

Industry Project Report



Identity Management At Credit Unions

*An examination of current practices and future trends
of Identity Management at Credit Unions*

www.uwebc.org/cureport2006

Joe Carmichael
Project Assistant

Alfonso Gutierrez
Associate Director, Research & Education,
UW E-Business Consortium
agutierr@wisc.edu



"Helping Industry Gain Competitive Advantage Through E-Commerce and E-Business"



Identity Management at Credit Unions

Joe Carmichael
Alfonso Gutierrez

An examination of current practices and future trends of Identity Management at Credit Unions

EXECUTIVE SUMMARY

WHAT IS IDENTITY MANAGEMENT

Identity management (IdM) is a system and associated processes and policies used to manage a user's digital identity including how the user can access electronic resources such as networks, files, or services from creation to removal. A user may be a credit union member, an employee, or a business partner. A user's digital identity, such as a password, is the username and associated attributes, such as a password or role.

In credit unions, IdM is applied as a method of addressing electronic security issues. This may include tasks as simple as managing how an employee logs onto the credit union intranet to combating problems as complex as identity theft and federated networking.

Through surveys, focus group discussions, and a case study this report identifies the most common identity management issues and concerns facing credit unions today and the current IdM tools and techniques being practiced at credit unions and other organizations. This information can be used to improve a current IdM system or to create a new one using the experiences of their peers as a guide. This report will be useful to both the executive who wants to further understand their organization's IdM needs and to the IT manager trying to communicate the importance of IdM to executives.

This study was a collaboration by the Credit Union Information Security Professionals Association (CUISPA), the CUNA Technology Council, CUNA Mutual Group, the Education Credit Union Council (ECUC), the University of Wisconsin-Madison's Division of Information Technology, and the University of Wisconsin-Madison's E-Business Consortium.

KEY FINDINGS

- IdM is in its early stages and is rapidly evolving. Many implementations of new IdM technologies, such as biometrics, are changing how identities are managed. These new implementations at credit unions seem to be more experimental than mature, though, and will likely see many changes before they become standard.
- The cost of IdM is far outweighed by the risks of not implementing IdM security measures.
- The biggest vulnerabilities lie not in faulty software or hardware packages, but in how users protect their passwords and credentials outside the system.
- Interoperability between disparate platforms or applications is a major hurdle.
- IdM is being managed by high level governance bodies such as Boards of Directors. This is good, as it quickly elevates identity management and security issues to the top of the organization. However, this model tends to leave out the more technically savvy members of the IT staff.
- Many IdM processes are performed manually, even though tools for automation exist that can reduce the number of errors made in creating and managing identities.
- Regulations demanding multiple layers of authentication are slowing down the validation process for each online user by seconds, adding up to thousands of hours each year. Focus group participants state that more are likely on the way.
- Members are not proactively requesting IdM tools or security features until they are directly affected by identity theft. They generally don't use the tools they are given, even when they were specifically requested.
- Microsoft appears to be the most dominant player — primarily through the prevalence of its Active Directory.
- Although there is much interest in biometrics and single sign on, few substantial implementations of these technologies stand out.

INTRODUCTION

WHO SHOULD READ THIS REPORT

This report is intended for credit union executives seeking greater knowledge of the practice of identity management, as well as future trends which will impact decision-making at their own credit unions. It is also written for IT managers needing to make a case for IdM to executives within the credit union.

The body of the report presents and discusses the results of the survey and focus groups and presents a case study from the University of Wisconsin—Madison Division of Information Technology. Several appendices follow, including a glossary of IdM terms and a copy of the whitepaper that accompanied the survey. This whitepaper can be used as a reference for IdM concepts encountered in the report.

INTRODUCTION

The term Identity Management (IdM) describes a system and associated processes and policies used to create, distribute, maintain, and terminate the digital identifier used to distinguish a user or group of users. This system utilizes specific hardware, software, and skilled professionals to actively manage how employees, credit union members, or federated business partners access both IT and other resources within the credit union.

Credit unions are currently implementing identity management in varying degrees. However, the advent of online banking, combined with existing techniques for utilizing networked electronics is increasing the need for IdM services in this industry. The value of electronic resources such as computers, servers, networks, and the data stored within them, as well as recent increases in digital theft have propelled IdM to the forefront of information security discussion.

The Federal Trade Commission (FTC) statistics indicate that identity theft is the fastest growing crime in the U.S., and it shows no signs of diminishing. The FTC reports that 27.3 million Americans have been victimized in the last five years, including more than 10 million in 2005. These alarming statistics lend credibility to the need for establishing effective and proven techniques for managing all the identities which may interact with the credit union's digital resources.

It is important that credit union executives understand the key concepts underlying IdM to best determine their organization's need for IdM and best address the concerns voiced by their information security professionals.

Despite being a complex information technology process,

IdM can be described using a life-cycle of four primary stages: Registration/Creation, Propagation, Maintenance, and Termination. Additionally, the Maintenance stage includes several steps for managing the day-to-day use of digital identities.

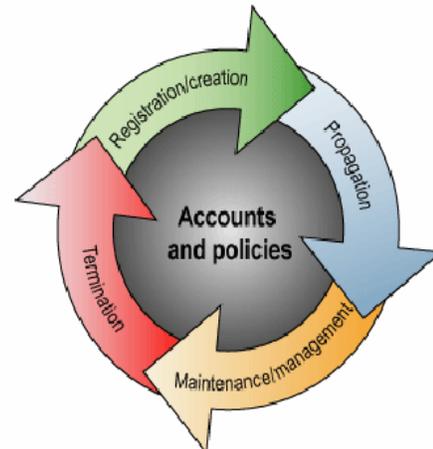


Figure 1: The four stages of an identity encompass how accounts and policies are managed. *Source: Burton Group, 2005*

CONTENTS

Pg.	
2	Introduction Demographics, Methodology, Governance
5	The Beginning and Ending of Individuals' IDs Creation, Registration, Termination
7	Locating Individuals' Identities Provisioning, Authorization, Synchronization
9	Proving Individuals' Identities Authentication, Sign-on, Techniques
11	Dealing with Your Business Partners' Identities Federation
12	Ensuring the Integrity of Identities Auditing
13	Building the Infrastructure Software, Tools, Vendors
15	Case Study UW-Madison Division of Information Technology
18	Appendix A: Glossary Definition of Identity Management Terms
19	Appendix B: Whitepaper Introduction to Identity Management Concepts
25	Appendix C: Acknowledgments Special thanks
26	Appendix D: References Citations of resources

INTRODUCTION

METHODOLOGY

This report is based on findings from a survey and subsequent focus group discussions. The survey was administered to approximately 350 credit unions with memberships in either CUISPA, ECUC, or the CUNA Technology Council. Ten percent of those surveyed responded. Following an analysis of the survey data, focus groups were held in which survey respondents were asked to discuss items of particular interest. Focus groups were attended by five of the survey participants.

DEMOGRAPHICS

In this study, the credit unions were categorized into four regions as follows:

Northwestern States

Idaho, Iowa, Kansas, Minnesota, Missouri, Montana, Nebraska, North Dakota, Oregon, South Dakota, Washington, Wyoming

Southeastern States

Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, West Virginia

Northeastern States

Connecticut, Delaware, District of Columbia, Illinois, Indiana, Maine, Maryland, Massachusetts, Michigan, New Hampshire, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Vermont, Wisconsin

Southwestern States

Arkansas, Arizona, California, Colorado, Louisiana, Nevada, New Mexico, Oklahoma, Texas, Utah

Analysis of the survey data revealed that **46%** of responding credit unions were from southwestern states with a majority of those responding from California. **11%** were from the southeast, **26%** from the northeast, and **17%** from the northwest.

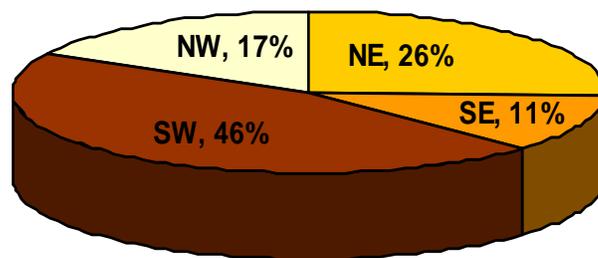


Figure 2: Distribution of survey respondents by region.

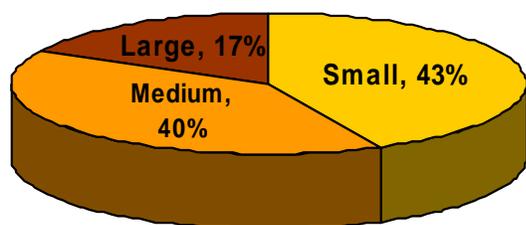


Figure 3: Distribution of survey respondents by asset size.

ASSET SIZE

Participating credit unions were also categorized by asset size as follows:

- Small — \$0-50 Million
- Medium — \$51-500 Million
- Large — \$501+ Million

The percentage of respondents from each size group was **43%**, **40%**, and **17%**, respectively.

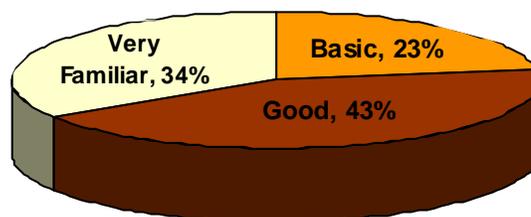


Figure 4: Distribution of survey respondents by level of understanding of IdM concepts.

LEVEL OF UNDERSTANDING OF IdM

Each of the survey participants was asked to rate their understanding of IdM. A whitepaper explaining the basics of IdM accompanied the survey. Participants with little or no previous exposure to IdM who had read the whitepaper were considered to have a basic understanding. Other options were "No Understanding," "Good Understanding," and "Very Familiar." Respondents described themselves as **0%** having no understanding, **23%** with basic understanding, **43%** had a good understanding, and **34%** claimed to be very familiar with IdM.

INTRODUCTION (CONTD.)

DEMOGRAPHICS COMPARISON

In searching for trends, comparisons were made of the three primary demographics. Notable trends were that (i) a respondent's understanding of IdM tended to increase with the credit union's size, (ii) credit unions in the southwest tended to have a better understanding of IdM while the southeast showed a trend toward a more basic understanding of IdM, and (iii) large and small credit unions were better represented in the southwest and medium sized credit unions responded more from the northeast.

Size to Region			Size to Understanding			Region to Understanding		
Size	Region	Percent	Size	Understanding	Percent	Region	Understanding	Percent
Small	NE	13%	Small	No Understanding	0%	NE	Basic Understanding	11%
Small	SE	13%	Small	Basic Understanding	40%	NE	Good Understanding	67%
Small	SW	60%	Small	Good Understanding	27%	NE	Very Familiar	22%
Small	NW	13%	Small	Very Familiar	33%	SE	Basic Understanding	50%
Medium	NE	43%	Medium	No Understanding	0%	SE	Good Understanding	50%
Medium	SE	14%	Medium	Basic Understanding	14%	SE	Very Familiar	0%
Medium	SW	21%	Medium	Good Understanding	57%	SW	Basic Understanding	25%
Medium	NW	21%	Medium	Very Familiar	29%	SW	Good Understanding	25%
Large	NE	17%	Large	No Understanding	0%	SW	Very Familiar	50%
Large	SE	0%	Large	Basic Understanding	0%	NW	Basic Understanding	17%
Large	SW	67%	Large	Good Understanding	50%	NW	Good Understanding	50%
Large	NW	17%	Large	Very Familiar	50%	NW	Very Familiar	33%

GOVERNANCE

An IdM governance board is a body of individuals dedicated to creating standards and policies regarding identity management. Such a board is responsible for guiding decisions related to IdM projects and their implementations. IdM governance boards also work with the IT department and the Board of Directors to defend security breaches involving members' or employees' identities.

