The Value Proposition for Identity Federations

Authors: Chris Phillips (CANARIE), Lucy Lynch (NSRC), Nicole Harris (REFEDS/GÉANT), Heath Marks (AAF), Joni Brennan (Kantara Initiative)

Editor: Heather Flanagan (REFEDS/Spherical Cow Group)

Contributors: Ann Harding (SWITCH), Klaas Wierenga (Cisco)

Original source for this document
https://wiki.refeds.org/display/OUT/The+Value+Proposition+for+Identity+Federations

Executive Summary

Purpose of the Document

Education and research institutions around the world are facing significant resource challenges that impact their ability to offer a modern collaborative environment. Campus infrastructure, from the network (both wired and wireless) up through identity management, needs to support inter-institutional collaboration on the part of their students, faculty. In order to understand the layers of costs and benefits involved in local, regional, and global collaboration, campus CIOs and IT staff must understand the value proposition for a stronger network, richer services, and a solid identity management infrastructure. In particular, establishing an identity federation to help support the global engagement needs to have clear value at the local level as well as the regional or global level in order to win the necessary funding in the light of all the competing needs of the institution.

This paper attempts to bring clarity to the questions that surround the heart of the value proposition for identity federation. Why should identity management and federation be prioritized? What arguments can campus CIOs use to sway the local and regional funding agencies that already have so many demands? What needs to be done to establish an identity federation, and have it interoperate with other identity federations around the world?

Document Structure

This paper was coordinated through REFEDS, the Research and Education Federations group. Federation operators and identity thought leaders have contributed their expertise to the text in order to help new federations explain the value proposition of identity federations to their own organizations and funding agencies. The paper is targeted at CIOs and offers both a high-level overview as well as more details to help guide a CIO's support team in the work that needs to happen to support campus identity in a scalable way, right up to the global federation level.

Why Identity Management and Federation

For a campus with minimal resources, making the argument for a campus-level identity management system can be challenging. Taking that to the next level, the support of participation in one or more identity federations, can be even more challenging. This section discusses the

logic behind campus- and federation-level identity management, the security aspects, and other benefits at the campus level.

Campus-level Identity Management

Educational institutions offer more than just knowledge to their students. There is a strong symbiotic relationship between an institution and its constituents. The institution offers a variety of things to its constituents, including administrative support to researchers; a brand-name to that students, faculty, and researchers can associate with; and, various services such as library access to the local community. Institutions are as much in the business of offering institution-branded identifiers and issuing credentials as they are in facilitating research and learning. They are also expected to secure that information from inappropriate use.

With that branding opportunity in mind, institutions must think about the security surrounding the brand. The institution needs to be prepared to prove and understand the affiliation of entities on the network for security and for scaling access, services, and responding to user demand in a targeted manner. The affiliation information can control access and encourage trusted relationships between users and services.

Understanding who exactly is on your campus from a network perspective enables a wide range of possibilities and improvements. From improving the overall security profile for your network, to being able to more effectively manage your electronic resources, to being able to answer any legal issues around privacy and access, knowing who is on your campus network and controlling their authentication and authorization is key. Having a strong local-level identity system makes expanding to use federated identity easier.

Identity Federations

Identity federations--multilateral arrangements that allow campuses to take advantage of the identity infrastructure and possibly of services offered at other institutions--began serious development in the higher education space around the turn of this century. The Shibboleth project was among the earliest platforms developed to take advantage of attributes shared between institutions and was first described at a meeting in 1999.[1] The first identity federations got started in 2001 in Europe.

From then until now, the growth of identity federations has been impressive. eduGAIN--an interfederation service that connects federations and services from around the world--has grown to include over 40 research and education federations world wide. Identity federations offer too much potential for network security, service sharing, and collaboration to ignore.

Participation in identity federations does more than just answer the needs of individuals and departments on campus. It highlights a branding opportunity for a campus as a whole. The value in having a researcher use their campus identity abroad is a powerful market factor in putting an institution's name in to the broader research and education marketplace. Supporting federated

identities allows an institution to manage participation and to express their local identity and security policies in such a way to support scalable access to both local and federated resources.

