Identity Management in Higher Education - A View of the Landscape

Identity Management in Higher Education: A View of the Landscape - June 17, 2013

1. Executive Summary

In February of 2013, the InCommon Technical Advisory Committee was charged with developing "...a document that presents the landscape of identity-related projects of particular relevance to the Research and Education (R&E) community, including information about their state, the relationships among them, and gaps among those relationships and between the capabilities they provide and what is needed by this community." During the Spring 2013 Internet2 Meeting there was a face-to-face meeting with the InCommon Steering Committee. At that time the charge was broadened; the Steering Committee requested that the document also serve to engender discussion within that group on substantial identity management issues related to Higher Education.

This is that document. It presents a functional view of the identity and access management landscape, highlighting projects of particular relevance to the R&E community, as well as alternative "lenses" onto the landscape to highlight implications for CIOs and their constituencies. It also provides several observations and recommendations for discussion in the Steering Committee.

Institutes of higher education and research are complex, highly dynamic, non-hierarchical organizations where people often have multiple simultaneous roles and relationships. Off-the-shelf identity and access management solutions do not generally meet the needs of higher education and research. In a very real sense, higher education is leading the creation of identity management solutions because it has to.

We are now at a "Henry Ford" moment in the creation of these services, moving from custom built solutions to "assembly line," off the shelf solutions and an entire ecosystem that will scale well beyond the early adopters. We have identified the following issues as particularly important to our next steps:

1. Many universities are struggling to implement effective identity management programs. They need help with:
   - Organizational structure
   - Value and risk assessment
   - Business process, and
   - Technology support.

2. There are multiple opportunities for InCommon and Net+ to extend the reach of identity and access management. Examples of these opportunities include:
   - Champion interface standards to facilitate deployment of new services,
   - Support global interfederation efforts to extend our federation efforts beyond national borders,
   - Foster the creation of usable federated applications to facilitate acceptance by end-users,
   - Leverage identities that people bring with them to higher education for efficiency and to improve user experience, and
   - Enhance privacy and security of identity information.

3. The CIFER project is in a unique position to coordinate the broad range of identity management related projects to assemble a comprehensive but modular set of identity and access management solutions that are suitable for use by universities in a cost-effective manner. Active engagement with the project will be required to meet this goal.

4. InCommon must continue to evolve its charter and its service profile to meet these challenges, particularly for the next round of new members, which will be smaller institutions with more limited resources than the early adopters.

This paper explores these issues, providing specific recommendations for InCommon and Net+. Priorities for these recommendations will need to be determined, and selected recommendations will require further effort and resources to define and execute specific actions. This is only the start of an ongoing strategic planning process for InCommon, and this paper is intended to be a living document, revised in the future to support that ongoing process.

2. Identity in Higher Education

Online services are growing rapidly. Universities are creating their own local services, but are also adopting cloud services into their IT portfolio, provided both commercially and by other universities. The size of that portfolio for a typical university could easily number in the hundreds of services. A small sampling includes:

- Massive Open Online Courses (MOOCs)
- Inter-institutional research collaboration
- Large and specialized resources in support of research (compute clusters, telescopes, LHC data, etc.)
- Library systems
- Grant administration systems
- ERP systems for human resources, financials, and student enrollment, etc.
- Systems for operational efficiency in multiple administrative areas, such as parking, benefits, prescription management, etc.
All of these require robust identity and access management. Over half of EDUCAUSE's Top Ten IT Issues for 2013 require identity and access management:

- 1 - Leveraging the wireless and device explosion on campus
- 2 - Training the workforce for the digital world
- 3 - Developing an institution-wide cloud strategy to help the institution select the right sourcing and solution strategies
- 4 - Facilitating a better understanding of information security and finding appropriate balance between infrastructure openness and security
- 5 - Determining the role of online learning and developing a sustainable strategy for that role
- 6 - Supporting the trends toward IT consumerization and bring-your-own device
- 7 - Transforming the institution's business with information technology

A well-integrated, robust identity management infrastructure is crucial to the success of progress on these issues. Universities require ERP-class identity management systems in order manage identities from multiple sources; perform identity proofing and registration; authenticate users during online sessions; maintain accurate and timely identity information; administer affiliations, groups, roles, and permissions; provision users into applications; and support audit and certification activities. (For more information about identity management systems, see the "Identity Management Functional Model" section of the InCommon Identity Assurance Assessment Framework.)

Not only must each university operate an enterprise identity management system for its community members, but organizations and service providers must simplify the integration of their identity and access management systems and federate their services internationally to enable the rich ecosystem of Internet-accessible services that has only begun to grow. Failure of these IDM systems means the unavailability of hundreds of services.

### 2.1. Why Must Higher Education Address This Issue?

Institutes of higher education and research are complex, highly dynamic, non-hierarchical organizations where people often have multiple simultaneous roles and relationships. The organizations are distributed, have varied funding models, and have a high degree of inter-institutional collaboration. Commercial IDM software currently addresses the typical company use cases rather than the campus ones. For example,