Key Findings

- Of those surveyed, 70% of credit unions don't currently have dedicated IdM governance boards. The common practice is to elevate IdM issues to established boards with wider scopes, for example, Boards of Directors.
- Although many credit unions have IdM standards in place, a significant number have not established formal policies. This may be a reflection of IdM not having the level of awareness necessary to gain priority over other issues.
- Only half of the credit unions have had members requesting IdM tools. This reflects a likely unawareness of the topic or apathy on the part of membership. It is also possible that members do not know what to ask for.

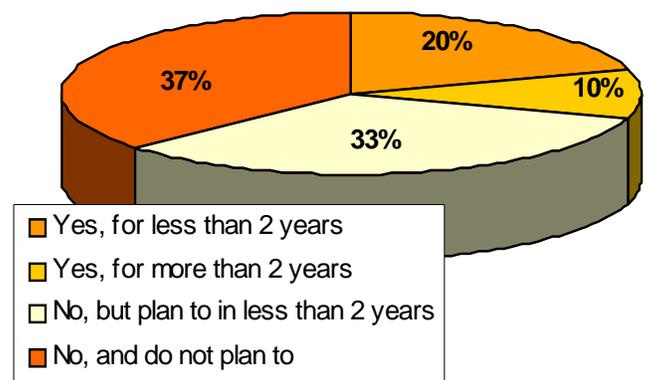
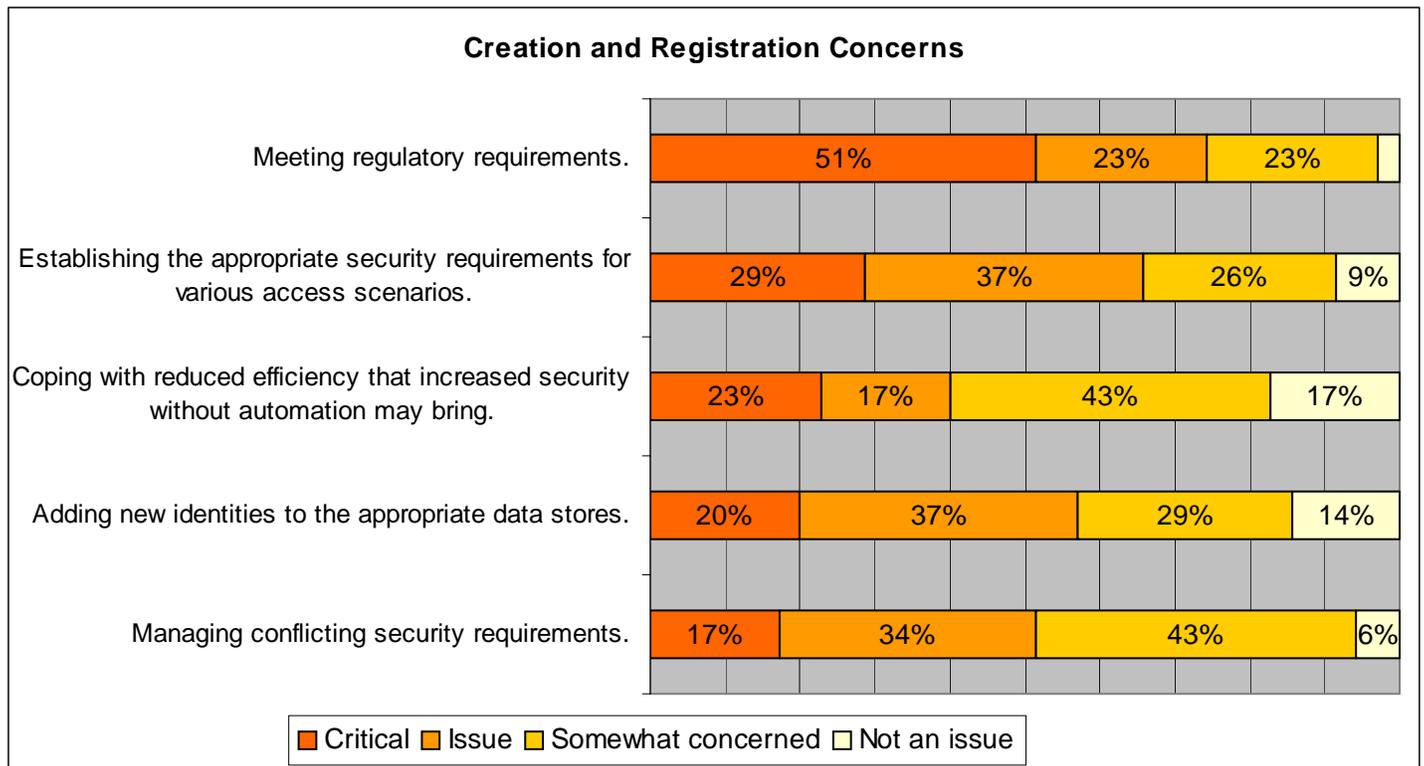


Figure 5: Percentage of survey respondents whose credit unions utilize a governance board for IdM issues.

THE BEGINNING AND ENDING OF INDIVIDUALS' IDENTITIES

REGISTRATION/CREATION

The registration/creation step is the creation of a new user's identity. It involves assigning some unique identifier, such as a username or ID number, to the user and assigning some initial attributes to the new identity. These attributes may be related to the user's role within the credit union, an initial password, or security clearances. Once an identity has been created, it is propagated to the appropriate databases or directories, which can be generally described as data stores.



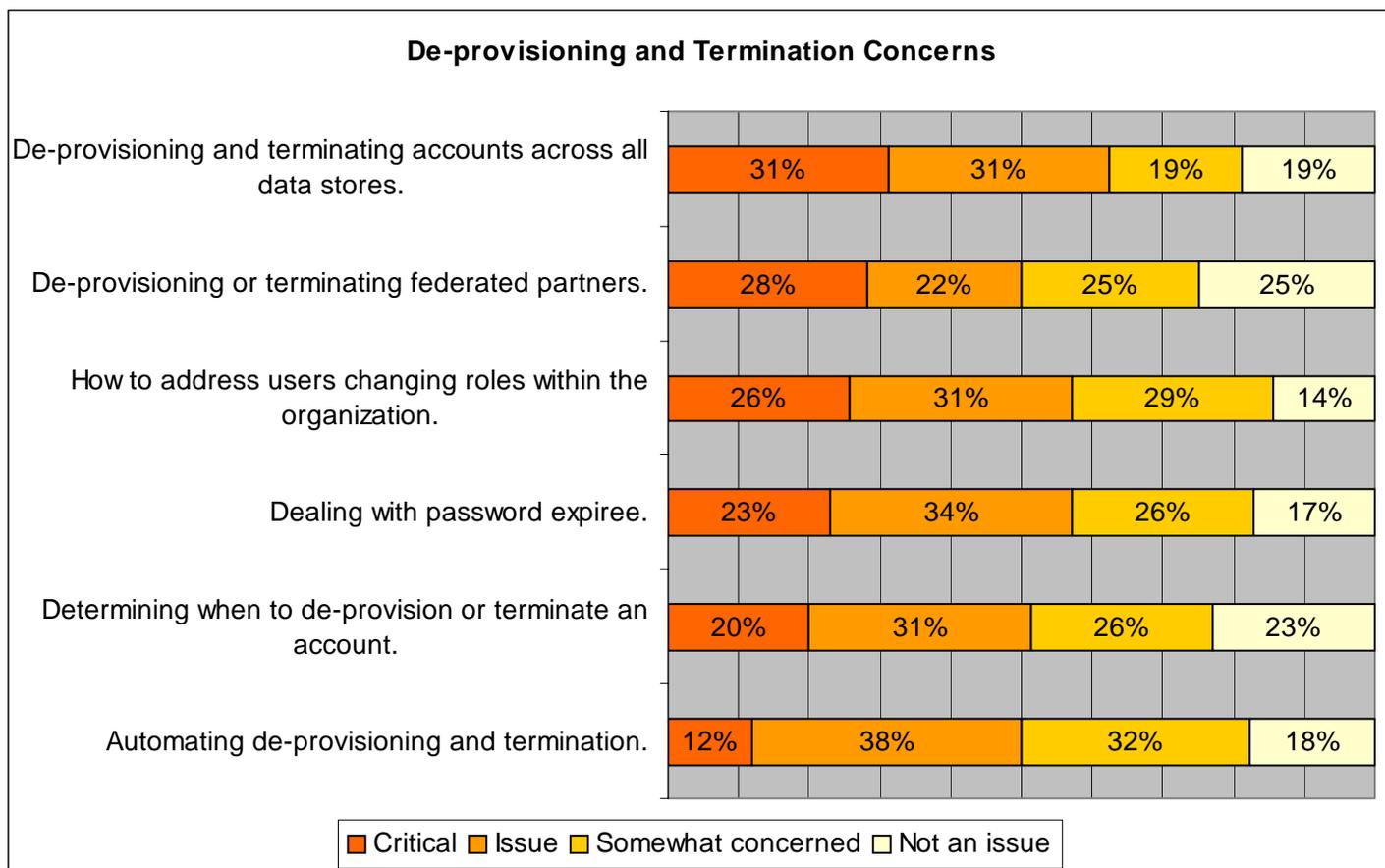
Key Findings

- Of those surveyed, 75% of credit unions are concerned about meeting regulatory requirements such as OFACT and the Patriot Act.
- Focus group participants feel that legislators are pushing for more layers of authentication.
- A major difficulty is balancing the slowdown caused by validation requirements with meeting regulations.
- Creating accounts is still a mostly manual process. Integrating IdM systems with HR systems may alleviate this when dealing with employees' identities.

THE BEGINNING AND ENDING OF INDIVIDUALS' IDENTITIES (CONTD.)

TERMINATION

Termination is handled in a similar manner to the creation step. However, instead of granting attributes, a user's account is stripped of credentials and entitlements and is deleted from the access granting data-stores. In some cases, an identity may be provided with a new set access information. If a user account is no longer necessary, though, the most secure option is to terminate the profile completely.



Key Findings

- It is difficult to manage all the department needs and business requirements involved in terminating an employee's clearance or password. It is easy to know when someone needs access, but much more difficult to know when they no longer need it.
- The termination process is a primarily manual process at present, but automation would have a large beneficial effect on both it and de-provisioning.
- If an employee is terminated, IdM staff must get the appropriate paperwork from HR immediately to promptly handle the access issue.

LOCATING INDIVIDUALS' IDENTITIES

PROPOGATION

Once an identity has been created, it must be added to the credit union's identity management system. Depending on the system, propagation may require identity integration tools. In systems that include multiple data-stores, middle-ware must be used to coordinate the identities of users that are stored in any of the separate identity data-stores.

