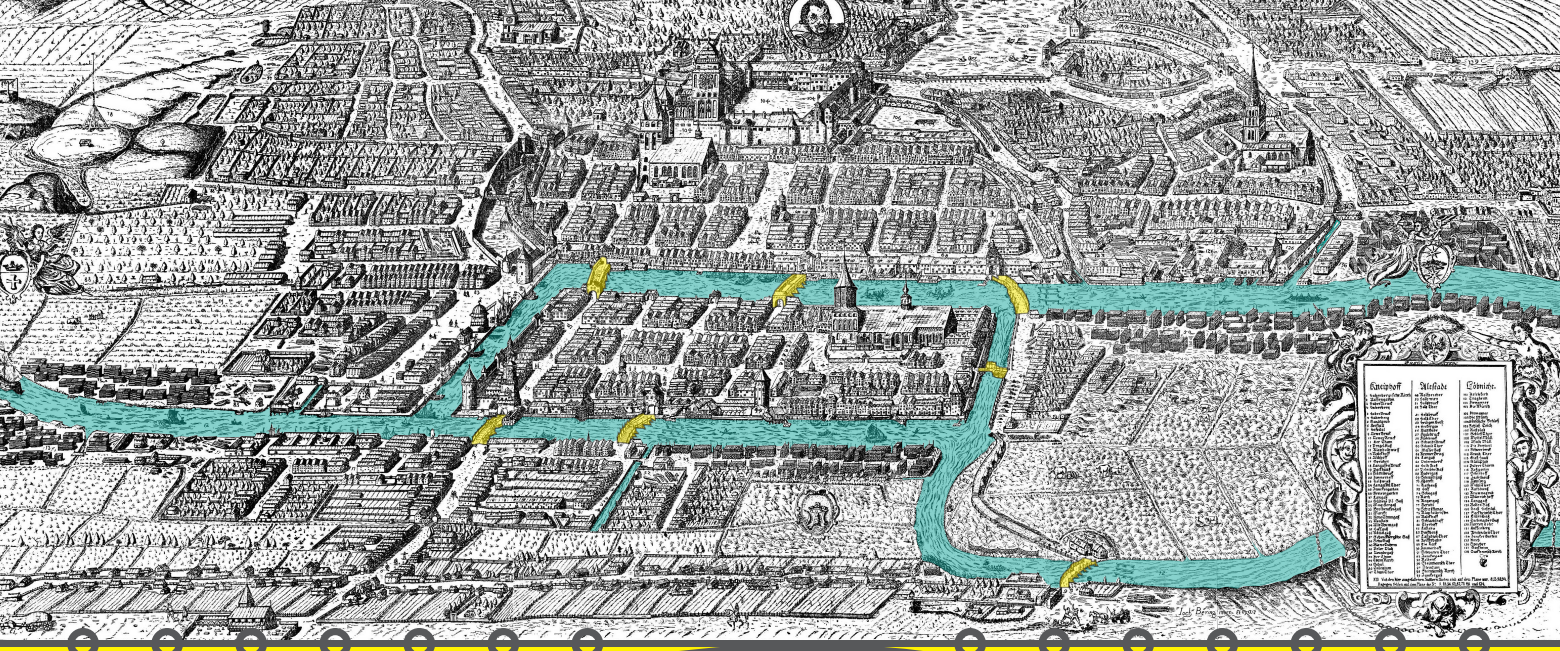


A Roadmap for Using NSF Cyberinfrastructure with InCommon

A practical guide for using InCommon and Identity Federation to support NSF Science and Engineering

Abbreviated Version: Benefits, Challenges, and Overview

William Barnett, Von Welch, Alan Walsh, and Craig A. Stewart
Indiana University

Please cite as:

Barnett, W., Welch, V., Walsh, A., and Stewart, C.A. *A Roadmap for Using NSF Cyberinfrastructure with InCommon: Abbreviated Version*. Available from: http://hdl.handle.net/2022/13025 and http://www.incommon.org/nsfroadmap.html

Acknowledgements

The authors thank the following individuals who volunteered their time to serve as the editorial board for the development of this document and provided invaluable feedback and suggestions: James Basney (NCSA/U. of Illinois), Michael Beyerlein (Purdue U.), Ken Klingenstein (Internet2), and Michael McLennan (Purdue U.). Ken Klingenstein also contributed much of the text for the Jean Blue use case in the Roadmap.