- A typical company, even a very large one, can populate its identity management system from a single source, its human resources system.
- Universities have a multitude of overlapping identity sources that must be matched and merged to identify duplicates and enhance information that is available from only a subset of the sources. The matching and merging algorithms must also accommodate the varying business processes and identity proofing requirements of the different sources. Examples of a university’s identity sources include:
  - Human Resources
  - Student System/Registrar
  - Alumni organizations
  - Admissions
  - Library
  - Sports teams
  - Student organizations
  - Donors
  - Parents
  - Health care professionals and clinical faculty
  - Continuing Education Programs (non-credit and certificate)
  - Temporary guests (sponsored and unsponsored)
- A typical company assigns roles and responsibilities in a hierarchical and controlled manner. The vast majority of people have a single position and role. Universities, in part due to the multiplicity of identity sources, are non-hierarchical, highly dynamic, and delegation is highly distributed.
- Common situations include a person who is in multiple Roles (e.g., both faculty and staff (and parent), or staff and student).
- A typical company has a well-defined set of business partners. Universities create partnerships on a daily basis, at all levels of the organization, without signed legal documents or administrative review. These partnerships may be long- or short-lived, but they can rarely afford significant delays to begin their work once the partnership has been formed.
- A typical company can manage credential assurance in a homogeneous way, whereas universities have diverse needs for assurance and multi-factor among their diverse constituencies. Universities must also often address the "not physically present" situation.
- A typical company has employees, and perhaps a few sponsored identities. Universities track identity for a vast range of relationships of varying "strength". There are core community members (e.g., faculty, students, staff). But, there are also "students" taking non-credit online courses who may be on a different continent. An IDM system needs to know what a person's relationship is and assign permissions appropriately; it also needs to impose appropriate requirements (e.g., for account activation and multifactor authentication).

Commercial identity and access management solutions have, naturally, conformed to the needs of the marketplace, leaving higher education with off-the-shelf tools that do not fully meet their needs. The most successful enterprise identity management systems in higher education are often home grown, and most using off-the-shelf software require significant local customization. This is particularly acute at smaller institutions and those with tight budgets, small staffs, and narrower staff skill sets. Other challenges include:

- Multilateral federation, required for multilateral collaboration, is nearly nonexistent outside of higher education and research. Commercial federating software typically supports only bilateral Federation.
- IT shops are often unprepared for the delivery of identity management as a business service, as opposed to technology.
- Organizational change may be required to achieve alignment with information security, source system administrations, departmental service providers, etc.

Projects aligned with higher education such as Shibboleth, Grouper, InCommon, and Kuali are improving this situation, but there is still much to do.

Ian Glazer, Research Vice President and Agenda Manager at Gartner, recently addressed these issues for the identity management industry as a whole in his thought-provoking video presentation, Killing IAM in Order to Save It. He observes that:

- Enterprise identity's world is fairly static. It does not match the richness of the contemporary web.
- IAM is "apart" from, not "a part" of, business services.
- Our descriptive language for identity management information, typically hierarchically-constructed LDAP directories and CSV files, is not rich enough to describe the more graph-structured nature of the web.

He says that IAM must "die and be reborn." It must become:
Governance models fall into the following basic categories:

- Priorities are set by the sponsors, typically to support a specific purpose. Ten of the respondents have some variant of this model.
- Sustainability models fall into the following basic categories. There is often a mix of strategies for a single project; only the primary strategy is tallied below. Fee-based sustainability models tend to be associated with the more mature activities with well-understood scope and value that is easily identifiable to their direct beneficiaries. Identity management’s current state of the art, however, often requires work that has not yet proved its value to beneficiaries. When this is the case, we tend to see grant-funded and volunteer-based strategies.
- User Fees. A fee is levied on project participants. Two of the respondents are supported in this manner.
- Sponsored. The project is funded by a grant from a sponsoring organization, which may be time-limited or ongoing. Six of the respondents are supported in this manner.

Higher education has been building this reborn successor for years. Mr. Glazer’s comments provide confirmation that we are moving in the right direction.

A decade ago Higher Education was able to define and promulgate common standards and practices, as well as deploy common software to support those standards. The rising use of cloud-based commercial services serving both commercial and campus customers, however, means we must collaborate increasingly with commercial providers in the future. Higher education is no longer in complete control of its destiny. Mr. Glazer’s comments provide confirmation that we are moving in the right direction, and reason to believe that our commercial collaborations will be fruitful.

Henry Ford and Identity Management for the 21st Century

When Henry Ford entered the automobile industry, custom cars of exceptional quality were being produced by highly-skilled craftsmen in small numbers. The people who drove cars were very enthusiastic about them, understood their inner workings intimately, had high tolerance for unpaved roads, knew proper etiquette when meeting other drivers, and carried their fuel with them. Now, people drive cars because they have to, have mechanics to fix their cars when they break (and AAA to tow their cars to their mechanics), complain about bumpy roads, must demonstrate knowledge of driving and the laws governing it, and there are gas stations everywhere.

We are at that Henry Ford moment in the maturity of identity and access management. We need not only software, but also support services, common policy, certification services, and well-paved paths to success. In order to reach thousands of institutions and tens of thousands of services, we must move beyond the current custom model for identity management systems.

3. The Process We Used

In support of Internet2’s effort to develop an identity strategy, a group was charged to develop a document that presents the landscape of identity-related projects of particular relevance to the Research and Education (R&E) community, including information about their state, the relationships among them, and gaps among those relationships and between the capabilities they provide and what is needed by this community. This Identity Landscape document is intended to provide information as input to strategic decision making by those providing leadership to the identified projects and to promote increased coordination among them. It is written with those audiences in mind, though we also expect it to be shared widely with the R&E public.

In order to collect the information in this document, we have employed two approaches:

- First, we created a short questionnaire and sent it to the leadership of over 40 open source, non-commercial projects of particular importance to identity and access management for higher education and research. The responses provided us with broad information about these projects’ goals, structure, funding, and challenges. The questionnaire and the responses we have received are contained in the appendices of this document.
- Second, we conducted a structured discussion with thought leaders in the field of identity and access management, both inside and outside of higher education. This has provided us with a valuable perspective, external to the authoring committee, on present and future trends and challenges we should pay attention to. In particular, this discussion highlighted the challenges that many non-R1 campuses will face in deploying and supporting a modern identity and access management infrastructure.

