.

Penn State's Password Practices Case Study (PDF) includes Renee Shuey's overview of Penn State's password practices.

University of California Password Resets Case Study (PDF) provided by Karl Heins, the UC Director of Information Technology Audit Services, explains why mandatory password changes may not be effective.

University of California Riverside Case Study (PDF) offered by Andrew Tristan explains the authentication approach at UC-Riverside.

University of Chicago's Authentication Architecture Case Study (PDF) included by Tom Barton discusses their authentication architecture.

University of Wisconsin-Madison Case Study (PDF) provided by Steve Devoti and Mairéad Martin describes authentication at the University of Wisconsin-Madison. Of note is a recent password policy.

EDUCAUSE Federal Policy offers an overview of existing and pending legislation.

EDUCAUSE Identity Management Working Group provides a resources site and email list covering identity management policy, process, and technology.

EDUCAUSE/Internet2 Computer and Network Security Task Force offers security-related resources to higher education.

Enterprise Directory Implementation Roadmap provides information for higher-education institutions interested in deploying enterprise directories.

Enterprise Services Glossary from Johns Hopkins provides a general technology-related glossary.

FastLane is an interactive real-time system used to conduct NSF business over the Internet.

Federal E-Authentication Initiative is working toward a common infrastructure for electronically authenticating the identity of users of E-Government services offered by a broad range of Federal agencies.

Credential Assessment for InCommon Federation Sampling of Three Universities (DOC) provides an example of how three universities fared on assessing their infrastructure and practices for assurance levels 1 and 2 using the E-Authentication Assessment Framework. The linked doc is the gap analysis of those assessments done.

Credential Assessment Suite from the Federal E-Authentication Initiative.

Electronic Risk and Requirements Assessment (MS Access) is a database-driven tool made available from the Federal E-Authentication Initiative for a more detailed risk assessment of applications.

Entropy Spreadsheet (XLS) helps you to determine your policy and LoA compliance.

Federal E-Authentication Guidance for Federal Agencies (PDF) provides a process for assessing risk of an application and assigning the requisite LoA for credentials.

NIST Publication 800-63 Electronic Authentication Guideline (PDF) discusses the specific components that affect LoA, how they differ across the levels, and what you need to implement to achieve each of the four Federal LoA levels.

Password Credential Assessment Profile (PDF) describes the LoA requirements E-Authentication levels 1 and 2.

Free Application for Federal Student Aid (FAFSA) is the online student Federal financial aid application.

Identity Theft Resource Center provides information on the disclosures of U.S. Data Incidents protection of privacy and approaches for mitigation of identity theft.

IETF links to The Internet Engineering Task Force web site.

Institutional Roadmaps

Cornell University (HTM)

University of Texas System (PDF)

University of Wisconsin-Madison Roadmap (PDF)

Kerberos Information

MIT provides the Massachusetts Institute of Technology's Kerberos distribution.

Microsoft

IETF: RFC 1510 via FTP

KX.509 information is the University of Michigan's distribute site of their Kerberos-to-PKI credential conversion software.

PKINIT is the University of Michigan's PKINIT site, the Kerberos Version 5 extension that provides for the use of public key cryptography.

Log Management for the University of California: Issues and Recommendations provides an example of issues associated with logging, security, and compliance.

National Institute of Standards and Technology's Computer Security Division

PKI Information

- Higher Education PKI Technical Activities Group (HEPKI-TAG)
- EDUCAUSE Identity Management Services Program

Resources/Help Desk and Passwords from Matt Smith from the University of Connecticut offers an informal survey on help desk and password reset issues.

Risk Assessment Framework (PDF or DOC) provides risk assessment guidance developed by the EDUCAUSE/Internet2 Computer and Network Security Task Force Risk Assessment Working Group.

SANS (SysAdmin, Audit, Network, Security) Institute

SANS Security Policy Project

Shakespeare On Cyberliability (PDF) provides an excellent discussion of institutional liabilities in cyberspace, written by Beth Cate, Associate University Counsel for Indiana University.