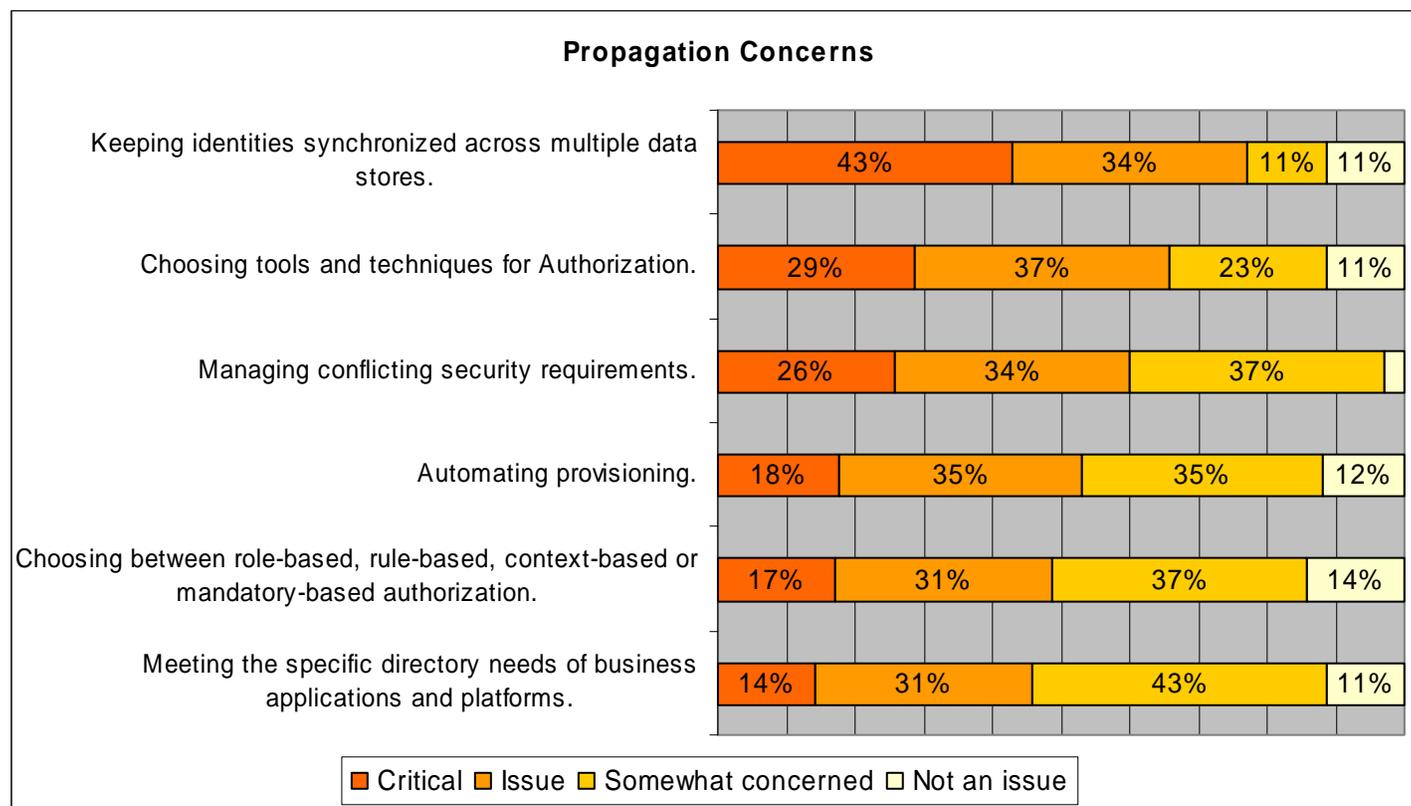
The identity may be stored on a relational server or on a distributed directory. A relational identity store, such as a SQL server, typically provides increased data protection, ease-of-use, and flexibility while exhibiting slower retrieval speeds than a distributed directory. In a distributed directory, information is not stored at a central location. Instead, it is maintained on dedicated directory servers and synchronized between them. The distributed system allows users to access data from any of many computers with a single sign on.

PROVISIONING

Once an identity has been created and propagated, it is provisioned. Attributes such as credentials, access rights, and entitlements are assigned to the identity. These attributes could include passwords, security clearances, and access privileges to certain resources. This information is typically stored in a distributed directory. Many IdM systems now use role-based provisioning, in which one of the initial attributes assigned to a new user describes their role within the system. The user's account is then granted access to a predetermined set of resources that are necessary to fulfill the duties of their role.

AUTHORIZATION

Authorization is the determination, by comparing the credentials associated with a user's authenticated identity with the security configurations of a resource, whether or not a user may access that resource or perform certain functions within it. These security configurations may be stored on a centralized server or in a distributed directory.



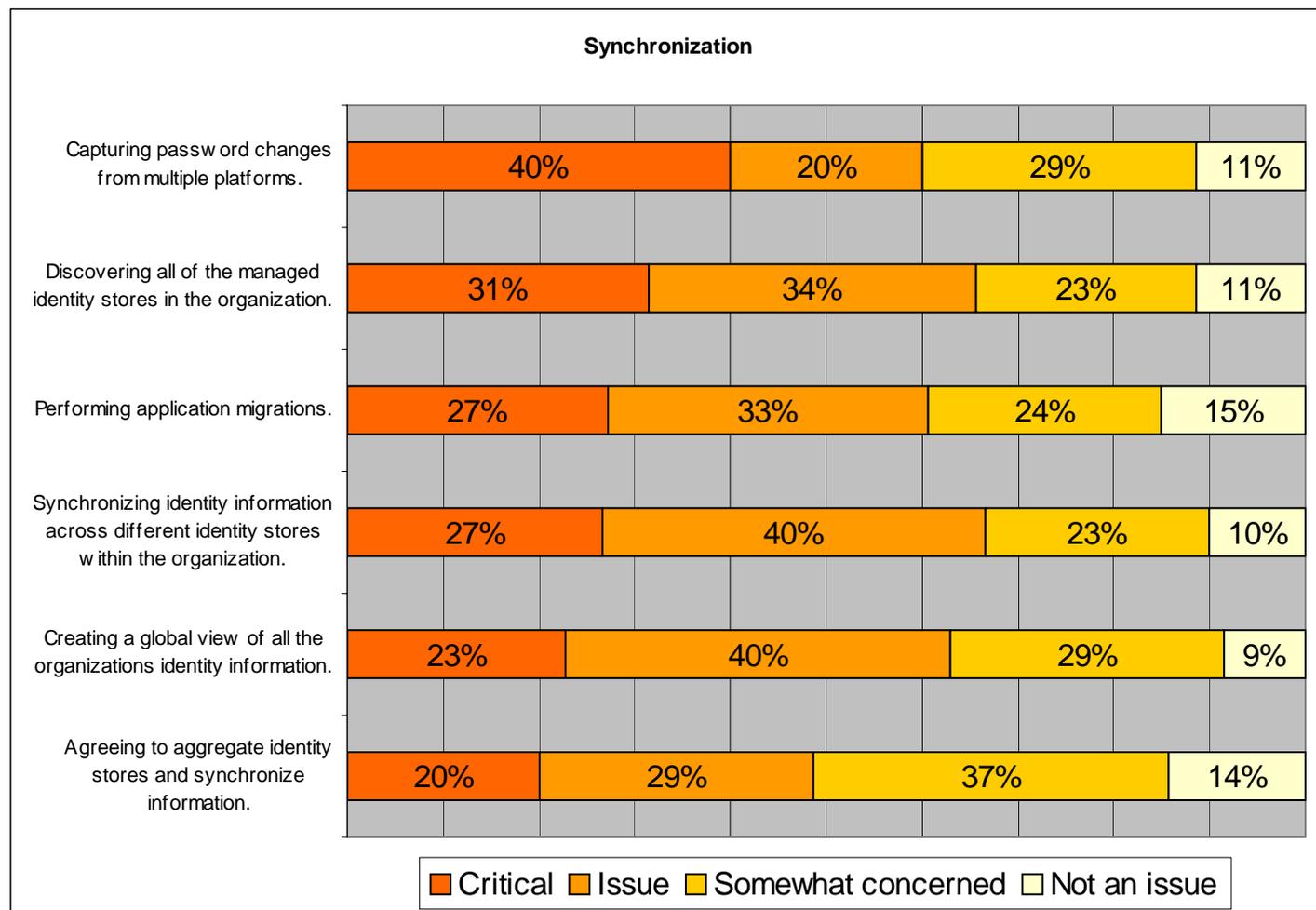
Key Findings

- Adding identities to data-stores is a manual process which is prone to data entry errors.
- Role-based provisioning is the easiest way to grant access.

LOCATING INDIVIDUALS' IDENTITIES

SYNCHRONIZATION

A type of identity integration, synchronization ensures that an identity is current at all data-stores. Software may be used to check for changes in an identity's attributes and apply those changes to all the servers and directories where the identity is being maintained.



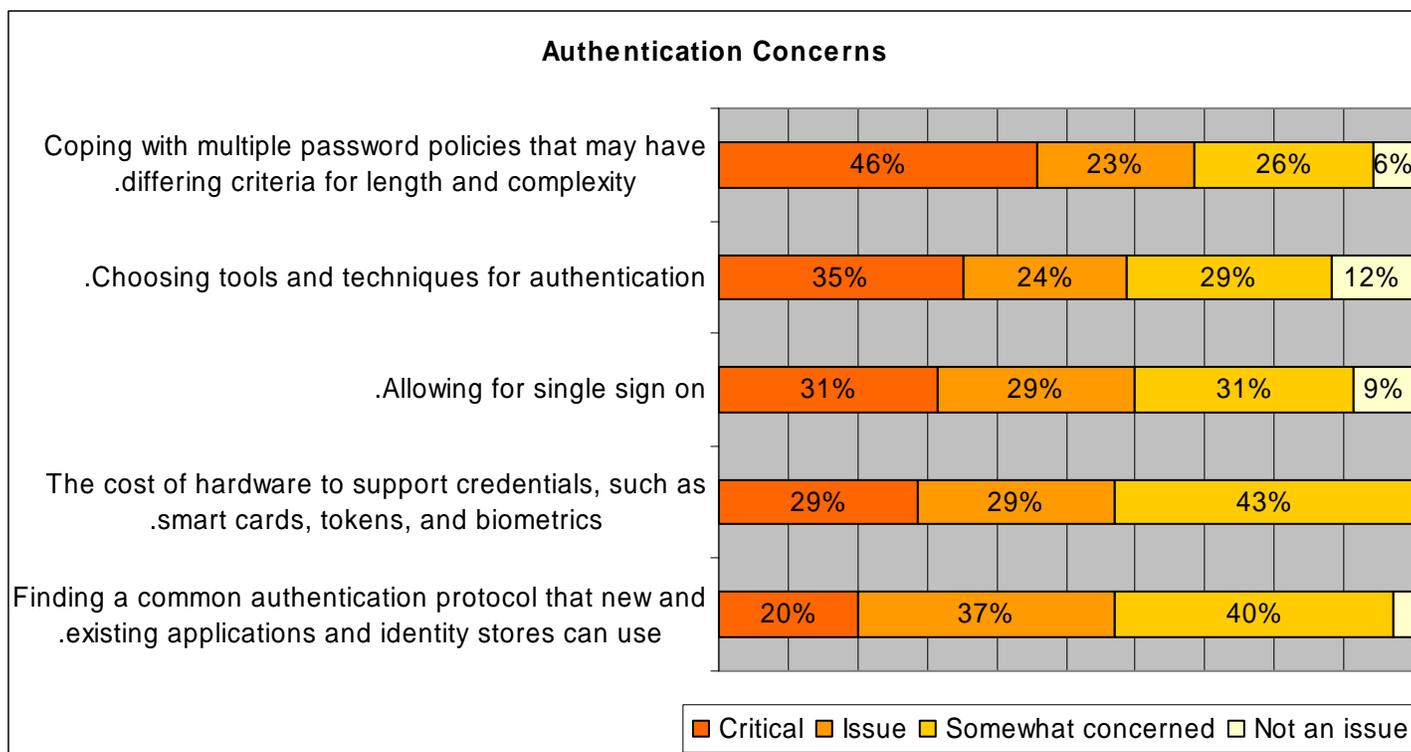
Key Findings

- Synchronization issues more often affect employees than members.
- Synchronization is a mostly manual process and is prone to data entry errors.
- Poor interoperability between systems is a big hurdle to synchronization.
- It is important to know where identity data such as attributes are stored, both in-house and with third parties.

PROVING INDIVIDUALS' IDENTITIES

Authentication and Sign On

When users try to access and utilize their identities, checks need to be made to ensure that the users are who they say they are. This is authentication. Several methods and tools exist for user identity authentication, and the best IdM systems use several methods in combination. Some of the most common authenticators are passwords, certificates, and Secure Socket Layers. Biometrics are quickly becoming a popular method for authentication. Biometrics compares physical characteristics of a user, such as a retina or a fingerprint, to a stored standard. Presumably, since such biometrics are unique to an individual, this is the best method of authenticating a user. As the technology improves, a combination of biometrics and smartcards, and small radio-frequency based storage devices, are expected to become the primary method of authentication.