4. What We Learned

This section summarizes the information that has been gathered from the project survey, as well as through discussions with identity thought leaders. Also included are "Likely Trends and Concerns" that were raised by the members of the identity landscape project team.

4.1. Project Survey Results

In general, our survey has revealed a rich set of interrelated activities, all serving to address important issues facing identity management in higher education. There is good knowledge among the leadership of these activities of interfaces and touch points with other activities and, for the most part, there are resources available to achieve goals, although often not as quickly as desired. Governance, funding, and sustainability models vary and are, at times, challenges for the projects. Also, differences in those models hamper inter-project collaboration at times.

The following subsections discuss various aspects of the questionnaire.

1. Governance. Governance models fall into the following basic categories:
   - Open Source Meritocracy. Priorities are set, to a large degree, by the interest and availability of developers, in the classic manner of an open source project. There is typically group review of decisions by lead developers, as well as an expectation that developer interest and availability are driven by concrete use cases. Eight of the respondents have some variant of this model.
   - Managing Sponsors. Priorities are set by the sponsors, typically to support a specific purpose. Ten of the respondents have some variant of this model.
   - Independent Formal Organization. An independent organization exists to govern the activity. Four of the respondents have some variant of this model.

2. Sustainability. Sustainability models fall into the following basic categories. There is often a mix of strategies for a single project; only the primary strategy is tallied below. Fee-based sustainability models tend to be associated with the more mature activities with well-understood scope and value that is easily identifiable to their direct beneficiaries. Identity management’s current state of the art, however, often requires work that has not yet proved its value to beneficiaries. When this is the case, we tend to see grant-funded and volunteer-based strategies.
   - Value Delivered to Volunteers. The project delivers high value to its participants. Participation is voluntary, but the value brings volunteers. There is often a contribution of the collaboration infrastructure from a sponsoring organization. Eleven of the respondents are supported in this manner.
   - Participant Fees. A fee is levied on project participants. Two of the respondents are supported in this manner.
   - User Fees. Users of the service/product are charged a fee. Three of the respondents are supported in this manner.
   - Sponsored. The project is funded by a grant from a sponsoring organization, which may be time-limited or ongoing. Six of the respondents are supported in this manner.
3. **Common Issues.** The common issues faced by these projects tend not to be those the projects were created to address, instead the following are common threads.
   - **Misalignment of governance and sustainability models.** Differences in governance and sustainability models can hamper inter-project collaboration. This has been mentioned in relation to CIFER, Grouper, and Internet2.
   - **Obtaining stakeholder input.** This is often an issue when there is no formal governance structure. This can often result in a project that loses support over time, as potential volunteers and stakeholders do not see value.
   - **Long-term sustainability.** This is, of course, a concern of any project, but it particularly true to those supported by time-limited grants. Sometimes the time limit matches the need for the activity, but sometimes some other organization will need to pick up a project if it is to continue.
   - **Available expertise.** Many aspects of identity management are complex and not yet understood broadly; there are currently very few true experts. Multiple projects mentioned the difficulty of finding participants with expertise in this field.

4.2. **Identity Thought Leader Discussion Results**

The following issues were identified in discussion with identity thought leaders and the authoring committee for this report.

1. **Organizational Preparedness.** Many institutions have difficulty launching and maintaining an effective identity management program. There may be issues of funding, expertise, and alignment among business units within the organization. What should InCommon be doing to inform campus CIOs of the federation’s strategic directions, as well as to help those CIOs be prepared to leverage those strategies? How do campus CIOs gain access to consulting services that understand Higher Ed’s needs, rather than fitting Higher Ed into products that do not fit its needs?
2. **BYO Identity.** Most people now enter institutions of higher education with existing credentials, some high assurance but most low (e.g., from Facebook or Google). What role should these credentials play in our landscape? How can these identities be linked with information maintained by the institution?
3. **Assurance for Social Identities.** This is an issue both for BYO Identity, as well as the social identity gateways that are starting to be deployed. What level of assurance should we associate with such identities? Are there ways to raise our trust in low-assurance credentials?
4. **Assurance Requirements for Online Courses.** Universities are increasingly providing course credit to students they never see. What are appropriate assurance levels for participation in such courses?
5. **Vendor Compliance with Standards.** Identity management is often not considered in RFPs and service contract negotiations; it is more often addressed as an integration issue during implementation. Because it is relatively new, federation is often precluded by this approach. How can we make federation a selling point for more vendors?
6. **Alignment with Evolving Standards.** OAuth2 and OpenID Connect represent standards that have broad industry attention, and overlapping capabilities with the standards used by InCommon. They also have very large players like Google behind them. What are the appropriate strategies for alignment with these and future protocols?

4.3. **Likely Trends and Concerns**

The following issues were raised in internal discussions of the identity landscape project team.