Before federated identity was the desire for campus single sign-on (SSO). As more services and materials were available online and the devices used to access them not supported by local IT staff, the proliferation of local accounts drove the need for consolidation and the ability to use a single account to access a wider variety of services. In particular, libraries were an early driver for federated identity. With the need to be open to all while also required to restrict access to certain material due to contractual obligations with publishers, libraries needed--and continue to need--more than just SSO. They need to know about the individuals using their services. Are they students? Faculty? Visiting scholars?

Campus IT staff also have a need to know who is using their services, both in response to basic security best practices as well as knowing where to allocate network resources. They are also responsible for protecting that data from inappropriate use.

Security Aspects

An institution with a strong identity management system and appropriate integrated services has a greater ability to know who is using their services. Include federated identity, and suddenly you have more control over access based on role or description without having to manage those external identities. Also, the external resources being used do not have to store the user credentials and information; they merely need to know that a user has been authenticated. Authorization decisions may also come as part of the information shared by an institution, but it does not get stored on the external resource. The goal for security is to control the proliferation of information without a user's knowledge or consent. Without strong identity management and support for federated identities, the institution ends up with a proliferation of accounts and credentials and users that simply reuse passwords across a variety of campus services.

Coming back to the branding aspects of a campus identity, the institution will benefit from well-aligned users who are using the network. Both the institution and the users have an investment in the reputation and viability of the institution. Users want to be highly identified and tightly affiliated, and in order to keep the value of that affiliation high, there is a higher priority than the usual regarding privacy. Allocating resources to manage and protect the network and account security is not just about responsibility to the subject, it's also about maintaining the reputation of the institution and its credentials. Institutions have a huge stake in their users being a credit to the institution. Users, in turn, have a huge stake in the institution having a high enough reputation to be a valuable asset. Both parties are invested in the security of campus-issued identifiers.

The Cost of Identity Management

The actual cost for deploying and managing local and federated identity services will vary depending on what is already in place on a campus. At a minimum, a campus needs an identity

management system that can be used to provide attributes about individuals, as well as systems and services that may act as Identity Providers (IdPs) and Service Providers (SPs).

The cost of identity management can be high in the early stages--insuring accurate data, managing timely revision when roles or privileges change, establishing and managing partner relationship and the technologies needed to exchange and confirm assertions--all take time, resources, and institutional buy in. A large legacy system will further increase the cost and complexity of moving to a centralized, federation-friendly identity system.

Section Highlights

Supporting identity management at the campus level can provide a strong start into a campus becoming involved in an identity federation. There are several benefits to building up an identity management program and participating in a federation, including support for institutional branding, network security, and increasing the collaboration opportunities for students, faculty, and researchers. The biggest challenge here is the initial high cost to build the necessary infrastructure and broad institutional buy-in required to establish an identity management program according to current best practices.

Global Value (Joni Brennan, Kantara)

This paper has discussed the value propositions of Identity Federation in detail and with particular focus on local and general regional considerations. These same value propositions can be extended within a global framework, however some key strategies are emerging when applying federation concepts at a global level. These concepts are in addition to the technical vectors that have been referenced.

Resource Allocation

Consider initially that implementing a federated approach may not take less, in terms of resources, than the deployment of non-federated systems. However, the value of federation is tied to the proposition that one can leverage nearly the same resources to gain an exponential return of investment in access to audiences over a more highly efficient information system.

Diverse Players

If this high level value is accepted, a next step can be to understand how to connect for efficiencies across the globe. When looking at federation models from this scale it can be helpful to also consider that, at a global scale, not only do regions connect but those connections are typically enabled over myriad types of verticals. In other words, as the scale and application

of the federation model grows, the types of organizations that are connecting to support a federation will tend to also become more diverse.

Previous Boundaries Blur

As federations grow across a global context to enable students, citizens, and consumers, access to trusted services one concept become more apparent. This concept is that of "borderless" identity. Borderless identity does not refer to a physical border, rather it is a way to identify a trend with identity services that recognizes that identity management systems, leveraging federation, often need to address multiple types of users in order to see the full scale potential of identity. For example, a person may move between personae throughout a day including: student, citizen, employee, and consumer. This shift with in persona use could all even occur with in the context of one student at one university. When Identity Management services leverage federation at global scale it becomes apparent that the most efficiency is gained by leverage one approach that enables users to move through their specific persona, all while maintaining an appropriate degree of partitioning of roles to protect their privacy.