Key Findings

- Authentication is any system’s first and main line of defense. This makes it a critical IdM topic.
- Most authentication protocols are written for one platform. This usually results in inoperability issues between Windows, Apple, or Linux systems.
- It is important to protect members’ data with multiple levels of authentication, e.g., for call center support and password resets.
- Encrypt password transmissions whenever possible. When encryption is not available, a Virtual Private Network can be an alternative offering secure transmission.
- The biggest vulnerabilities in any identity management system stem from peoples’ behaviors. People write down passwords they can’t remember, walk away from logged-in workstations, share passwords and accounts, use simple, easy to remember passwords, and download applications or files that create security holes. Education and awareness are the best options for mitigation.
- Members want convenience more than security.
- Different applications have different password length and complexity requirements. Vendors need to be pressured to incorporate strong authentication into their applications.
- Password expiree works well with employees. It is not recommended for members as they will be upset at the inconvenience of having to change their password at regular intervals.
- Single sign on is an issue more for employees than it is for members, but as credit unions expand their services to include credit cards, loans, investments, and federated services the topic will become more relevant to members.
- Single sign on may alleviate synchronization difficulties, as password changes are typically performed manually.

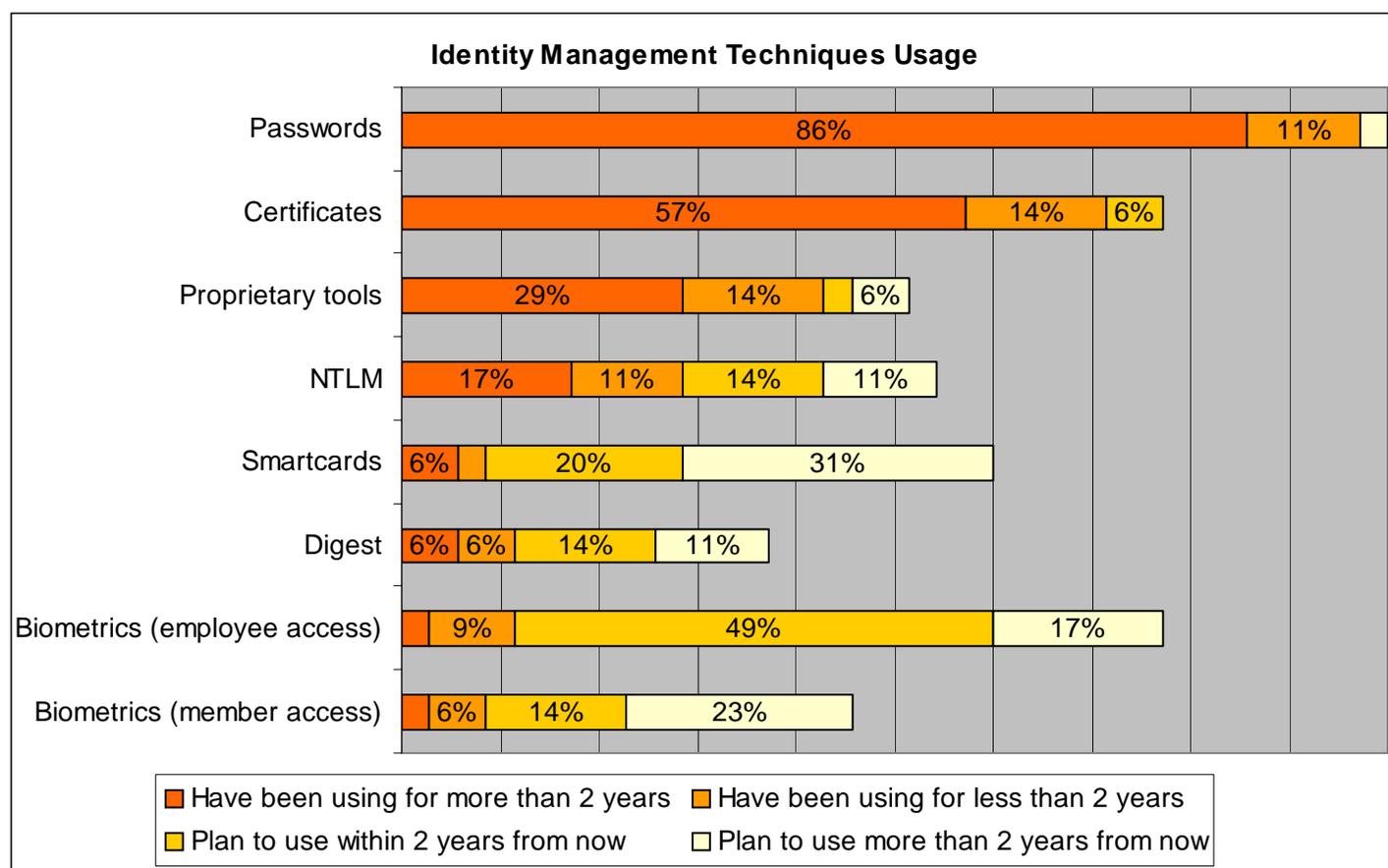
PROVING INDIVIDUALS' IDENTITIES

Specific Techniques for Proving Identity

Many specific techniques exist for managing identities from one task to another. Techniques such as passwords, certificates, smartcards and biometrics all aim to create a simpler, more secure environment for the end user. The effectiveness of any of these tools is, of course, dependent on how it is implemented and the extent to which the user adheres to guidelines surrounding their usage. Each also has associated pros and cons.

Passwords are the oldest, least expensive, and most widely adopted method of authenticating a user. Their length and complexity can be adjusted to meet the needs of an organization, they can be changed readily, and there is an infinite number of password possibilities. Passwords can also be forgotten, are frequently written down leaving them vulnerable to being found, can be deciphered, and suffer from the fact that many users do not log-off when they leave a terminal they are logged in to.

Certificates, smartcards, and biometrics are more expensive alternatives to passwords. Certificates are files residing on a computer which vouch for that computer's identity. Certificates must be purchased from an issuing authority. Smartcards are devices that hold user credentials and which can be carried in a wallet, pocket, or keychain. These are often a very secure but expensive method of authentication with excellent user convenience. Biometrics is an emerging technology which allows users to be identified by fingerprints, retinal scans or other unique physical identifiers. Applications for biometrics will vary greatly between employees and members.



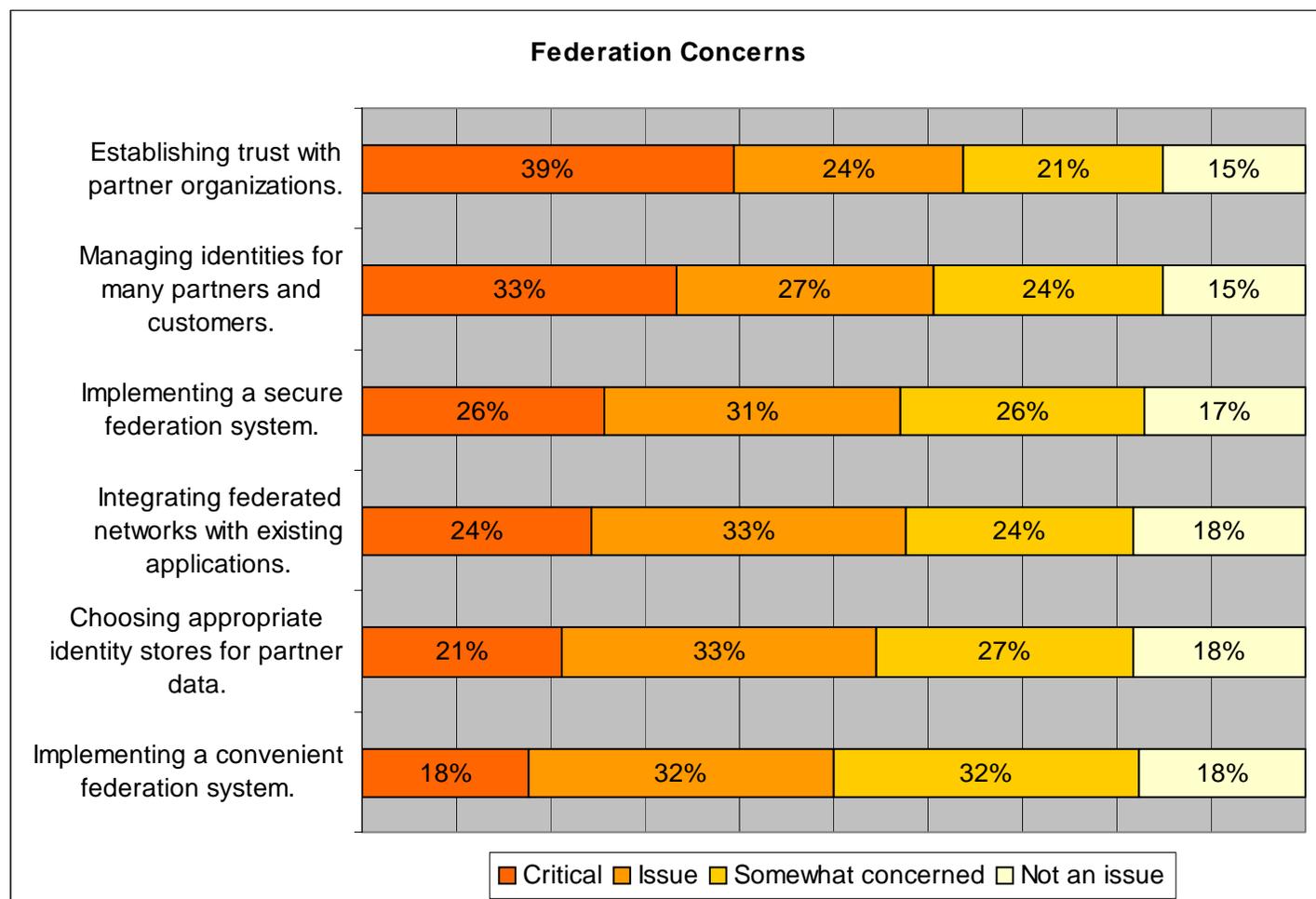
Key Findings

- There is currently a lack of consensus amongst credit unions regarding the use of biometrics, but it is expected to become one of the more accepted methods of authentication. The cost is lower than tokens and certificates, but typically requires a second form of authentication to be secure.
- There are many logistical difficulties in requiring members to use fingerprint readers from home, such as providing each member with a scanner and ensuring that it is installed and functions properly.
- There are some privacy and sanitary issues associated with biometrics.
- Members are unwilling to carry anything extra, e.g. smartcards, hardware tokens.

DEALING WITH YOUR BUSINESS PARTNERS' IDENTITIES

Federation

Federation works on the principle of digital trust. A user may authenticate at a certain sign-on point, but wants to access resources from another department, network, or business partner. In a federated network, the second service provider would recognize the authentication process of the first and would not require the user to sign-on with another set of credentials. Trust may be granted to individual users or to whole domains.