1. **Integration of NetPlus providers and campus IDM systems** continues to be a challenge. Most NetPlus providers have technical solutions targeted at the consumer market, and are not prepared for institutional programs in a federated environment.
2. **Crossing Institutional Boundaries.** Research, instruction, and even administration are increasingly contained within institutional boundaries. How can we deploy institutional services that support delegated management of distributed authorization? How can we deploy a common, standardized approach for provisioning, authentication, and authorization for cloud based applications?
3. **Managing Different Types of People.** How do we support growing sets of people who have only loose relationships with the campus? How do we provide scalable identity vetting and proofing for students taking online courses for credit? How do we provide services that span K-12 and applications that span those periods of life (e.g., portfolio)?
4. **Extending the Reach of Federation.** What should we be doing to increase participation in the federation, both by institutions and service providers? The first 200 InCommon members were relatively easy, as they have the resources to innovate and require relatively little support; how do we include the next 2000 members?
5. **Evolving Awareness of Privacy.** What can be done to preserve privacy while maintaining usability and scalability? With help from FaceBook, users have become increasingly aware of how many commercial service providers collect and then share both PII and usage patterns.
6. **This Stuff Can Be Hard on End-Users.** How can we hide the complexity from end-users without sacrificing security? Delegation of authority to manage groups and permissions is part of the model that will be used to achieve scalability. However, User Interfaces for those tasks are still primitive, and the concepts are foreign to many users.
7. **Identity Assurance.** What do campuses need to do to prepare to assert higher levels of assurance for their community members? Upgrading business processes and deploying multi-factor authentication are common issues.
8. **Tools in Support of Audit, Attestation, and Other Reporting.** These tools exist commercially, but are often not implemented in research and education.
9. **Difficulties configuring commercial products (e.g. Active Directory) for FICAM standards.** FICAM’s “real security” approach has sometimes set the bar so high that campuses have to reconfigure their AD environment and remove less secure functionality that is relied on.

5. **Observations and Recommendations**

5.1. **Organizational Preparedness**

Many institutions are struggling with various aspects of identity management.

1. As a business service, as opposed to technology, identity and access management is often difficult to place within the technology support organization (or within the campus organization). From the campus perspective, Identity Management will probably have a broader definition than just digital credentials. It also may require partnerships with other organizational units that have not existed in the past. Examples of service roadmaps, organizational structures, and funding strategies, particularly targeting a management audience, are needed.
2. Owning and operating the technology that supports identity and access management is not cheap, particularly for smaller institutions.
3. There is little awareness of the issues surrounding identity assurance, or its value and risks for a campus.
4. Service providers, such as online course providers, are often unaware of risks associated with incorrect identification of their users, independent of whether the services are internal to an institution or are federated.
5. There is a growing linkage between identity and access management and aspects of security management. Organizations should ensure that there is sufficient and appropriate communication.

**Recommendations**

1. InCommon should provide campus CIOs with a roadmap showing federation-wide strategic directions on a regular basis, including sequencing and a timeline. This roadmap should include the value for member institutions, as well as the expectations placed on those institutions.
2. InCommon should provide campus CIOs with documentation, case studies, templates and other tools to help CIOs create local roadmaps for identity and access management. This should include information about the business value derived from implementing the steps in the roadmap.
3. InCommon should work closely with the CIFER project to ensure that a high-quality, comprehensive and modular set of tools is available for easy, cost effective adoption by institutions.
4. InCommon should foster the adoption of common institutional policies and practices for identity management that are supported by pre-configured, readily-deployed CIFER distributions. In general, InCommon should be developing strategies that bring “Henry Ford IDM functionality” to the US Higher Education community.
5. InCommon should explore the viability of “Identity as a Service” offerings, either from InCommon or other third parties, leveraging a “CIFER Certification” for customers that adopt common institutional policies and practices for identity management. (As Henry Ford said, “Any customer can have a car painted any colour that he wants so long as it is black.”)
6. InCommon should provide campus CIOs with documentation showing the issues, value, and risks of identity assurance.
7. InCommon should provide service providers with an easily understood risk assessment tool to help them select appropriate assurance profiles.

5.2. Extending the Reach of Identity Management and Federation

The concepts of identity management and federation continue to expand and adapt to support new ways of providing services to our community. We need to identify and support opportunities for increasing the reach of our efforts to other communities, as well as new applications. The following are examples of where this is an issue:

1. Cloud services, especially, lack standard interfaces and practices for provisioning and deprovisioning, and for managing access. Campuses will only be able to use the growing portfolio of Net+ providers if those providers share a common set of interfaces for provisioning and authentication. Otherwise, campuses will not have the resources required to implement custom interfaces for each provider.
2. Commercial IDM products do not meet the identity, role management, and provisioning needs of campuses; using them on a campus often requires significant customization.
3. Campuses require powerful group management capabilities that can define both ad hoc groups and groups based on affiliation and other identity attributes, while providing the ability to manually “fine tune” group membership to conform to ad hoc requirements. It must be possible to delegate administration of groups in a very distributed fashion, and it must be possible to extract group memberships from the system for provisioning into applications, both locally and in the cloud.
4. Interfederation (including edugain and eduroam) provide the ability for US campus community members to operate effectively in a global environment.
5. Bring Your Own (BYO) Identity and/or Credential. Today everyone being issued a digital identity by a campus already has an identity issued by one of the “social providers” (or, soon, by COMMIT). The NSTIC initiative is promoting an Identity Model that includes both Identity Providers and Attribute Providers. Campuses are beginning to leverage social identities with applicants, parents, and online students in non-credit courses. NSTIC and OASIS also have efforts underway to deploy business processes and technology to elevate the Level of Assurance of social identities to a level that would be acceptable for business transactions at banks. It is likely that over time campuses will stop issuing credentials and instead rely on elevated social identities. Campuses will then become Attribute Providers, associating attributes such as Affiliation=Student to a social identity.
6. Applications and services often do not federate well, or have poor usability because of poor UI support for Federation.
7. By 2011 half of all devices shipped were mobile, and the PC was in serious decline in terms of market share. Applications on mobile devices, however, generally do not support the federated authentication protocols currently supported by campuses.
8. InCommon has not developed many of the support services that are often provided by other national federations that were funded to address the needs of all universities and colleges. InCommon was created by R1 universities. Because the R1 universities have the resources to innovate, as well as a relatively low need for support, In order to address all US Higher Education, and other communities like K-12, a broader range of services will be needed. Participation by the full range of institutes of higher education and research in the US will require many steps, including the following:

**Recommended Actions**

1. InCommon and Net+ need to be champions for standard interfaces, particularly for provisioning, deprovisioning, authentication and authorization. This will likely engender the development of standards, design patterns, and tools for use by software service providers. InCommon and Net+ should foster the creation of education and tools to assist application developers in building usable federated services. This will likely need to include usability studies of federated applications to determine good design patterns.
2. InCommon should continue to support the creation and coordination of open source efforts, such as Shibboleth, Grouper, and Kuali KIM, that enable and extend identity management’s applicability in higher education and research.
3. InCommon should continue to support efforts in support of interfederation (including edugain and eduroam) in order to enable global collaboration and access to services.
4. InCommon should facilitate pilots using standards that are becoming increasingly prevalent among commercial Internet services and some campus-based services.
5. InCommon should continue to track and support efforts to assess and, where appropriate, leverage identities and credentials that are administered by entities that are external to InCommon, particularly social identity providers.
6. InCommon should track and, where appropriate, foster the deployment of solutions for mobile devices that support federation.
5.3. Overlaps (Or the Lack Thereof) and Eliminating the Gaps

As has been mentioned earlier, the leadership of research and education's open source identity management activities have good mutual knowledge of the other activities that touch on theirs. Information is shared readily, so there is not a lot of overlap. This is different from the commercial space, where competition fosters extensive and intentional overlap among multiple vendors’ product suites. When there is overlap in the open source space, the normal "open market" process identifies the leaders, and redundant efforts are retired; forking of projects is unusual in this space. For example, there was a time when many institutions were building home-grown web single sign-on systems; now CAS and Shibboleth are the clear leaders.

The following projects warrant further discussion:

- **CAS, Shibboleth, and SimpleSAMLphp.** While all are single sign-on systems, they address different situations. CAS protects applications used within an enterprise and is typically managed by application administrators. Shibboleth addresses both federated and enterprise applications but is typically managed by systems or platform administrators. SimpleSAMLphp integrates directly into application code, and can be used without any system administrator involvement. Bringing some of CAS's "developer friendliness" to Shibboleth would be helpful. Both CAS and Shibboleth have large installed bases; it would be difficult to replace one with the other. It is common and simple for CAS and Shibboleth to be used together.

- **Grouper and Kuali Rice KIM.** Both Grouper and KIM manage groups and permissions. What distinguishes KIM from Grouper is that it is optimized primarily for the specific set of Kuali applications (although can often be used outside of that application sets), whereas Grouper is agnostic about the applications it manages. Organizations that use Kuali applications need KIM, and organizations with a more heterogeneous technical environment need Grouper.

A glance at the list of projects under nearly every category in Appendix - Introduction to the Identity Landscape will show apparently overlapping projects. In actuality, they often reflect the multifaceted nature of each category. While one could envision a single, all-encompassing solution for each category, that is not achievable in practice. Multiple cooperating activities are often the best way to address these complex issues.

The CIFER project provides an opportunity to establish common functional standards for interfaces among the components of identity and access management systems, enabling alternative components to be used as appropriate for the environment. It also serves to fill gaps; software to implement person repositories and to provision services are specific needs that CIFER is addressing.

The various IAM software, like most open source software, requires local technical expertise and operational effort to deploy, which may put it out of reach for many of the smaller institutions. There is an opportunity here for third-party support.

### Recommendations

1. InCommon and CIFER should monitor their support of projects regularly to leverage other activities in order to make the most effective use of resources.
2. As mentioned in the Organizational Preparedness section, InCommon should foster common CIFER configurations of IAM software and explore the viability of third-party "Identity as a Service" offerings.

5.4. Governance and Financial Sustainability

Different governance and financial sustainability models seem to work better or worse for different types of activities.

- "Heavier" models for governance and sustainability tend to work best for activities that address well-known operational issues with well-understood scopes and costs. Kuali and InCommon, for example address such well-known issues, and they are governed by independent formal organizations or managing sponsors and are funded by participant and user fees.

- Projects that push the envelope generally require "lighter" models. Projects, like Grouper, with an emphasis on innovation do not typically develop well-understood scopes or costs until later in their lifetimes. They typically work best with governance models like open source meritocracy, and are sustained through sponsorship and/or value delivered to volunteers.

As identity and access management matures, projects like CIFER can help move IAM software from one governance model to another especially as it transitions from innovation periods into operational periods. This will likely cause strain in the ecosystem, as governance and financial sustainability (and cultural) models can collide. Such strains, however, are not new to the open source world, so there is hope. Linux distributors like Red Hat and Ubuntu have had great success in this over the years.

5.4.1. Governance and Financial Sustainability for InCommon

InCommon falls in the category of an activity that addresses well-known operational issues. However, InCommon's charter is evolving over time, and may expand to include both service and development aspects. In addition, the membership profile with respect to required support services is changing. Finally, InCommon itself continues to be an agent of change, supporting innovation and development efforts. InCommon must continue to adapt its service portfolio to these changing circumstances, using an appropriate governance model for various activities.