Further, to achieve this type of fluid approach to identity many organizations are partnering with non-typical organizations to meet needs. Governments may partner with banks or telephone carriers to enable a more frictionless approach to citizen identity. Health care providers may partner with government or financial institutions for trust anchors regarding health care identity management. As our digital lives seek to more closely alight with our physical lives these types of diverse and fluid partnerships seem to emerge more and more with in the global identity management landscape.

National Perspectives

With regard to national identity management and identity assurance programs we see very similar trends emerging with regard to a more fluid approach to identity. Just as every community has a unique set of needs to fulfill by leveraging federation, nations also have specific needs to address. In the United Kingdom, the needs of libraries have driven much of the national identity federation [*citation needed*]. In Australia, support for research has been a significant driver [*citation needed*]. While each nation may have specific use cases that consider their local culture and customs, nations all tend to have a common base line of requirements for trust with in national and international identity federations.

Mutual Recognition of National Federation Practices

Moving forward from the inception and evolution of Trust Frameworks, national programs are also evolving. Around the world nations are working to ensure they can engage with their citizens for myriad purposes. Typically the purpose is around ensuring citizens have access to government services for example.

Perhaps one region where this concept of federation of national identity programs is so compelling would be in the European Union. The European Union is, in itself, at federation of

nations. In this regional federation each nation has its own sovereignty however each nation also benefits through shared resources that can be leveraged through shared trusted governance and tools. One use case focuses on the delivery of health care to citizens of EU nations. The delivery of health care services relies upon identification of the patient and, ideally, through a technical and governance federation, health care data could be shared at rapid speed through trusted networks. These types of identity federations bring greater delivery of services to citizens while mitigating or at least reducing fraud within in a system. Given the strong uses cases with in the European Union the European Commission has developed the eIDAS (REFERENCE) that serves as the set of rules and tools for European Union member national identity management programs. The eIDAS lays out a framework that will ideally connect each nation of the EU while respecting the national sovereignty of each nation. Essentially this is an inter-federation project that aims to:

- create efficiencies
- lower burden on government
- lower friction for citizen access to services
- leverage shared resources of partner
- reduce fraud
- mitigate risks

Section Highlights

The global perspective focuses on vertical and national based approaches. However the use case essentially represents critical thinking and operational practices that draw from the same DNA of identity federation. The national programs can learn valuable lessons from academic federations and it's possible that academic federations can learn from the national approaches. All of this ideally leads to a reasonable core understanding of the benefits of federation as force multiplier across regions, industries, and research and academia. This is a reminder that identity federation is a powerful tool that aligns with the practices of people who are simultaneously students, citizens, consumers, and users… all within a few moments of any given day.

Getting Started

Whether the goal is improved campus network management, broader access to global services on the part of your community, supporting campus researchers regardless of their physical location, or all of the above, a strong identity management infrastructure starts with buy-in from a variety of campus constituents. In particular, the campus Bursar, Registrar, and Provost.

Business Case (Heath Marks, AAF)

When developing your business case there are 4 key activities which need to be considered:

1. The technology required (in this case, the tools and platforms around identity and access management),
2. The policy required (including federation policies, organizational policies, and security policies),
3. A business model regarding the operations of the federation; and,
4. A Service Delivery system to support the use of the service(for example, web content and a knowledge base for help desk support, training, communication and outreach, and marketing).

Keeping those items in mind, you need to understand the following areas in enough detail to inform your business plan.

The Market

- Potential customer demographics. Is your target market students, faculty, visiting scholars, staff? How do their needs differ when it comes to identity management? The support, technology and policy requirements vary between market segments. Researchers may require accesss to very different systems than campus administration. Student needs will differ from visiting scholars. From a service perspective, cloud services have different requirements for single sign on and federated access than administrative systems or teaching and learning sites. Government sites for grants are likely to require something else entirely. Understanding these areas should help focus your plan on exactly what is needed, and in what priority order, for your institution.
- Market research / environmental/industry analysis. A great deal of existing material has been created in the federated identity management area. What other international federation initiatives exist? What have others done and how widely has their work been adopted? With resources always a limiting factor, making sure to thoroughly review the existing global landscape will allow you to reuse other's innovations and save time on service development.