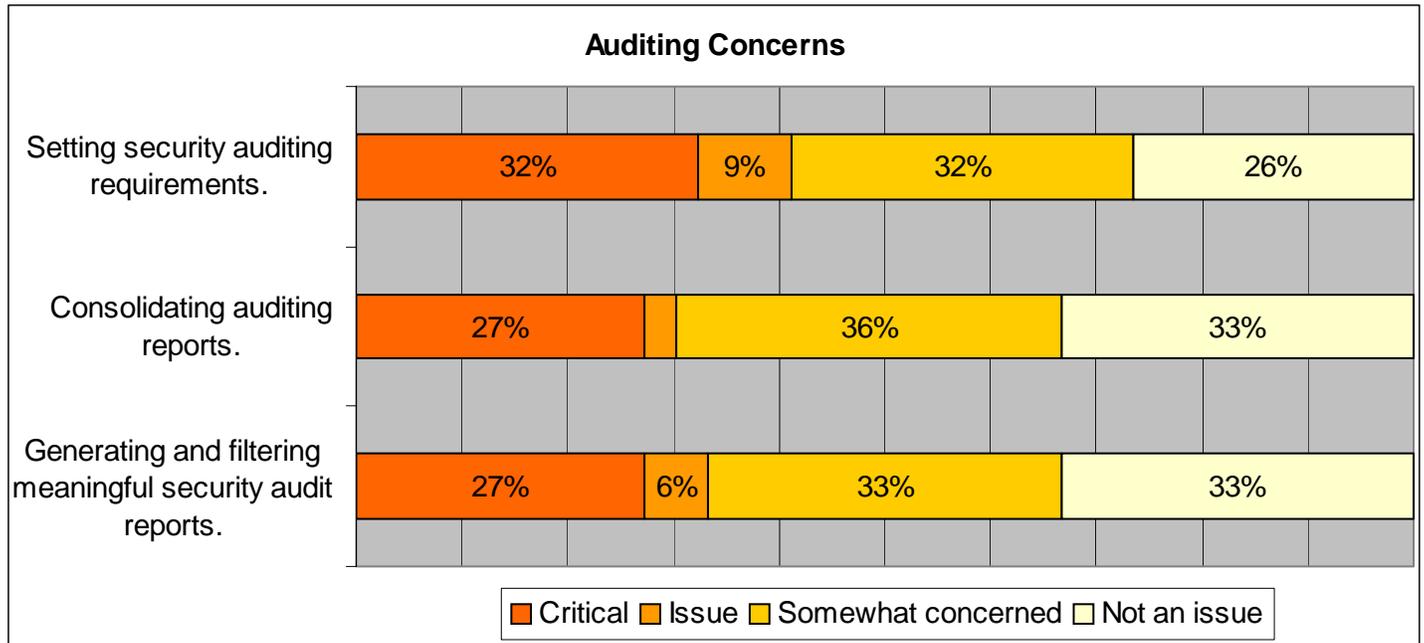
Key Findings

- The practice of federation is limited at credit unions. It is relegated almost exclusively to ATMs, vendors, and outsourcing partnerships. Credit unions are typically not federating services.
- Federated partnerships generate many of the same requirements for identities as internal IdM systems. The IdM system must still authenticate and authorize outside users.
- The major barriers to federation are that most vendors and partners do not take security as seriously as the credit unions and that auditing partners is extremely difficult. When a partner’s security is not as strict as the credit union’s, establishing equal levels of trust is very difficult.
- Internal security policies don’t directly affect third parties. Credit unions have to hold partners to the same standard of security as the credit union, which may strain relationships if the standards are too high or too expensive to implement.
- Federated accounts are very important to terminate when they are no longer needed as they grant outside access to resources. They are often forgotten, though.
- Credit unions should try to keep track of which employees have been federated to other companies as well as who has been federated to their own.

ENSURING THE INTEGRITY OF IDENTITIES

Security Auditing

Security auditing is an important and often overlooked segment of IdM. Audits may be done to test a system for security weaknesses or to check for possible recent security breaches. In the case of testing for security weaknesses, an IdM system is attempted to be broken into by a known and trusted source so that any flaws are found and fixed before an actual malicious attack is conducted. It is also a good idea to maintain logs of user activities to ensure that the system is operating as expected. Some logging programs highlight suspicious activities and known security threats within a log.

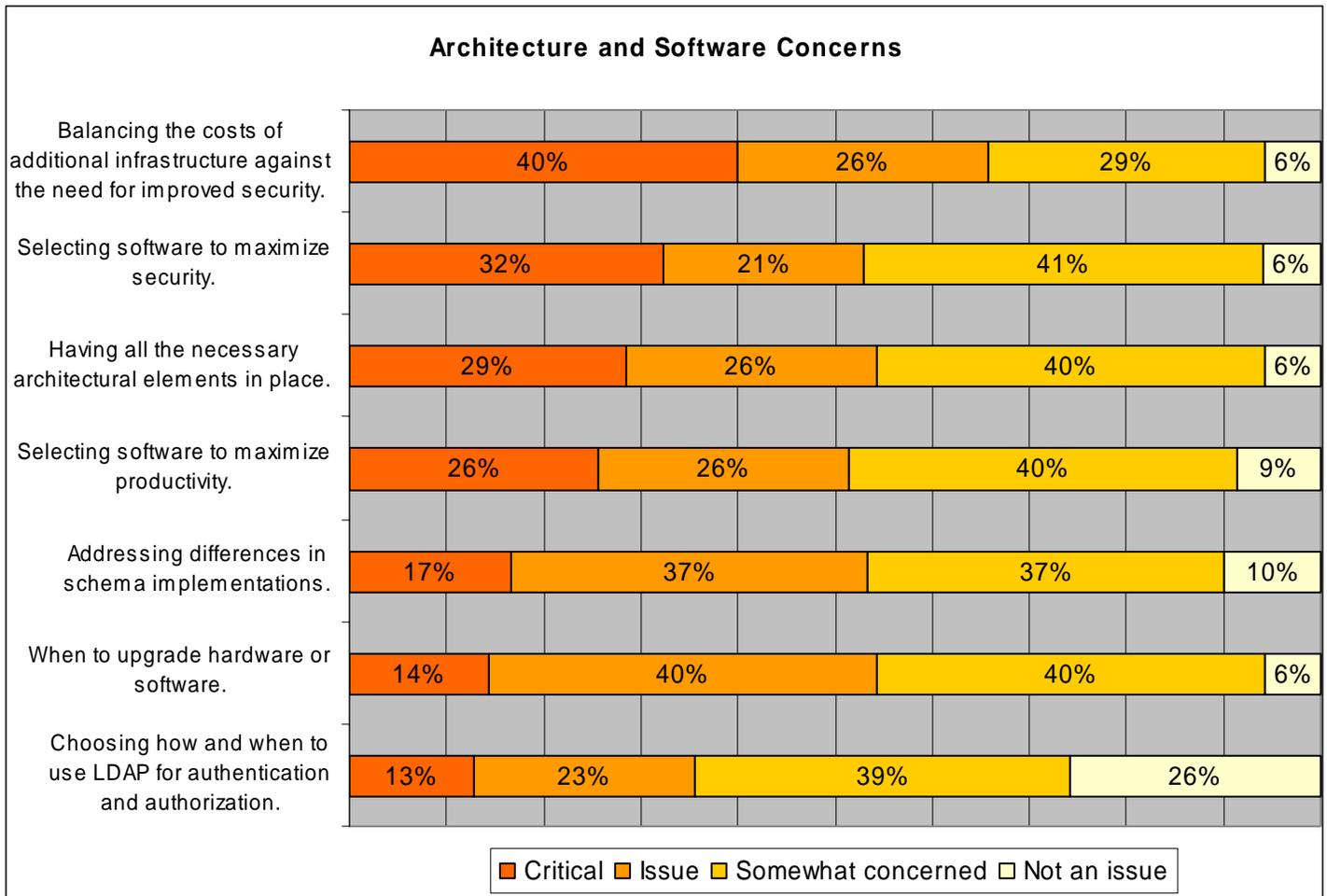


Key Findings

- Currently, most security auditing at credit unions occurs after an attack. There is little real-time auditing, as real-time requires lots of resources and automation. These are expensive, and generally cost more than the insurance to cover fraud.
- Online fraud is still perceived minimal compared to traditional check and credit card fraud.
- The three main strategies for auditing IdM systems are:
 1. Auditing log dumps to find when events happened.
 2. Auditing log dumps to analyze past trends.
 3. Analyzing in real time to project trends or catch security breaches as they happen.

BUILDING THE INFRASTRUCTURE

A significant amount of architecture is required to operate an IdM system. Most established companies have many disparate networks and data storage systems, and linking them together into a cohesive system that allows for automatic propagation, provisioning, synchronization, and other IdM best practices can be a complex and difficult task. Many different hardware, software, and middleware tools are required to maintain a functional, secure, and convenient system for accessing system resources.



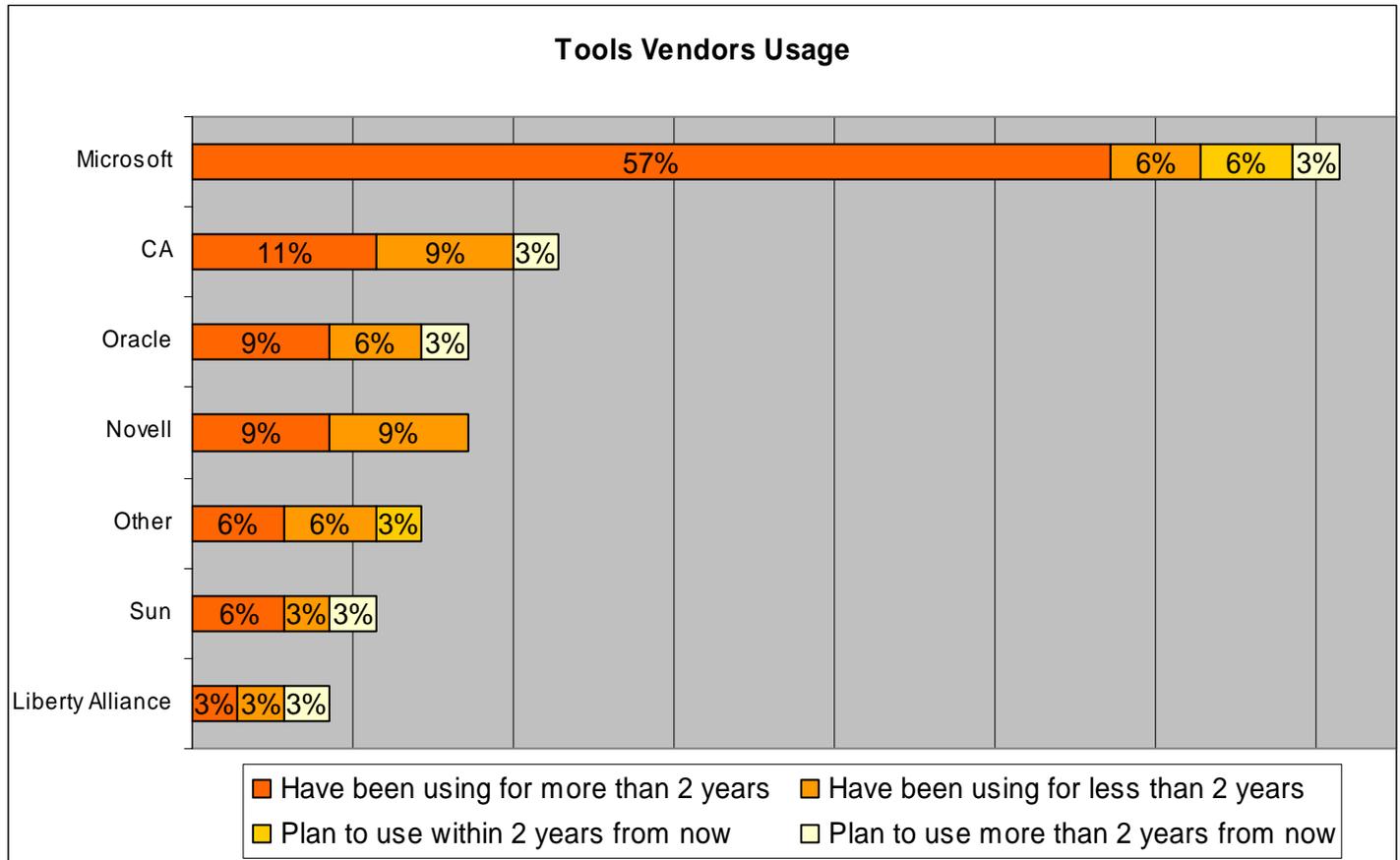
Key Findings

- Normal risk analysis and ROI measures aren't always the best metrics when addressing security. Focus group participants feel that members having good experiences is more often a priority than ROI.
- Paying for a good security/IdM infrastructure can be viewed as similar to buying insurance and may help maintain reputation and member trust.
- Common credit union priorities are: 1. Member experience 2. Risk management 3. Employee productivity.
- Convenience and security don't necessarily have to be mutually exclusive, but the costs are usually higher when building a system which considers both.