Appendix A: Change Log

[December 2004] Enterprise Authentication Implementation Framework Draft released.

[October 2005] Enterprise Authentication Implementation Roadmap Draft released. Reorganized content into an implementation process (hence Roadmap name change), interleaving policy, process, and technology as a way of underscoring the need to work together on these issues.

[August 2006] Second Roadmap Draft released. Rewrote the text and refocused it for IT management. Leveraged the Federal E-Authentication Initiative work as a basis for decision making and planning. Added more explicit navigation for ease of use, a thesis statement for clarity, eight case studies for relevance, and multiple links to campus sites for examples. Added search tool.

Appendix B: Sample Technical Requirements

Mark Bruhn, then Chief Security Officer at Indiana University, developed the following list of possible technical requirements for authentication while at one of the NMI-EDIT workshops:

- Open source and/standards compliant - there are too many different operating systems to get locked into a proprietary solution
- Well-supported
- High availability/reliability
- Scaleable to >150,000 principals
- Not burdensome supporting <5000 principals
- Multi-factor: plug-in locally-determined methods
- Logging – minimally, the date, time, source IP, username, remote logging (e.g., to loghost)
- No password passing; or at least strong encryption of the password in transit
- Passwords not stored at all, or at least stored one-way encrypted
- Facility for users to change their own passwords; forces various formatting requirements
- Facility for users to change their own passwords, if they don't know the old password
- Opportunity to configure with password expiration, history, and intruder lockout
- Authentication protocol should an open standard
- Facility for managing users, passwords, and associated metadata, both by people and by other systems
- Authentication should be two-way: Client-to-Service, Service-to-Client
- Support separate authentication zones with configurable trust relationships
- Both the authentication and management services should provide clear APIs

Appendix C: Single Sign-on Considerations

Because of the popularity of SSOs and its complexity of issues, it serves as a great example of interdependent policy, technology, and business process.

The benefits of coordination and integration of authentication into a Single Sign-on system are well established, and include:

- Improved security through the reduced need for a user to manage and remember multiple sets of authentication information.
- Consolidated account management interface through which all the component authentication systems may be managed in a coordinated and synchronized manner.
- Reduced system administration overhead and response time in adding users or modifying access rights improves security by maintaining the integrity of user account configuration, including the ability to inhibit or remove a user's access to all system resources in a coordinated and consistent manner.

On the other hand, there are non-trivial risks with implementing SSOs, and organizations should consider the following:

- Organizations must have systems that manage authentication and authorization as separate and distinguishable processes. Otherwise, an SSO system may introduce an unacceptable risk.
- Users are known to share their credentials with a friend and co-worker to access their email, documents, or homework problems. If the organization extends the use of this credential by implementing an SSO, the shared credential can then be used to access critical application functions the user may not have intended to share, such as performing assessments, submitting financial information, modifying benefit enrollments, or accessing transcripts. Once organizations recognize this potential for credential sharing, they often become much more concerned about who is really accessing and modifying application data.
- Some applications (such as test taking) require verification that the identified person is the same one using the workstation. In an SSO design, the person may have completed the single login task several hours ago, which may not be sufficient verification for the application. While some SSO systems allow an application to force a re-login, many do not.
- An application must trust a 3rd party authentication system to correctly assert the identity and authentication credentials of a user and protect the authentication credentials used to verify the user's identity to the secondary domain from unauthorized use.
- The authentication credentials must be protected during transfer between the primary and secondary domains against threats that may lead to masquerade attacks, such as interception or eavesdropping.

An SSO may most reasonably be achieved for a defined domain of similar applications or systems that have similar security requirements. Despite the appeal of SSO, business or security drivers may justifiably lead organizations to maintain multiple authentication systems.

Given this, a more realistic goal would be reduced sign-on, which limits the number of authentication systems, resulting in fewer user credential data stores and processes to manage, as well as fewer user authentication methods.