The authors thank the following individuals for sharing experiences and suggestions, which greatly improved this document: David Banz, Matt Kolb, Redmond Militante, and John O'Keefe. The authors also wish to thank Guy Almes (Texas A & M University), Jim Bottum (Clemson University), Gary Crane (SURA), Patrick Dreher (Renaissance Computing Institute), Gerald Giraud (Oglala Lakota College), Andrew Grimshaw (University of Virginia), Sandra Harpole (Mississippi State), Dave Jent (Indiana University), Ken Klingenstein (Internet2), Miron Livny (University of Wisconsin), Lyle Long (Penn State University), Clifford Lynch (CNI), D. Scott McCaulay (Indiana University), John McGee (Renaissance Computing Institute), Michael R. Mundrane (University of California, Berkeley), Jan Odegard (Rice University), Jim Pepin (Clemson University), Jim Rice (South Dakota State University), Larry Smarr (Cal-IT2), and Brian Voss (Louisiana State University), all members of the NSF Advisory Committee for Cyberinfrastructure (ACCI) Task Force on Campus Bridging, for suggestions regarding the content of this document.

The authors thank the InCommon staff for their support and the excellent materials they are producing, which were invaluable in authoring this document. Additionally, Tom Scavo of InCommon provided valuable feedback on several occasions during the writing of the document.

The authors thank the Indiana University Center for Applied Cybersecurity Research, affiliated with the Indiana University Pervasive Technology Institute (PTI), and PTI for funding staff writing and supporting this document. In particular, thanks go to Malinda Lingwall of the PTI for help with the layout and production of the final Roadmap document, and Maria Morris in IU Creative Services for the design of the layout of this report.

This material is based upon work supported by the National Science Foundation under Grant No. OCI-1040777 to Indiana University. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation, the Indiana University Pervasive Technology Institute, or Indiana University.

Other materials related to campus bridging may be found at:
https://pti.iu.edu/campusbridging/

PERVASIVE TECHNOLOGY INSTITUTE
INDIANA UNIVERSITY

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

About This Document

This document provides a Roadmap for using the InCommon identity federation to enable researchers to access NSF cyberinfrastructure (CI) via their campus authentication service. It presents benefits and challenges of using InCommon for NSF cyberinfrastructure, and guidance in overcoming the challenges. The Roadmap has three main sections, each aligned for a different audience:

A. *Benefits, Challenges and Overview* is intended for campus and project leadership, scientists and engineers using CI. It provides a summary of InCommon, relevant technologies and the benefits and challenges their adoption brings.

B. *The Guide to Technical Deployment* is intended for information technology professionals, from campuses and NSF cyberinfrastructure projects, and is a guide for deployment of InCommon software and services.

C. *The Guide to Policy and Business Processes* is intended for managers and policy makers, and discusses the policy, privacy, financial and other factors of InCommon deployment. Again it is both for staff from campuses and NSF cyberinfrastructure projects.

A final section provides a glossary, references and other resources.

This document is an abbreviated version of the whole Roadmap, omitting sections B and C to focus on issues of interest to campus and project leadership. The complete document can be found at http://www.incommon.org/nsfroadmap.html

In order to be insulated from inevitable changes in technologies and to be as comprehensible as possible, the document avoids capturing technical details when it can, instead providing references to existing (particularly online) documentation provided by InCommon, Internet2 and other organizations.