BUILDING THE INFRASTRUCTURE (CONTD.)

Tools Vendors

There are dozens of vendors offering IdM solutions. The major players, though, are familiar names. The widespread use of Microsoft Windows and its Active Directory make it a prominent vendor in the IdM field. The Liberty Alliance, a not-for-profit organization, is taking a different approach than the other vendors. It is working to provide open-source, standards based systems for federation and other IdM techniques.



Key Findings

- Microsoft generally has more vulnerabilities than proprietary systems, but proprietary systems are much more expensive and usually painful to integrate and maintain.
- Focus group participants mentioned that many credit unions use tools from multiple vendors to manage identities in different ways. They felt as though most people are not aware of the systems they don't see daily, and so lesser known vendors may be underrepresented in this analysis.
- According to focus group participants, base systems are often from vendors, but considerable in-house customization is often performed on these software and hardware packages to better fit the needs of an individual credit union.

CASE STUDY: UNIVERSITY OF WISCONSIN—MADISON DIVISION OF INFORMATION TECHNOLOGY

Much can be learned from the examples of successful predecessors. This section looks at the University of Wisconsin—Madison's Division of Information Technology (DoIT) identity management system. Within this case study is information about current and future methodologies and technologies.

GOVERNANCE

The University of Wisconsin-Madison recognizes that IdM technologies are not the only elements influencing the success or failure of IdM. Equally, if not more important, are the policies and governance structures that inform the adoption of technology. With that in mind, the University formed the Identity Management Leadership Group (IMLG) in 2005. This group is comprised of campus leaders with responsibility for systems that provide or consume identity data. The major goal of this group is to support the University's continuing efforts to build an IAM infrastructure that allows DoIT to retain their highly decentralized organizational structure while at the same time minimizing 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 DoIT 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.

Specifically the IMLG is charged with:

- Defining identity management process roles and responsibilities for obtaining access to information and services
- Establishing criteria about how decisions are made
- Coordinating and negotiating access to information and services
- Seeking efficiencies, especially in the area of eliminating duplicative cards for ID and security purposes

CREATION

Methodologies

Person data is submitted to the University Directory Service (UDS) from the student and HR administration systems, as well as from a Special Authorization system which stores data on "non-traditional" affiliations and populations. Matching algorithms merge and cleanse the data for use by client systems. Source data is maintained to facilitate troubleshooting.

Technologies

The UDS person registry is implemented in an Oracle database with a subset of UDS data expressed by means of

the Sun One Lightweight Directory Access Protocol (LDAP) server. Consumers of directory services have a number of ways to access data including LDAP calls, database views and reports, file exports, and Web services.

The Future

DoIT is endeavoring to make the matching and merging process more transparent to providers of data to ensure accuracy. They are investigating a more centralized identity proofing and registration process to better control the inputs to the UDS.

DoIT is concentrating on Web services interfaces and is investigating standard schemas for the communication of identity data.

PROPAGATION

Methodologies

No centralized service is in place to make available a joined "view" of identity information. This has been a conscious choice as reflecting data from authoritative systems, by merging, cleaning and making available via the University Directory Service (UDS) (a more meta-directory model) was determined to be a more workable choice than implementing virtual directory technology. However, the need for joining identity data has been considered throughout the implementation of the University's IdM deployment. Specifically, the data model supports common keying across the UW system. In addition, all user objects are provisioned with a Publicly Visible Identifier (PVI) which is unique and persistent, allowing systems to link local identity data or transaction logs with an identity stored in the UDS or in the UW System Identification, Authentication and Authorization system.

The Future

DoIT's work in this area is policy and administratively focused on promoting the proper use of identifiers to link data from disparate systems (for example with the use of PVI).

MAINTENANCE AND MANAGEMENT

Provisioning

Methodologies

The University of Wisconsin-Madison (UW-Madison) has deployed a centralized IdM infrastructure which can provide person data and identity related services to campus and system customers. This infrastructure was developed and is managed centrally. Person information is expressed in the UDS which provides or is the data source for a number of IdM related services. The UDS contains information on over 160,000 students, staff and others associated with the University; for example, a recent addition to the UDS was the undergraduate applicant population,

CASE STUDY (CONTD.)

significantly improving the University's ability to offer services to potential students. The UDS has been integrated with a number of key service providers including the enterprise portal, web mail, web calendar, course creation software, financial systems, the campus television network, and institutional data repositories. Self-service NetID provisioning is also provided.

The UDS has also been expanded to include person information for all UW campuses, supporting system wide services and an increasingly mobile user base.

Technologies

The UDS person registry is implemented in an Oracle database with a subset of UDS data expressed by means of the Sun One LDAP server. Consumers of directory services have a number of ways to access data including LDAP calls, database views and reports, file exports, and Web services.

The Future

DoIT is working on Populations, Affiliations and Service Entitlements (PASE), a role based identification system which will replace the Photo ID Special Authorization system that currently stores demographic, affiliation and sponsor information for non-student/non-staff populations.

Other projects include an attribute delivery initiative which will validate the user's needs for IdM data and the methods most appropriate to deliver it. SAML, Shibboleth and enhancement and standardization of Web services will likely be part of any solution and fits well with the University's work on Service Oriented Architecture.

On demand provisioning is also being explored.

Authentication**Methodologies**

The UW-Madison currently has two enterprise-wide authentication mechanisms, WebISO (web initial sign-on) and PKI (Public Key Infrastructure), with direct LDAP and RADIUS services are also provided. Centralized credential stores support authentication services. WebISO is the University's web access management system; WebISO (and other authentication systems) are supported by a Lucent, common identifier, the NetID. Over 50 applications currently use WebISO to control access.

The PKI system is relatively new and has 250 active users. The system issues client certificates for digital signing and encryption. Use of PKI is voluntary but is being marketed as a way for UW-Madison Faculty, Staff and Students to help protect their identity and the content of their elec-

tronic communications. After a rigorous in-person credentialing process, customers retrieve their client certificate via a web-based interface which supports all the major browsers. Certificates are escrowed offsite with appropriate administrative checks and balances.

Technologies

WebISO uses the open source PubCookie system; UW-Madison was one of the Internet2 Institutions responsible for the development of PubCookie.

The PKI certificates are chained to a ubiquitous commercial Root Authority, the Equifax Secure E-Business CA1. DoIT uses a web-based interface to administrate the PKI system, for both certificate request granting and certificate management with GeoTrust maintaining their online CRL. Certificates can be encrypted and stored locally or stored on an Aladdin E-Token cryptographic token. DoIT supports S/MIME encryption and digital signing in various major email clients such as Outlook, Outlook Express, and Thunderbird in the Windows environment and Mail.app and Thunderbird in the Macintosh environment and also support digital signing of documents within the Microsoft Office suite.

The Future

DoIT is continuing to integrate WebISO with high profile applications including web mail, web calendaring and the portal, in support of their goal of true single sign on.

DoIT will begin offering digital signature capability on all outgoing mass emails to the campus community. Their philosophy is to be proactive with the adoption of PKI in sensitive applications across campus. The campus is currently considering an idea to unify its campus ID card systems and PKI is being considered as a potential solution in this scenario. The Public Health Information Network implementation at the UW-Madison is also considering using PKI to ensure compliance with their dual factor authentication requirement. DoIT will be conducting 6 month and 12 month implementation studies to determine how well PKI is meeting the needs of our end users.

DoIT is investigating the feasibility of a Kerberos service to provide client-server-based authentication services and as a possible solution to risks involved in allowing client access to LDAP.

Attributes**Methodologies**

A number of loosely coordinated interfaces and methods are used to manage campus systems that provide or consume IAM information or services. Entitlement information managed by the central IAM is currently hard-coded. Self-

CASE STUDY (CONTD.)

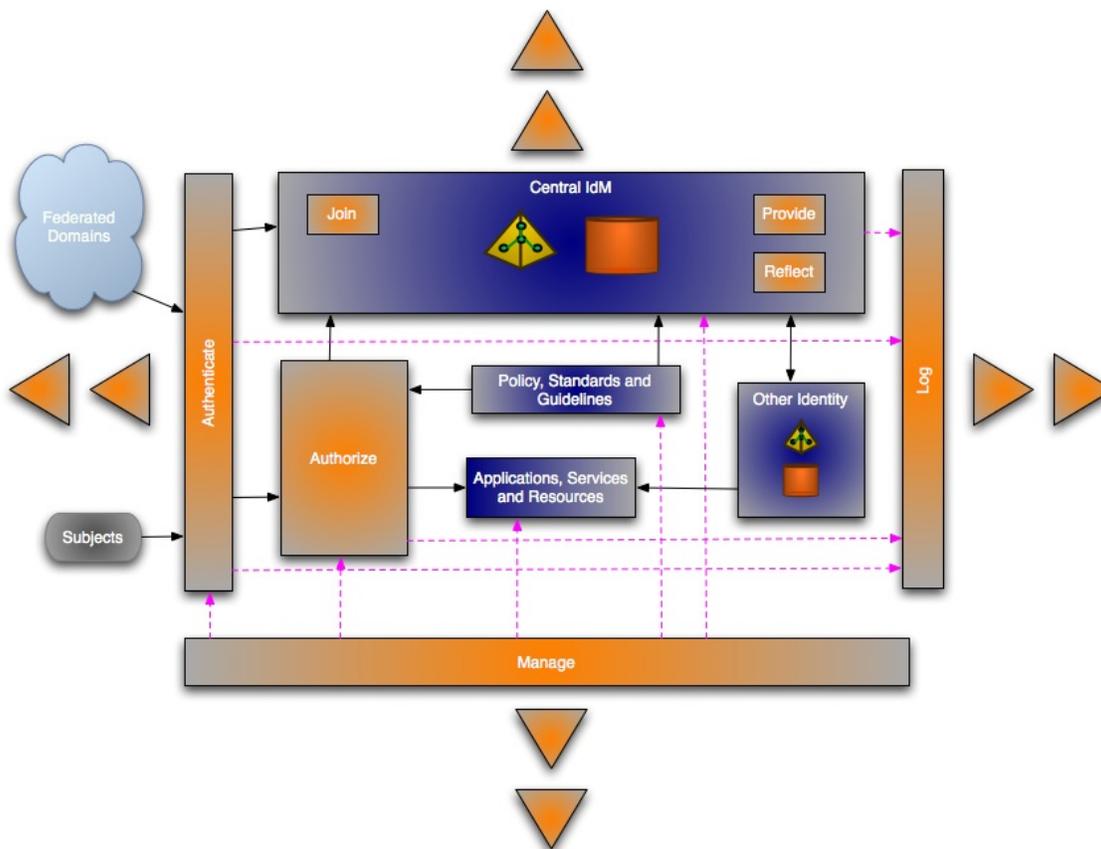


Figure 6: University of Wisconsin Division of Information Technology planned Web Services Identity Management Architecture. Source: UW DoIT *Identity and Access Management (IAM) at the University of Wisconsin-Madison*

registration and self-service password reset are provided for NetID. Self service provisioning and management of digital certificates is provided.

The Future

DoIT’s primary efforts in this area revolve around the creation of the Populations, Affiliations and Service Entitlements (PASE) system. This system will allow authorized individuals to define new user populations, group those individuals into affiliations and define and populate custom attributes. The system will also provide for the definition of services and the linking of these services to affiliations to create entitlements. Interfaces will be provided to allow service providers to easily determine who may have access to their service. A key feature of the system includes the expression of administrative roles and workflow functionality that will allow service providers and affiliation managers greater control and requiring less involvement by system administrators.