The Federation Strategy

After coming to an understanding of who your customers really are and what they need, as well as an understanding of what the market has to offer in terms of best practice and reusable policies and services, you need to consider your strategy. First, your vision statement: What are you trying to achieve with a federated identity service, and where do you want that service to be in the next five years? Next, your marketing strategy: how will you grow your federation? Will you follow a 'build it and they will come' model of hope, or will you build in something more active in terms of strategic outreach to your communities? And last, your roadmap: what are your short and long term goals, and what is your action plan for reaching those goals?

The Business Model

As with any service, there are basic structural decisions to be made and actions to be taken. These are not unique to identity management; all business functions need to establish these

boundaries. This area involves understanding costs, establishing sustainability, and measuring the return on investment (ROI).

- How will you cover the start up costs of your federation(s)? Costs will need to include time for research, training staff, hardware or cloud service purchases, and pilot testing, evaluation, and possible transition to a production service.
- Will this be a product under one of your existing business units, or will this be something that is outsourced to a third party? This has budget implications regardless of which model you choose, and choosing a model depends on the politics and structure of your organization.
- How will you sustain the ongoing operational costs of your federation as it grows? Will this be a fee-based service (at which point you need to understand your pricing strategy) or will this be a cost center for your organization? Establishing an identity management service at any level is not a 'install and forget' item. Ongoing development and research to stay current with best practice, operational support to handle upgrades and security issues, and possible expansion into new markets all require consideration for how to fund the activity into the future.
- How will you measure the ROI for the service? Establishing these criteria at the earliest stages makes future reporting significantly easier.

As always, the ultimate goal of a business offering is to provide value to your customers. As you build the business model, think about how you can clearly demonstrate or highlight that value to the community.

Management and Ownership

As was mentioned as part of the business model, an organization needs to consider whether this service will be done internally or outsourced, completely or in part. Rather than considering this as an either/or scenario, consider the possibility that operations may be handled internally, but innovation and development may be handled externally either by a third-party business partner or by the identity federation community. Alternatively, the campus may provide development and direction, but a third-party provides the operational management of the service (rebooting services, installing software, etc.)

- Who is going to be responsible and accountable for keeping the operations running smoothly on the federation technologies?
- Who will provide innovation and development for those services?
- Who is going to provide technical support to the end users of the technologies, noting that support in a federated environment can sometimes be challenging as the environment is decentralised over many sites the operator has no control over.

In any and all cases, as you put together your business plan, you need to know what key personnel will be required to support the model you choose to follow and what roles need to be filled to make this work. These roles may be outside your business unit; for example, the campus must have someone who can be responsible for student and faculty identity data.

Innovation

Innovation must be a part of your business plan, not just for the initial discovery of what is required, but to provide information on how to make these services relevant as best practice and community requirements change. By making innovation part of your future service delivery, you provide a stronger and more attractive area for the campus or other funding source(s) to continue to invest in identity services.

Section Highlights

A business plan should be one of the first things done as an organization considers establishing or expanding their identity management services and becoming part of an identity federation. A business plan should offer clear guidance on how the effort will be funded, where innovation will happen, and how to measure success. While many of the areas that need to be considered in such a plan are not unique to identity-related services, they will set the direction of the effort for the next five to ten years.

Campus Systems

A campus requires at least one system of record to store information on the campus body. Several campuses keep student, faculty, and staff records in separate systems. A common practice when faced with several systems of record for the different constituencies is to have those information stores feed into a single campus directory. The business practices around the systems of record is critical to the overall quality of the data. Processes must be in place at the very least regarding how data is entered into the system and how individuals or roles might be marked as inactive.[2]

Joining Existing Identity Federations at the Campus Level (Chris Phillips, CANARIE)

> Go fast alone or go far together. - African Proverb

At your campus you likely have a number of applications in your portfolio each with diverse data and authentication needs. What's common among them are your users and their desire for a common, safe and secure consistent user experience as well as their data at the right place, at the right time for the right reason.