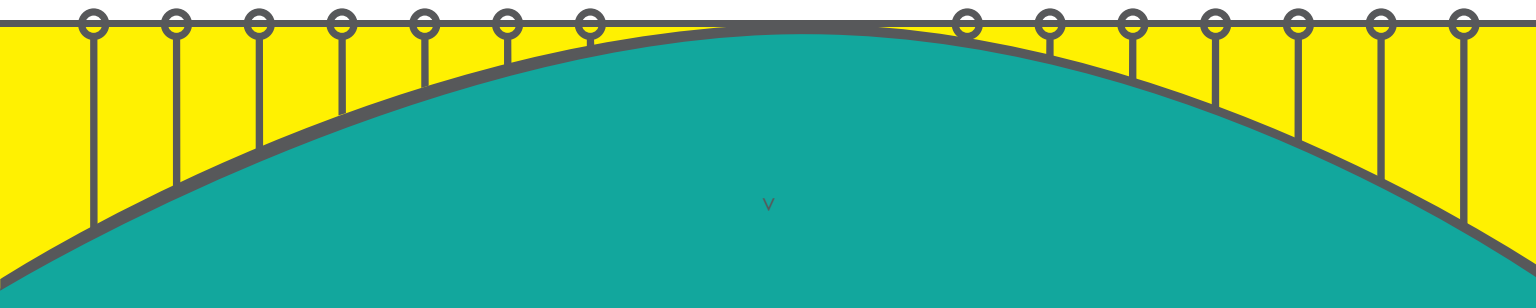
Document Scope

There are a wide variety of federated identity technologies and organizations that seek to form trust amongst organizations for online collaboration. This document is specific to InCommon, with its focus on higher education and research institutions, institutions that are highly aligned with the NSF science and engineering community.

This document also focuses on the needs of NSF cyberinfrastructure (CI) Projects, which are projects providing computer-based resources (e.g., compute cycles, data resources, shared instrumentation, web-based applications, virtual organizations) to scientists and engineers, and having some need to identify those researchers in order to, for example, perform access control, resource authorization, audit usage, or provide personalization. A full discussion of CI is beyond the scope of this document, for context the reader is referred to [59]. As subsequently discussed in Section A.1, NSF CI projects frequently have requirements above and beyond normal InCommon service providers and this document focuses on meeting those requirements.

In addition, the document is scoped as follows:

- InCommon is most accurately a federation based on the SAML protocol, and this document has chosen to focus on Shibboleth as a popular open source SAML implementation used in InCommon. Alternatives to Shibboleth, InCommon and SAML are discussed in Section A.5.
- As discussed in the Guide to Policy and Business Processes, InCommon allows for higher levels of assurance beyond the base level required for membership – i.e. Bronze and Silver. For the purposes of brevity, this document constrains itself to a brief discussion of when these higher assurance levels may be appropriate for a CI project to consider.
- This document covers cyberinfrastructure projects serving NSF researchers and institutions of higher education and research that host those researchers. Effort was made to discuss experiences with a variety of institutions of different sizes as to avoid assumptions regarding available resources and expertise.



A. Why Use InCommon and Federated Identity

> "Today's scientists and engineers need access to new information technology capabilities, such as distributed wired and wireless observing network complexes, and sophisticated simulation tools that permit exploration of phenomena that can never be observed or replicated by experiment. Computation offers new models of behavior and modes of scientific discovery that greatly extend the limited range of models that can be produced with mathematics alone, for example, chaotic behavior. Fewer and fewer researchers working at the frontiers of knowledge can carry out their work without cyberinfrastructure of one form or another."

As this quote from the National Science Foundation's (NSF) "Cyberinfrastructure Vision for 21st Century Discovery" [59] describes, cyberinfrastructure (CI) is a key and necessary component to support increasingly collaborative science and engineering. As opposed to traditional high-performance computing, a key goal of CI is to support scientific collaboration through a variety of computational, network, data and software elements distributed across campuses, regional, national and international organizations, and spanning scientific communities.

Critical to supporting the CI ecology is a well-coordinated, usable identity management system on which CI services can be built to allow for trusted collaboration and sharing of compute and data resources across researchers' institutions. To this end, the joint EDUCAUSE-CASC workshop on CI [13] recommended:

> "Agencies, campuses, and national and state organizations should adopt a single, open, standards-based system for identity management, authentication, and authorization, thus improving the usability and interoperability of CI resources throughout the nation."

The same workshop report continues and specifically recommends the InCommon federation as the current best solution for broad adoption.