### Recommendations

1. InCommon should adopt an effective portfolio management strategy that balances the needs of its increasingly diverse membership while continuing its mission of innovation.
2. This document is the start of a strategic planning process. An appropriate strategy for maintaining this document's currency should be part of that process.
6. Appendix - A Functional Model of the Identity Landscape

6.1. The Global Perspective

Identity management for research and education is a complex web of players and interactions. Campuses are the stewards of identity information about the people in their communities. They manage identity for their community members and people with various relationships, do identity vetting (perform a Registration Authority role), issue credentials, and manage Roles, attributes, permissions, and provisioning. Identity Federations, often organized around national boundaries, are collections of campus identity providers and service providers that consume that identity information to deliver their services; Federations rely on a common policy and technical framework. Interfederation provides the policy and technical framework allowing operation across Federation boundaries. There are also many service providers that are not federation members.

This appendix describes the chief elements of identity management for higher education and research, along with current activities (by projects and organizations) that are related to each. Since this is such a complex field, the following appendix, Implications for CIOs, provides alternative views of the identity landscape to highlight the implications for CIOs and their constituencies.

Note that a comprehensive market survey was not within the scope of this project. This is a rapidly developing market segment, and there are many more activities in the world that could be listed here. Cloud service providers are growing particularly rapidly. We have tried to be selective, primarily listing open source activities with direct impact on higher education and research.

6.1.1. Federations

Federations exist to enhance trust among their member institutions and service providers. Each federation provides a legal, contractual, and technical infrastructure that enables the controlled exchange of the institutions’ identity information within the federation to support inter-institutional collaboration and access to services and resources within the federation.

R&E federations are coalitions of institutions with common interests, and nearly all utilize interoperable technologies based on the Security Assertion Markup Language (SAML) suite of standards. Because of the legal and contractual aspects of a federation’s infrastructure, however, federations tend to be comprised of institutions that share a common legal framework; their members generally exist within national borders. We are starting to see inter-federation infrastructure being built as bilateral agreements are forged among federations, and we can expect this to accelerate as successful models emerge.

- **Identity Provider Operator (IdPO).** An IdPO is a federation member institution that operates an Identity Provider (IdP), the technology component that transmits identity information to Service Providers. An IdPO is responsible for the accuracy, security, and privacy of its community members’ identity information. This is done through the operation of business processes and technology (an Identity Management System - IDMS) for:
  - verifying the identity of community members,
  - maintaining accurate and timely information about community members,
  - registering community members’ authentication credentials,
  - maintaining the groups and roles to which community members belong,
  - authenticating community members during online sessions, and
  - releasing information about community members to Service Providers according to established privacy policy.

- **Service Provider Operator (SPO).** An SPO is an organization that operates a Service Provider (SP), the technology component that delivers online resources. Service Providers rely on identity information from IdPs to do this. SPOs may also be IdP Operators, or they may be independent.
6.2. Putting It Together - Federations

Federations can be viewed as a collection of members, IdP Operators and SP Operators, that collaborate to provide services to the IdP Operators’ community members.

Examples of federations include:
- InCommon (US)
- eduroam
- SWITCH (Switzerland)
- UCTrust (California)
- UT System (Texas)

Activities relevant to federations overall are listed below. Projects relevant to specific services of federations are listed under each service description.
- CommIT
- InCert
- The Quilt / InCommon collaboration

Federations provide the following services to enhance trust and interoperability among their member institutions:

- **Attribute Exchange Technology Framework.** Federations define a framework for the exchange of identity attributes among its members. In most cases, this framework is based on the Security Assertion Markup Language (SAML), although there are other frameworks, such as Globus, which is popular in the research computing grid community, and OAuth is growing in popularity in the commercial sector. The framework will also define a common vocabulary for attributes, such as eduPerson. Relevant activities include:
  - ADFS
  - ScalePriv NSTIC Grant
  - Shibboleth
  - SimpleSAMLphp
  - uApprove
  - OpenID Connect

- **Certification.** Certain of the Interoperability and Trust Standards may require certification of members’ organizational maturity, policies, practices, etc. The federation will provide this certification, or define how it may be obtained. Relevant activities include:
  - FICAM
  - InCommon Assurance
  - OIX
  - Kantara

- **Interoperability and Trust Standards.** The federation defines the standards its members must meet. Some of these standards may be required for all members, such as basic technical interoperability standards, while some may be required only under certain circumstances, for example, to assert high-assurance identity information (assurance profiles), or to receive attributes from IdP Operators without specific negotiation with each institution (service categories). Relevant activities include:
  - FICAM
  - InCommon Assurance
  - saml2int
6.3. Putting It Together - Interfederation

Interfederation on a global scale is a rapidly developing area of the identity management landscape. Interfederation can also refer to inoperation between different vertical sectors (e.g., Higher Ed and BioPharma) or with other communities (e.g., social identity providers). As such, it is difficult to project what interfederation will look like in the future, but the increasingly global nature of research and education demands attention to these issues. REFEDS, a group that explores approaches to the mutual needs of research and education identity federations worldwide, is a key player in this space.

Interfederation relies on the following:

- **Metadata Exchange.** These are technical mechanisms for exchanging information about the cooperating federations’ members.
- **Inter-Federation Agreements.** These are agreements, often bilateral, among the cooperating federations that govern the use of metadata, mapping of assurance and service categories, responsibilities, etc.
- **Assurance Mapping.** These are the mechanisms, technical or otherwise, for mapping identity assurance profiles among federations.
- **Service Category Mapping.** These are the mechanisms, technical or otherwise, for mapping service categories among federations.
- **Protocol Translation.** These are gateways and other mechanisms that translate the protocols used by different federations.