On the other end of the spectrum your institution wants to be consistent on delivering quality services in a safe and secure manner with the ability to audit and manage risk effectively and centrally all without growing the cost of managing operations at the same pace as services get added.

Balancing these and other requirements when the application portfolio is small and centrally managed takes some co-ordination, but is doable. However, inevitably user demand increases and begins outstripping your team's capacity to deliver on time and within budget. How can you sustain adding more and more services without growing your team at the same rate as you add applications? How do organizations handle tens to hundreds of applications without having to match each application with a dedicated staff?

Campus IT teams that are adding applications at a greater pace than adding staff have taken the time to assess the portfolio and identify the common elements between their application and focused on what they should maintain control over and what they want to delegate out to others. Realizing that central IT will NOT be writing and maintaining every application on campus is a first step in this direction. The second step being recognizing what central IT SHOULD maintain control over and its role to advise and apply IT governance principles as to how the institution's data and core components like authentication should be handled and implemented. Often campus IT teams lead by example as well as offer tools and components to their partners in the departments or external 3rd parties to leverage. While there is room for innovative approaches, there is a wealth of resources available to the campus IT shop from the Identity Federation.

Identity Federation tools and techniques embody best engineering practices to tame the IT portfolio and are equally valuable to use locally within your campus as they are externally outside the institution to collaborate at a more broad scale. By framing how you deliver campus applications as if they were also being used by more than just your campus you are empowering yourself to be able to tap into applications that may already exist implemented in this fashion like Learning Management Systems (LMSs) or being able to leverage pre-built components designed for plug and play use out of the box.

As important as the tools are, clarity around who are the stakeholders at the table and the policies that your applications operate within are just as important.

While the end user is an obvious stakeholder, the institutional stakeholders are not as obvious. Some campus' break their stakeholders into roles around who handles end user data; data Stewards who and ultimately responsible and accountable for the collection and usage data and data Custodians, those who curate, protect and implement the will of the Stewards.

Additionally, qualities about the data are important to capture, maintain and express in the right context. Organizations that go through data classification practices are better able to describe how personal and identifiable information may be or that it may be public information. As well, the caliber and confidence in which the institution assures others about its data can dictate the context in which the data may be used. Some applications may require high levels of confidence around how a user signed in such as using a second factor or may require that a user must have gone through an elevated identity proofing process before accessing an specialized application requiring a more vigorous validation of the end user.

There is a symbiotic relationship between identity federations and campus environments. A campus can amplify the value of its application portfolio and utility of its identities (and hence

value to end users) by being a member of the identity federation tapping into the services and tools it has. In return, the identity federation is strengthened by campus' that maintain a consistent best practice environment around their identity data and services that the identity federation shares among its peers on behalf of the campus.

Federated Identity

The use of federated identity technologies to enable campus-wide single-sign-on does not necessarily require joining a federation (though that is one of the possibilities as a result of establishing a federated identity on a campus). Campus single-sign-on across a variety of applications and services may be considered an expression of federated identity. Having that single identity to control authentication and authorization across a variety of services means a more efficient use of ICT staff on campus. As discussed, it is also a critical part of the overall brand of an institution.

However, when joining a federation a campus may then take advantage of pre-existing agreements around liability, technical parameters, attributes to be exchanged, and more, that will allow an organization to use a repeatable process for connecting with partners that has already many of the required things "filled in". In other words, if your campus joins a federation, working through the legal and technical requirements happen one time, not once for each service. The efficiency is compelling, and an important part of a business case to be made for joining a federation.

Educause, a non-profit organization focused on advancing higher education through information technology, wrote a short paper on federated identity management that continues to be useful to organizations still considering the cost and value of building an identity infrastructure that supports federation on their campus. See "7 Things You Should Know About Federated Identity Management."[3]

Federation Policy Guidelines

When your campus identity system contains the necessary information about your populations and can share those attributes, then it is time to consider whether to join or create an identity federation.