The InCommon federation represents an implementation of federated identity. Federated identity refers to the practice of one organization receiving and utilizing identity information regarding a user from another organization, typically the organization at which the user is employed or is otherwise a member. The objective is that the latter organization leverages the work the first organization has done in enrolling the user, managing a credential (e.g., password[1]) for the user, and asserting attributes about the user.

Federated identities in general, and InCommon in particular, are becoming standards in establishing trust in the research sector. InCommon has other federal partners, including the Department of Energy's Energy Sciences Network (ESNet) and the National Institutes of Health.

---

1 We note that campuses are free to use any authentication credential they desire with InCommon, however passwords are common and this document tends to use that term, as it is familiar for many readers.

The goal of this Roadmap is to encourage more effective scientific collaboration and team science supported by campus and NSF CI by fostering the use of InCommon in order to:

1. Allow researchers to more easily collaborate and coordinate multiple resources through a single identity system rather than spending effort on managing multiple identities.
2. Allow NSF CI projects to leverage InCommon saving effort spent on establishing their own identity systems.
3. Allow campuses and other institutions to provide their researchers with a consistent identity system for local research and administrative computing, and remote research computing.

The Roadmap strives to achieve this goal by providing campuses and CI projects with the rationale and guidance for deploying and using federated identity, joining InCommon, and supporting collaborative science using that infrastructure.

A.1. What is unique about NSF CI?

A reasonable question is why NSF CI needs a roadmap in addition to the guides for adoption of federated identity and InCommon that already exist? NSF CI represents a number of science-enabling collaborations and resources, including rare (even unique) and valuable computational, data and instruments. CI representing these resources often has one or more of the following attributes, which make them atypical of InCommon service providers:

- Strong requirements for secured sharing: Computational resources are commonly among the worlds most powerful and it is not unheard of for them to fall under U.S. Export Control law. NSF CI also manages scientific data created and owned by researchers, data which can have privacy, integrity and trusted sharing requirements based on its implications to research results that can effect scientific standing and policy issues (e.g., climate change, human subjects information).
- Distributed researcher communities: A NSF CI project typically has distributed, dynamic researcher communities that don't conform to any group of researchers at any one campus or other institution. For example, access to TeraGrid is granted via a national allocations process that occurs multiple times per year [66]. Many projects have less formal processes involving collaboration participants who may come and go depending on current research interests and their alignment with the project.
- A history of identity management: Because of the nature of their resources and communities, NSF CI projects often have stringent, self-managed access control requirements. To meet these requirements, there is a history in NSF CI projects of performing strong vetting of their users and persistent account management. This creates a situation of researchers having multiple

digital personas (one for their institution plus additional personas for each project they are involved in), thus creating a barrier to trusted virtual collaboration.

- A need for incident response: NSF CI projects often have a need to perform incident response to understand the implications of any data breech; a need that is otherwise underrepresented in typical federated identity applications.
- Non-web access modalities: NSF CI projects often have command-line access modalities that are not currently supported by typical federated identity software (though as we discuss in Section D.2, such support is planned). For example, a common means of accessing NSF CI is through secure shell (SSH) to obtain command-line access and do job submission.

A.2. Brief Overview of Federated Identity and InCommon

We briefly present some basic terminology regarding federated identity and InCommon as shown in Figure 1. For more complete and technical definitions of the terms, the reader is referred to the Glossary.

The term "**federated identity**" refers to the ability to utilize a user's identity, as managed by one organization, across multiple organizations. A collection of organizations that agree to a common set of practices and policies for federated identity are referred to as a federation, with the member organizations being referred to as participants.

An example of a federation is InCommon, which focuses on institutions of higher education and organizations providing services to those institutions. InCommon is governed by its members [25] and operated by Internet2.