Auditing Methodologies

The UW-Madison Security group recognizes that log collection and analysis, including correlation of events is an

important tool in protecting University resources as well and ensuring and demonstrating compliance with governmental regulations and University policy. Currently, authentication events related to the centralized IdM systems are logged centrally. Individual hosts are responsible for logging authorization events.

Technologies

Currently, Windows event logs, Unix syslogs, and various application/web logs are in use. DoIT has netflows, centralized syslogs for some systems. HP Openview aggregates some events, but does not comprehensively address authentication and authorization.

The Future

DoIT is in the process of evaluating and considering a SEM (Security Event Management) systems that will correlate security related events occurring across systems. Their initial focus will be on authentication events.

APPENDIX A: GLOSSARY

Active Directory — A database that stores information about the locations of users, groups, passwords, and security information.

Attribute — A property which contains some value which describes a user.

Authentication — The process of validating an individual's identity.

Authorization — The process of granting permission to a user to access selected files or programs after the user's identity has been authenticated.

Biometrics — A technology for authentication which measures some physical property of an individual, such as retinal patterns, fingerprints, or ear geometry, and compares it to a recorded standard from that individual.

Certificate — A data record used in authentication. A certificate contains information about its owner and the issuing Certificate Authority's signature. It also contains the owner's public key.

Digest — A method of organizing information stored in a database for quicker access to each piece of data.

Entitlement — Access rights or restrictions assigned to a particular user or group.

Exchange Server — A server which controls email and groupware data.

External User — A user accessing network resources from outside the organization, such as via the internet or a virtual private network.

Federation — A system in which one entity trusts the authentication of a user at a partner entity's network.

Identity Store — A database or directory which stores digital identities and their associated attributes and credentials.

Internal User — A user accessing network resources from within the organization.

LDAP — Lightweight Directory Access Protocol. A protocol used to access directory listings from a database.

Middleware — A category of computer software used to integrate disparate computer systems within an organization.

NTLM — NT LAN Manager is an authentication protocol used in many Microsoft network protocols for authentication and may be used to facilitate single sign on and federation.

Orphan Account — An account which is no longer needed but has not been terminated.

Portal — A piece of the identity management architecture which handles the initial access to a network. Portals often manage authentication. They are also responsible for directing traffic to the appropriate resources.

Propagation — The automatic application of a new user's identity to selected directories and servers in a network.

Provisioning — The process of assigning users access to the system resources they need. Provisioning may be done on a role-based, rule-based, context-based, or mandatory-based system.

Registration — The initial step taken by either the user or the administrator when a digital identity is created for the user, often granting a username and password.

Security Auditing — Examining security logs to determine that aspects of identity management, such as authentication or authorization, are functioning as expected. Logs may also offer information about who accesses what resources and when.

Security Groups — Groups of users who share similar attributes and entitlements.

Single Sign On — A form of authentication which allows a user to sign on once and access all systems for which they have authorization.

Smartcard — A small, card-sized device which contains data. In terms of security, a smartcard typically holds an inaccessible private key for authenticating the owner.

SQL Server — A relational database server which uses the Structured Query Language (SQL) to access data which is stored in a dataset of tables.

Synchronization — The process of comparing the data about a user stored in multiple locations and updating the information at all locations to reflect the most current information.

Termination — Eliminating a user's account once it is no longer needed.

APPENDIX B: WHITEPAPER

WHAT IS IDENTITY MANAGEMENT

Identity management (IdM) is a system and associated processes and policies used to create and remove a user's digital identity and manage the user's ability to access electronic resources such as networks, files, or services. A user may be a credit union employee, member, or business partner. A user's digital identity, for the purpose of this project, is the identifier and attributes associated with either an individual or group of users.

IdM also includes the hardware and software that builds the architecture necessary to manage and maintain digital identities.

At credit unions, IdM is applied as a method of addressing electronic security issues. This may include tasks as simple as managing how an employee logs onto the credit union intranet to combating problems as complex as identity theft and federated networking.

WHY MANAGE IDENTITIES

Today, credit unions, along with other financial institutions, are facing the challenge of implementing effective IdM measures to protect their member, employee, and business partner data. The importance of effective IdM methods — coordinated across operations and business partnerships — to combat identity theft and manage valuable IT resources cannot be overstated.

There is no single solution to this challenge. Effective IdM involves coordinating a myriad issues, from risk management, legal and compliance, and technology issues to marketing considerations, reputation risk, and more.

THE IdM PROCESS

A digital identity follows a typical life-cycle. First, an identity must be created. In some cases, users are allowed to perform this first step, while in others IT administrators do the registration. Once the identity has been created, it must be propagated to relevant networks and databases. An identity, once distributed, begins the most involved stage of its life: maintenance and management. Maintaining an identity involves many factors which include provisioning, authentication, authorization, federation, synchronization, auditing, and entitlement. When an identity has fulfilled its useful life, it may be de-provisioned or terminated.

THE IdM ARCHITECTURE

Each step in the process of managing identities requires specific hardware and software elements. The simplest architecture may include a portal to manage log-on, databases and directories to store and reference identities,

directory services for managing roles and groups, and provisioning services to associate identities with programs and applications. An IdM architecture can be much more sophisticated, though, depending on the size of the credit union and the number of disparate networks and computer systems that must be integrated.

WHO SHOULD READ THIS PAPER

This paper is intended to accompany the Credit Union Identity Management Survey. It is written with survey participants in mind, and the structure mirrors that of the survey. The paper should be useful to anyone wishing to gain a basic knowledge of the Identity Management process and associated architecture.

CONTENTS

Pg.

21 Identity Management at Credit Unions

An overview of Identity Management and why it is important to the credit union industry.

21 The Identity Management Process

The four stages of the Identity Management life-cycle and how they can be leveraged.

23 Identity Management Architecture

A description of the typical components of an Identity Management architecture.

25 Best Practices

Best practices for both the Identity Management process and implementing an Identity Management architecture.

IDENTITY MANAGEMENT

The term Identity Management (IdM) describes a system and associated processes and policies to create, distribute, maintain, and terminate the digital identifier used to distinguish a user or group of users. This system utilizes specific hardware, software, and skilled professionals to actively manage how employees, credit union members, or federated business partners access IT resources.

Credit unions are currently implementing identity management in varying degrees. However, the advent of online banking, combined with existing techniques for utilizing networked electronics is increasing the demand for identity management services in this industry. The value of electronic resources such as computers, servers, networks, and the data stored within them, as well as recent increases in digital theft have propelled IdM to the forefront of information security discussion.

The Federal Trade Commission statistics indicate that identity theft is the fastest-growing crime in the U.S., and it shows no signs of diminishing. The FTC reports 27.3 million Americans have been victimized in the last five years, including more than 10 million last year. These alarming statistics lend credibility to the need for establishing effective and proven techniques for managing all the identities which may interact with the credit union's digital resources.

Also, the cost and importance of information technology infrastructure demands that these resources be securely protected. A good identity management system is one line of defense in preventing unauthorized access to critical business tools and sensitive data.

It is important that decision makers at credit unions understand the key concepts involved in identity management so as to best determine their organizations need for IdM and how to best address the concerns of their information security professionals.

THE IDENTITY MANAGEMENT PROCESS

Despite being one of the most complex information technology processes, identity management can be described using a life-cycle of only four stages: Registration/Creation, Propagation, Maintenance, and Termination. Additionally, the Maintenance stage includes several steps for managing the day-to-day use of digital identities.

The following figure depicts the four stages of the identity management life-cycle:



Figure 1: The four stages of an identity encompass how accounts and policies are managed. *Source: Burton Group, 2005*

Each of the four stages presents its own unique set of issues and techniques to consider.

1. Registration / Creation

The registration/creation step is the creation of a new user's identity. It involves assigning some unique identifier, such as a username or ID number, to the user and assigning some initial attributes to the new identity. These attributes may be related to the user's role within the credit union, an initial password, or security clearances. Once an identity has been created it is propagated to the appropriate databases or directories, which can be generally described as data stores.

2. Propagation

Once an identity has been created, it must be added to the credit union's identity management system. Depending on the system, propagation may require identity integration tools. In systems that include multiple data stores, middleware must be used to coordinate the identities of users which are stored in any of the separate identity stores.

The identity may be stored on a relational server or on a distributed directory. A relational identity store, such as a SQL server, typically provides increased data protection, ease-of-use, and flexibility while exhibiting slower retrieval speeds than a distributed directory. In a distributed directory, information is not stored at a central location. Instead, it is maintained on dedicated directory servers and synchronized between them. The distributed system allows users to access data from any of many computers with a single sign on.

3. Maintenance / Management

Following provisioning, an identity begins the major portion of its life-cycle. It must be maintained and managed. The maintenance and management stage is divided into Authentication, Authorization, Federation, Synchronization, Security Auditing, and Entitlements.

Provisioning

Once an identity has been created and propagated, it is provisioned. Attributes such as credentials, access rights, and entitlements are assigned to the identity. These attributes could include passwords, security clearances, and access privileges to certain resources. This information is typically stored in a distributed directory. Many IdM systems now use role-based provisioning, in which one of the initial attributes assigned to a new user describes their role within the system. The user's account is then granted access to a predetermined set of resources which are necessary to fulfill the duties of their role.

Authentication

When someone tries to access and utilize an identity, a check needs to be made to ensure that the user is who they say they are. This is authentication. A user's identity may be authenticated by any of many tools, and the best systems use several methods in combination. Some of the most common authenticators are passwords, certificates, and SSL. Biometrics is quickly becoming a popular method for authentication. Biometrics compares physical characteristics of a user, such as a retina or a fingerprint, to a stored standard. Presumably, since such biometrics are unique to an individual, this is the best method of authenticating a user. As the technology improves, a combination of biometrics and smartcards are expected to become the primary method of authentication.

Authorization

Authorization is the determination, by comparing the credentials associated with a user's authenticated identity with the security configurations of a resource, whether or not a user may access that resource or perform certain functions within it. These security configurations may be stored on a centralized server or in a distributed directory.

Entitlements and Attributes

Attributes are the individual data items that make up an identity. Entitlements are the pieces of data associated with an identity that tell system resources what the user is or is not allowed to do. Entitlements and attributes can be granted to individual users, but are more typically distributed to logical groups of

users such as particular departments or security clearance levels. For example, all employees who are accountants may be granted access to the company's financial records software, while being denied access to files detailing an upcoming marketing campaign. This style of entitlement allows for IT workers to make necessary changes more quickly and efficiently.

Federation

Federation works on the principle of digital trust. A user may authenticate at a certain sign-on point, but wants to access resources from another department, network, or business partner. In a federated network, the second service provider would recognize the authentication process of the first and would not require the user to sign-on with another set of credentials. Trust may be granted to individual users or to whole domains. In the credit union world, Automatic Teller Machines are an example of a federated system.

Synchronization

A type of identity integration, synchronization ensures that an identity is current at all data stores. Software may be used to check for changes in an identity's attributes and apply those changes to all the servers and directories where the identity is being maintained.

Security Auditing

Security auditing is an important and often overlooked segment of identity management. Audits may be done to test a system for security weaknesses or to check for possible recent security breaches. In the case of testing for security weaknesses, an identity management system is attempted to be broken into by a known and trusted source so that any flaws can be found and fixed before an actual malicious attack is conducted. It is also a good idea to maintain logs of user activities to ensure that the system is operating as expected. Some logging programs highlight suspicious activities and known security threats within a log.

4. Termination

Eventually an identity may no longer be needed. Rather than leaving the stale account to sit dormant and provide a possible outlet for system abuse or security breaches, the identity and all its attributes should be de-provisioned and removed from all servers and databases. This prevents users who may have changed from one class of user to another from accessing resources they no longer need. Termination also prevents employees or members who may have left the organization from having a possible way to access resources. Some IdM software will automatically de-provision or terminate identities when a user's role changes or is eliminated.