The policy guidelines for an identity federation can actually be applied at a local level, if your institution is structured in such a way as to have several discrete departments or campuses. Significant work was put into determining what should go into a federation policy[4] and to create a template[5] (which continues to be updated as new information appears in the federation landscape) for future federations to follow.

Section Highlights

The key to realizing the value of identity federation starts at the campus level. Even if campuses never join an identity federation, they will find that the best practices suggested by identity federations are just as applicable for single sign-on across the diverse campus environment; a feature that campus constituents are coming to expect.

Identity and Virtual Research Organizations

Even before the Internet, researchers tend to collaborate across institutions with others in their field. Today, enabled by the access offered through the Internet, this style of collaboration today allows for large, multi-national collaborations that share access to scientific instruments or large data sets. These virtual research organizations, commonly referred to as 'VOs' provide an opportunity for individual institutions to expand brand awareness through the actions of their researchers in these broader forums.

The desire for this type of collaboration is often one of the strongest use cases for participating in an identity federation. Generally, a single institution would rather avoid establishing accounts for all the virtually visiting scholars; managing the roles and life cycle associated with accounts that have no other affiliation with the institution dilutes the brand and is not an efficient use of resources.

When necessary, however, VOs can and do establish their own identity management services to support their members. This requires a diversion of their resources away from science and towards basic infrastructure that would be unnecessary if all the institutions participated fully and released the basic identity attributes through one or more identity federations.

Legal Limitations

VOs have specific challenges when it comes to participating in a federation. Often, while they are structured and discrete entities, they are not always legal entities with the ability to sign contracts with federations. Since they may not be legal entities, they cannot assume any liability that is associated with the federation agreement and the management of identities. Institutions can assist VOs by making their formal participation in a federation unnecessary; by participating in federations and releasing the necessary attributes, institutions can enable researchers to use their own institution-based identifier in VOs around the world.

Infrastructure

Offering this kind of service to campus researchers is just one of the benefits of providing a strong identity management system and by participation in a federation. No additional action beyond what is already required for offering identity services to campus researchers. It is better to have campus infrastructure available than to waste money reinventing the necessary identity architecture within each research group.

Policies and Permissions for Information Sharing (Attribute Release)

Campuses collect and store a wealth of information about their constituents. From name to home address, course information to roles within the institution, the single most useful piece of information that is used by federated services is what's called the eduPersonPrincipleName. This unique identifier, described in the eduPerson schema, allows for federated services to uniquely associate a local account with an individual. Even a person's name, email address, and affiliation, while useful, are not as important as the unique identifier that allows a service to assign the correct access control information against a given identity.

There are ways to balance the desire and expectation for security and privacy on the part of the individual and their institutional IdP. Research and Education federations are beginning to support what are known as entity categories.[6] These categories group Service Providers according to basic, common criteria, and IdPs can base their decision to release attributes based on entity category, rather than a per-SP review for suitability.

A short white-paper, created through REFEDS, is available that describe the needs of VOs, studies done that support VO requirements, and what technology providers, policy makers, and funding agencies can do to help the VO identity infrastructure space.[7]

Section Highlights

Providing support to researchers–who often collaborate beyond campus boundaries–is a critical use case for federated identity and displaying the identity brand of a given institution. Campuses have a strong role to play here, as virtual organizations themselves often cannot sign contracts or enter into legally binding agreements.

Federated Services

Education is global, and federated services simplify the work to reach out beyond what is available locally. CIOs who have already started looking into the possibilities offered through identity federation are often keenly interested in services like eduGAIN, eduroam, and the possibilities involved in leveraging social identity. Standardization through implementations of services like these is happening to make it easier for global interactions to move forward. This section offers a high level review of those services, points to any requirements and instructions on how to deploy them, and offers comments on the limitations inherent in each service.

eduGAIN

eduGAIN is simple and powerful interfederation service that allows members of participating federations to access specific resources in other federations, without having to explicitly join

those additional federations directly. A variety of services are offered on campuses, particularly in libraries, based on eduGAIN participation. eduGAIN is an idea that works best when all members both consume and offer services through eduGAIN; having only a few institutions offer access to services and therefore bear all the costs of that access with no visible return on that investment makes for a poor long-term business model. For now, though, eduGAIN is growing steadily as more and more national or regional federations come online.