The following activities are particularly relevant to interfederation for research and education:

- CILogon
- Virtual Organizations (such as LIGO)
- InCommon TAC Interfederation Subcommittee
- InCommon Quilt Pilot Project
- Research & Scholarship Category
- Metadata Aggregator
- Metadata Query Protocol (MDX)
- Social2SAML Gateway
- IdP Proxy (i.e., SAML to SAML Gateway)
- NSTIC IDESG
- ORCID
- PEER/REEP
- REFEDS
- VIVO
IdP Operators are the stewards of identity information about their community members within a federation. This information is provided to services providers operated by the institution or by other federation members. At a very high level, the flow of information through an institution’s identity management service can be described as follows:

1. Information is collected from a variety of identity sources (e.g., student information system, payroll, friends of the library) on an ongoing basis. It is matched against existing data to remove duplicates and merged into a repository.
2. The information in the repository is enhanced over time by information from the Identity Sources, as well as business processes specific to identity management, including identity proofing and the assignment of community members to groups and roles.
3. After appropriate filtering, information about specific users is shared with Service providers through the use of authentication and attribute access services.

The following provides short descriptions of the building blocks of an IdP Operator’s identity management service:

- **Attribute Access.** This is a broad range of interfaces used by Service Providers to obtain information about their users. These methods may be invoked during a session, or they may be out of band. Those invoked during a session include Shibboleth, CAS, LDAP, and Active Directory. Out of band methods include provisioning frameworks like SCIM. Relevant activities include:
  - ADFS
  - CAS
  - Comanage
  - ConnID
  - IRMA
  - Kuali Identity Manager
  - OAuth
  - OpenICF
  - OpenLDAP
  - PubCookie
  - SCIM
  - Shibboleth/LTI Interoperability
  - SimpleSAMLphp
  - Syncope

- **Authentication.** These are services that can be used to verify the identity of a user. They are sometimes part of Attribute Access services, and sometimes are standalone. Examples include Kerberos, Shibboleth, CAS, PubCookie, LDAP, and Active Directory. Relevant activities include:
  - CAS
  - IRMA
  - Kerberos
  - PubCookie
  - ScalePriv NSTIC Grant (Multi-Factor Authentication)

- **Governance and Audit.** This is the institution’s management oversight and review structure for identity management. It provides a framework for verification and enforcement of compliance with institutional policy. Relevant activities include:
  - FICAM
  - InCommon Assurance
  - Kantara
**Group and Role Administration.** These are the technical and business services that administer the association of groups and roles with community members. These associations are then used to determine appropriate permission assignments within services. Grouper is the prime example here, because of its strong support for the requirements found in R&E. Many commercial identity management suites also contain group and role management modules. Relevant activities include:
  - Grouper
  - Kuali Identity Manager

**Managed Attribute Sharing.** These tools give individual users a role in the process of deciding which attribute information should be shared with each Service Provider.
  - UMA
  - uApprove
  - uProve
  - abc4trust

**Identity Match.** This service merges information from Identity Sources into the Repository, resolving situations where the same person appears in multiple sources. Typically, there are no strongly-identifying match keys like SSN that are used by all sources, so the Identity Match is usually implemented as an automated heuristic that refers questionable transactions to identity management staff for resolution. The heuristics are, more often than not, implemented by home-grown software that is closely tailored to the eccentricities of the institutions. Relevant activities include:
  - Identity Match

**Identity Vetting.** These are processes, such as examining a photo ID card or verifying an address, that increase the institution’s confidence in the identity of community members. Most Identity Sources perform identity vetting, but an identity management service may provide proofing as well to ensure consistent compliance with standards, as well as to gain higher confidence for specific individuals than is provided by their Identity Source. Relevant activities include:
  - NIST 800-63
  - FICAM
  - InCommon Assurance
  - Kantara

**Identity Source.** These are the systems of record that the institution uses to maintain information about students, faculty, staff, etc. Identity Sources also include more ad hoc membership lists used by campus organizations. While these Identity Sources are typically operated by other organizational units within the institution, they may also be operated by the identity management service.

**Policy.** These are the policies that govern identity management. These policies address issues such as stewardship, privacy, technical interoperation, organizational responsibilities, definition of campus roles and affiliations with their associated benefits and services, etc.
  - NIST 800-63
  - FICAM
  - InCommon Assurance
  - Kantara

**Repository.** The repository is the collection of information managed by the identity management service. It may be implemented as a single, tightly-integrated database, or (more commonly) it may be the union of databases maintained by the set of tools used in the identity management system.
  - Kuali Identity Manager
  - CPR - Central Person Registry
  - OpenRegistry
  - Syncope

### 7. Appendix - Implications for CIOs

A robust and effective identity and access management strategy carries many implications for university Chief Information Officers. CIOs must marshal their resources appropriately in order to align the efforts with their institutions’ strategic priorities. Further, they must represent the needs of the institutions’ community members and service providers. They must also be prepared to partner with external service providers.

Identity and access management is a many-faceted field with many interrelated components and activities.

It is our hope that this Identity Landscape has served to provide overall context for all of this. In order to provide more insight into how this relates to the point of view of CIOs, however, we present a few more lenses onto the landscape.

#### 7.1. The CIO as Institutional Enabler Perspective
As an enabler for institutional priorities, the CIO must map those priorities to technology-based services and resources. The diagram above illustrates this:

- Many priorities (such as Collaborative Research, MOOCs, Library Systems, Specialized Resources, and Cloud Computing) involve the provision of services and resources to select members of the community; this makes Group and Role management important. Federation and Interfederation are also important for inclusion of as broad a set of services and resources as possible. Finally, Assurance is required by any critical or sensitive service that is placed at risk by unauthorized users.
- Bring Your Own Device (BYOD) generally brings its own identity infrastructure along with the device, particularly for mobile devices. Interfederation, particularly Social Gateways, are important for the integration of these identities.
- Operational Efficiency is achieved through Group and Role management that enables individuals through delegation of authority. Assurance is required by any critical or sensitive service that is placed at risk by unauthorized users.