IDENTITY MANAGEMENT ARCHITECTURE

A significant amount of architecture is required to operate an identity management system. Most established companies have many disparate networks and data storage systems, and cobbling them together into a cohesive system that allows for automatic propagation, provisioning, synchronization, and other IdM best practices can be a complex and difficult task. Many different hardware, software, and middleware tools are required to maintain a functional, secure, and convenient system for accessing system resources. The following section details some of the architecture options associated with the different steps in the IdM process.

1. Registration / Creation

The creation of a new identity is typically taken care of using a combination of hardware and software at the portal level. The portal, which handles the initial access to a network, provides an interface for users to create new accounts and later to log-in. Once the user or administrator has input a unique identifier and some initial attributes, the identity is passed on for identity mapping.

2. Propagation

A new identity must be stored in the data-stores associated with whatever resources the user will be accessing. This step is illustrated in Figure 2 as “Identity mapping and referral.” These data stores may be relational databases such as SQL servers or a distributed system which utilizes LDAP. These directories will also hold the many attributes used to determine how a user should be allowed to access resources.

3. Maintenance and Management

As in the IdM process, maintenance and management make up the bulk of the architecture. This function can become exceptionally complex, as the roles of various architectural elements can be blurred across the process steps. Also, some IdM systems have additional requirements which necessitate more structural pieces or more sophisticated tools.

Provisioning

Provisioning is handled by provisioning services. These services are usually provided by a provisioning server which connects applications and resources with

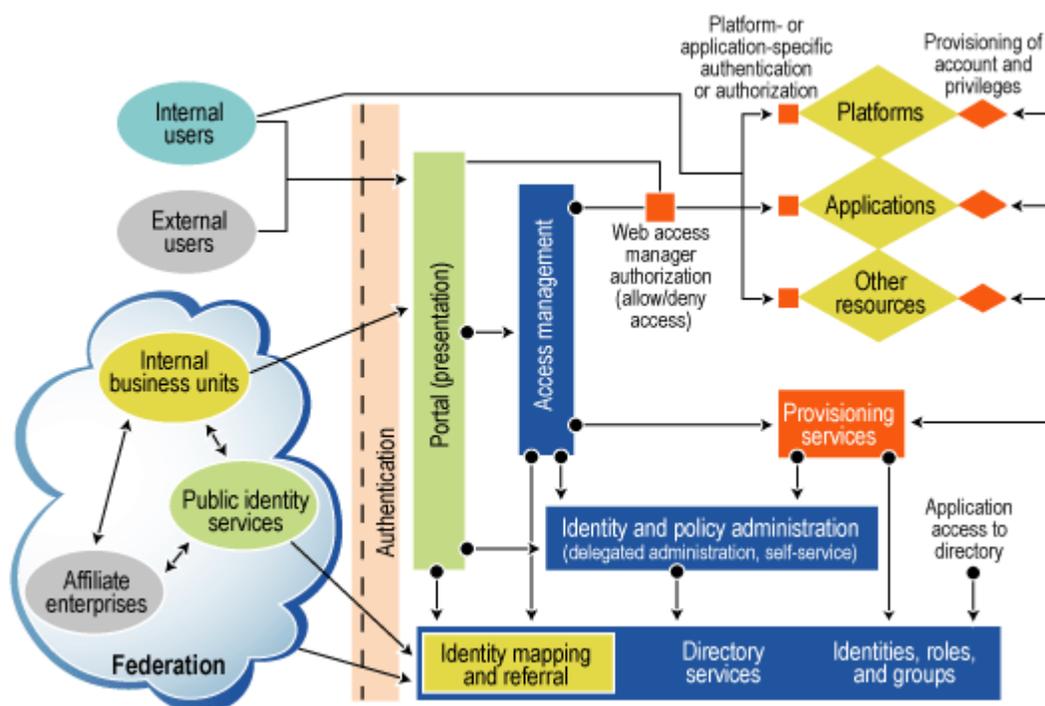


Figure 2: A typical IdM architecture showing elements for authentication, authorization, provisioning, federation, attributes, and other process steps.
 Source: Burton Group, 2005

the data-stores in which identities and attribute data are held. Provisioning services, as can be seen in Figure 2, are central to identity management; influencing security policies and role-based decisions while answering to authorization and application protocols.

Authentication

Authentication tools can be implemented at any step of the IdM process, however it is usually handled at log-in by either a portal or the web-access manager.

Portals offer a single interface for users to enter their credentials and be directed to the appropriate resources. A portal can be built to authenticate internal or external users, as well as federated partners. Portals come in three main varieties, which all present the user with a related set of information.

A web access manager (WAM) typically has more functionality and tighter security than a portal. WAM are usually integrated with portals though, so that each tool can complement the strengths of the other. A WAM, like a portal, requires minimal or no client software. Both utilize a policy server to connect users to resources using LDAP or SQL.

Authorization

Authorization is presented in Figure 2 as “access management.” After the portal, WAM, and policy server determine that a user is indeed who they claim to be, the authorization server accesses a users credentials and determines which resources to grant access to. The authorization server connects with all aspects of the identity management system to compare the user’s attributes and entitlements to those required by applications and other resources.

All users—internal, external, and federated—undergo some form of authorization.

Attributes and Entitlements

Attributes and entitlements are stored in servers or directories along with the user’s unique identifier. These values are used to provision an account and grant or deny access to resources during the authorization stage. It may be simpler and more secure to maintain all attributes in a single, centralized data-store, though it may be faster and more convenient for the user to store this data in a distributed manner.

Administrators can use virtual and meta-directory services to make updates to this information. It is also possible to implement some degree of automation in assigning attributes based on roles and rules.

Federation

Federation depends on domains accepting the authentication credentials of other domains. This is primarily performed using specialized software with existing servers, though dedicated servers can be used and may be needed to handle additional traffic. Once a user has been authenticated at their own domain, a request for authorization is placed at the resource’s host network. Depending on the level of trust established by administrators on either network, different attributes and entitlements may be granted to federated users. The information for these trusted partners is stored in the same way identities are stored for native users.

Synchronization

Specialized software connects the various servers and directories which store identity information. Depending on the size and age of a credit union, there may be a number of disparate data-stores which the synchronization software needs to update with the most current information for each user. Synchronization is necessary when identity management is aggregated, too, as user attributes can change from a number of sources. With delegated administration a user could change a credential, a password for example, from their cellular phone, laptop, or PDA. These many access points must be up to date with the requirements of a credit unions many digital resources.

4. Termination

Termination is handled in a similar manner to the provisioning, propagation, and creation steps. However, instead of granting attributes, a user’s account is stripped of credentials and entitlements and is deleted from the access granting data-stores. In some cases, an identity may be provided a new set access information. If a user account is no longer necessary, though, the most secure option is to terminate the profile completely.

ADDITIONAL RESOURCES

As mentioned, the architecture which supports the identity management process can be very sophisticated. Many resources exist which provide more background on the aspects of an IdM system. Microsoft, Burton Group, Forrester, and many identity management vendors offer detailed specifications of the specific tools which fulfill each of the mentioned architectural elements.

BEST PRACTICES

When implementing an identity management scheme, there are a number of best practices to help build an effective and efficient system. The following list outlines ten goals and techniques for developing an identity management program:

Governance

The credit union should create a governance board to set policies regarding identity management including passwords, access privileges, security standards, auditing policies, and software procurement. This will streamline implementation and should standardize administration practices. This will also help guarantee that the IdM system delivers what the credit union needs.

Authentication

Arguably, authentication is the root of identity management. Having a robust, reliable, and strong mechanism for authentication will create a more secure network.

Passwords

Passwords accompany authentication in terms of importance and leveraging the effectiveness of an IdM arrangement. Passwords should adhere to a system-wide policy with as much complexity as possible for as much security as possible. Also, users should be able to change their own passwords. This reduces the workload on the IT staff.

Single Sign On

Requiring users to remember many passwords encourages them to write hints or the passwords themselves on paper. This is a tremendous security threat and can be diminished by using a single-sign-on system.

Automation

Automating steps such as propagation, provisioning, and de-provisioning will reduce the strain on IT workers, and may free up enough resources to focus on IdM analytics and functions.

Scalability

The architecture involved in an identity management system should be extensible and flexible. It is important to plan for an uncertain future.

Convenience

Identity Management should be a transparent, simple process for the users. Single-sign-on and federation can reduce the number of times users are required to enter passwords, while smartcards, tokens, and certificates can perform authentication and authorization functions automatically.

Synchronization

Identity data should be aggregated and stored in a system which allows quick and easy synchronization to reduce log-in errors or access problems.

Auditing

An often overlooked aspect of identity management is security auditing. Real-time monitoring with automatic notifications, logging, and good filtering can be used to ensure that the IdM system is effective.

Role Based

Using a role-based provisioning system will drastically reduce maintenance complexities when employees change functions within the credit union.

APPENDIX C: ACKNOWLEDGMENTS

Special thanks to Sue Racine, Tammie Kovacs, David Meunier, Mark Meyer, Dan Wallen, and Chris Rowland of CUNA Mutual Group, David Rohn, Cheryl Sorenson, and Doug Benzine of CUNA & Affiliates, April Clobes of the Michigan State University Federal Credit Union, Lorraine Zerfas of the Education Credit Union Council, Remar Sutton of Remar Sutton & Associates, Kelly Dowell of the Credit Union Information Security Professionals Association, and Ron Broaddus of the Greater Nevada Credit Union for their expertise and support throughout this project. Also, thank you to focus group participants Tim Keran of Teacher Federal Credit Union, Tom Giangreco of Orange County Teachers Federal Credit Union, Doug Fox of Heritage Community Federal Credit Union, Patricia Kelly of Spokane Teachers Credit Union, and Ed Machiado of National 1st Credit Union for their time, expertise and opinions. Thank you to Mairead Martin, Craig Dunigan, Mike Roszkowski, Keith Hazelton, and Steve Devoti of the University of Wisconsin Division of Information Technology for their technical support. Also thank you to Mairead Martin for her participation in the identity management case study. Finally, thank you to all of the survey respondents for taking the time to share their views of Identity Management in the credit union industry.

APPENDIX D: REFERENCES

- Wikipedia. (2005, September). http://en.wikipedia.org/wiki/Identity_management
- Google. (2005, September). Define function.
<http://www.google.com>
- Blum, Dan, Burton Group. (2005, August). Identity Management: Federated Identity
<http://www.burtongroup.com/ImageEmitter/ImageEmitter.aspx?action=PDF&cvid=792>
- Devoti, Steve, CUNA Mutual Group. (2005, August). Identity Management Concepts
- Microsoft. (2005, August). Microsoft Identity and Access Management Series
<http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/default.msp>
- Oracle. (2005, April). Buyer's Guide for an Access and Identity Management Infrastructure
- M-Tech. (2005). Defining Enterprise Identity Management
<http://idsynch.com/docs/identity-management-defined.html>
- Blum, Dan, Burton Group. (2004, December). Identity Management: Principles
<http://www.burtongroup.com/ImageEmitter/ImageEmitter.aspx?action=PDF&cvid=679>
- Martin, Mairead, University of Wisconsin—Madison Division of Information Technology. (2004, August). Evolution of the University Directory Service (UDS)
- Blum, Dan, Burton Group. (2004, June). Identity Management: Templates
<http://www.burtongroup.com/content/download.aspx?cid=129>
- Ali Pabri, Uday O. (2003, September). Role-Based Access Control
http://www.certmag.com/articles/templates/cmag_department.asp?articleid=370&zoneid=63

About UW E-Business Consortium

The UW E-Business Consortium (the industry membership base of the UW E-Business Institute) is Wisconsin's premier organization that helps companies gain a competitive advantage through e-business. Our members - business executives and senior managers from the Midwest's leading companies - tap into world-class university resources and the collective experiences of this B2B and B2C group to address and share strategic e-business and information technology challenges, best practices and lessons learned.

For more information, contact Assistant Director of Member Relations, Christina Paschen (608) 265-0645 or clpaschen@wisc.edu