To participate in eduGAIN, review the General Requirements[8] posted on their wiki.

eduroam

eduroam is a services that allows roaming network access. As students, staff, or faculty visit other institutions or locations, they can gain access to the eduroam network using their home account credentials. No guest accounts or open networks are required, which in turn decrease the burden of support on the part of the network administrators and improves the overall security profile of the network.

To participate in eduroam, see the How-to information[9] on their wiki.

Social Identity Mapping

In today's world, many individuals have an account on a social network, such as Twitter, Facebook, or Google, before they have an institutional account. As such, several institutions have raised the question as to whether it is a more efficient use of resources to simply take advantage of those social identities rather than building the infrastructure required for an institution-based identity. If individuals are already familiar with and expect to use their social identity, why is an institutional identity useful?

This paper has emphasized the strong branding associated with providing institutional credentials to individuals. There is a loss of user privacy and loss of institutional control when a social identity is used in favor of an institutional identity. The technical complexity for an institution actually increases as handling user-controlled attributes, such as what comes out of a social identity, for the purpose of proving institutional affiliation is a very complex technical problem. Still, some institutions want to pursue this as a way to get more users actively partaking in campus services.

Students in particular may find it a burden to use something beyond their social identities to access information and materials. Those students are, however, potentially a source of future faculty and researchers, and as such having them use the branded identifier both protects their information from casual sharing and helps inform them of the value of using a branded identifier from their campus.

There is a place for social identity in a campus setting, though it is tightly limited in scope. Campuses that need to provide resources to visitors (e.g., summer program attendees) may find

that using a social identity for these individuals allows tighter control over the campus' branding while still supporting knowledge and control around access to network services.

Section Highlights

Campuses may further build their case for supporting identity federation by looking at some of the services available in a federated environment. This includes services such as eduroam, eduGAIN, and even using social identities on the campus network.

Conclusion

CIOs have a responsibility to help guide their campus towards making the most efficient use of resources possible, both for the short- and long-terms, while also aiding in the overall business of the campus by offering key infrastructure to help make the institution function best in a regional and global context.

There are great opportunities for showing leadership in this space, from partnering with the local thought leaders in the Bursar's, Provost's, and Registrar's offices, to participating in a broader forum with other campus leaders who are determining the best way to leverage regional and global resources.

This paper focused on the value proposition largely at a campus or institutional level. For organizations considering the creation of an entirely new federation, additional considerations need to be addressed, such as whether to follow a hub-and-spoke or mesh model [10], understanding the legalities around international data sharing and privacy legislation, and more.

---

[1] Gettes, M., and R. Morgan, K. Hazelton, P. Hill, K. Klingenstein, M. Poepping, F. Grewe, "Middleware Web-Auth Project." September, 1999, <http://kingsmountain.com/doc/shibboleth/Middleware-Web-Auth-Project.htm>

[2] "Identity Management InfoKit." <https://identitymanagementinfokit.pbworks.com/w/page/50989755/Home>

[3] "7 Things You Should Know About Federated Identity Management," Educause, 2009, < https://net.educause.edu/ir/library/pdf/EST0903.pdf>

[4] Harris, N. "An Introduction to Federation Policy." a presentation at the EuroCAMP meeting, October 2012, <https://www.terena.org/activities/eurocamp/oct12/slides/nicole-eurocamp-nov12.pdf>.

[5] Vermezovic, M. "Identity Federation Policy Template document." <https://www.terena.org/activities/eurocamp/oct12/programme1.html>

[6] "Entity Categories Home" <https://wiki.refeds.org/display/ENT/Entity-Categories+Home>

[7] "Ongoing Challenges in the VO space" <https://wiki.refeds.org/display/GROUP/Ongoing+Challenges+in+the+VO+Space>

[8] "General Requirements for Joining eduGAIN" <https://wiki.edugain.org/General_Requirements_for_joining_eduGAIN>

[9] "How To Deploy eduroam On-site or On Campus" <https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus>

[10] "Federation Architecture" <https://wiki.edugain.org/Federation_Architecture>