### 7.2. The CIO as Technology Provider Perspective

An institution's CIO is typically charged with management and coordination of all aspects of identity and access management, as outlined in Putting It Together - IdP Operators. As a technology provider the CIO will see the following:

- Registrar and Human Resources, among other identity sources, as critical partners.
- Service Providers within the CIO's direct purview.
- Computer Use Policy, Privacy Policy, and other applicable institutional policies.
- Software Development and integration of IAM components.
- Operations of IAM components and their underlying infrastructure.
- Office of Identity and Access Management. This is the part(s) of the organization responsible for the business processes of identity and access management. This may be an identified organizational unit or assigned to one or more other organizational units.

### 7.3. The End-User Perspective
End-users want to access Service Providers. They want to know that the Service Providers are reputable, and they want their privacy protected. They understand the importance of following the rules and working with administrative offices at their institution, like the Registrar, Human Resources, and the Office of Identity and Access Management. Users don’t care how all the pieces fit together, as long as they do fit.

- **Administrative Offices (Registrar, Human Resources, Office of Identity and Access Management).** These are offices within the institution that administer business processes related to identity.
- **Computer Use Policy.** These are the institution's policies governing the end-user’s use of the institution's resources.
- **Privacy Policy.** This is the institution's privacy policy. It governs the administration, release, and use of the end-user’s identity information.
- **Service Categories.** Also known as Certification Marks, Service Categories are assigned to Service Providers to indicate various aspects of a Service Provider's purpose and operational practices. They are assigned by a trusted authority, such as a federation, and provide end-users with an indication of a Service Provider’s reputation and trustworthiness. The CIFER Project envisions a role in providing Certification Marks for Service Providers in ensuring services conform to IAM software standards and best practices.
- **Service Provider.** This is a service that an end-user may elect to use.

### 7.4. The Service Provider Operator Perspective

Service Provider Operators want to enable access to their services by end-users, both individually and as members of institutions’ communities. They may form relationships with individuals, institutions, or federations in order to accomplish this. They require varying degrees of assurance in the true identities of their end-users.

- **Assurance.** This is the combination of policy, practice, technology, and agreements that determines the Service Provider Operator’s confidence in the identity of an end-user.
- **Federation.** A federation represents multiple member institutions. Service Provider Operators can typically use the same technical interfaces for IAM services for all IdP Operators within a federation, as well as other federations with interfederation agreements in place.
• **IdP Operator.** An IdP Operator represents multiple end-users. When a federation is not involved, Service Provider Operators are typically required to provide different interfaces for different institutions.

Depending on circumstances, a Federation may enter into service agreements with Service Provider Operators on behalf of all members, or service agreements may be formed with institutions or individuals.

8. Appendix - The Project Survey

8.1. Questionnaire

• **Project Name.** The name of the project.
• **Contacts.** The people who provided this information.
• **Overview / Mission.** A brief overview of the project's reason for being, what the products are, etc.
• **Goals / Roadmap.** Specific goals the project has for the future. If available, also a time frame for achieving those goals.
• **Approach to Work.** How priorities are set, the process for releasing deliverables, collaborative work style, expectations of members, etc.
• **Strategies for Sustainability.** Strategies for funding, inclusion of new members, etc.
• **Relationships with Other Projects.** Areas where there is observed interdependence or similarity with other projects.
• **Observed Gaps.** Elements of the identity landscape that do not seem to exist, but are needed to achieve the project's goals.
• **Challenges.** Potential roadblocks to achieving the project's goals.
• **More Information.** URLs where further information about the project is available.
• **Notes.** Miscellaneous notes that do not fit in the other categories.

8.2. The Projects

Survey responses are available in Known Identity Projects, a compendium of all major identity management related activities that were discussed.

9. Appendix - Top 10 IT Issues from EDUCAUSE

The follow are taken from EDUCAUSE’s Top-Ten IT Issues, 2013: Welcome to the Connected Age.

1. Leveraging the wireless and device explosion on campus
2. Improving student outcomes through an approach that leverages technology
3. Developing an institution-wide cloud strategy to help the institution select the right sourcing and solution strategies
4. Developing a staffing and organizational model to accommodate the changing IT environment and facilitate openness and agility
5. Facilitating a better understanding of information security and finding appropriate balance between infrastructure openness and security
6. Funding information technology strategically
7. Determining the role of online learning and developing a sustainable strategy for that role
8. Supporting the trends toward IT consumerization and bring-your-own device
9. Transforming the institution's business with information technology
10. Using analytics to support critical institutional outcomes

10. Acknowledgments

We thank the following people for their contributions to this document.

• Peter Alterman
• Tom Barton *
• Steven Carmody *
• Rob Carter
• Paul Caskey *
• Nathan Dors
• Michael Gettes *
• Gary Grafe *
• Keith Hazleton *
• Roland Hedberg *
• Jim Joki *
• Ken Klingenstein *
• John Krienke *
• Scotty Logan
• Nicholas Roy *
• Tom Scavo *
• Mark Scheible *
• Renee Shuey *
• David Walker, editor *
• Ann West *
• Bill Yock

* Member of the Identity Landscape Subgroup of the InCommon Technical Advisory Committee