Within a federation, participants are identity providers that instantiate institutionally managed services that authenticate users and allow their identities to be shared with service providers, who consume those identities in order to provide access to resources or services. For example, the Indiana University identity management system represents an **identity**

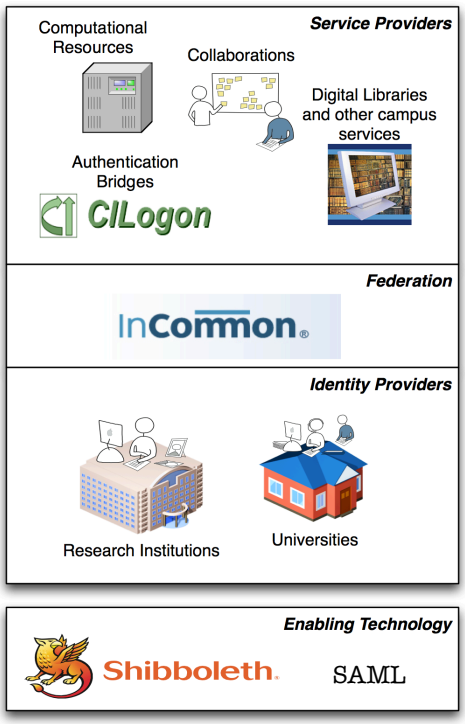


Figure 1. The InCommon landscape showing Identity Providers (campuses and institutions), the InCommon Federation, and Service Providers such as digital libraries, campus services, collaboration, and cyberinfrastructure. Enabling technologies include the SAML standard and the Shibboleth software.

provider, providing institutional credentials and guaranteeing that researchers with Indiana University logins have been physically vetted. A **service provider**, such as the Indiana Clinical and Translational Sciences Institute HUB [43], accepts institutional credentials from a number of identity providers and allows users of those identity providers access to cyberinfrastructure services such as data management and shared computational facilities.

The term "**identity**" is used to refer the aggregate of **identifiers**, which uniquely identifies an individual, with a collection of zero or more **attributes** regarding that person. Identifiers can be ephemeral, used only for a single session, pseudonomymous, persistent for arbitrarily long periods of time but not reflecting the user's physical identity, or fully identifying, persistent and reflective of the user's physical identity (e.g., an email address). Attributes provide information about a person such as their institutional role (e.g., faculty), department, class enrollment, or contact information (e.g., phone number). **Privacy** is preserved by the controlled release of identity information to service providers, a process referred to as **attribute release**.

InCommon is based on the **SAML** standard [67], which defines message formats and protocols to provide for interoperability among participants. Building on SAML, **eduPerson** [15] defines a set of user attributes common to educational institutions that is heavily used in InCommon.

A key function of the federation is to manage and distribute **metadata** among its participants. Metadata, whose format is defined by the SAML standard, is information that describes federation participants (identity and service providers) and allows participants to securely communicate identity information.

To utilize InCommon, software is needed that implements the SAML standards and provides identity providers with the tools to provide identities, service providers with the tools to consume identities, and users of the system the tools to express their intents with regards to authentication and privacy. A number of commercial and open-source SAML implementations are available. **Shibboleth** [78] is frequently used in InCommon. It is freely available as an open source project spearheaded by Internet2, and the focus of choice for this Roadmap.

A.3. Benefits for Researcher, Institution and CI Project

In this section, we describe the benefits for using federated identity and InCommon to support NSF science and engineering from three perspectives: that of the NSF researcher, that of the CI project, and that of the researcher's institution.

A.3.1. Benefits to the Researcher

To help understand the benefits of federated identities in research, we introduce you to Jean Blue, Professor and Researcher, and present a morning in her life supported by federated identity.

> Dr. Blue gets up in the morning and logs into her campus to check her email. One of the notes is from her campus sponsored research office, indicating

that a report is due on her NSF grant. She goes to the sponsored research office web site, and selects the research.gov link there. Because she previously logged in to her campus to check email, and because research.gov trusts her campus to provide accurate, up to date identity information, Dr. Blue's prior authentication is automatically used to allow access to her research.gov account and Dr. Blue uploads the requested report.

Another one of her emails alerts her to new data posted on the translational research wiki at National Institutes Health (https://www.ctsawiki.org/wiki/). She navigates to wiki, which like research.gov uses her prior institutional login to authenticate and welcome her directly to her personal wiki page. Seeing new data sets available, she decides to launch a job on the TeraGrid to analyze them. She opens a browser window to CILogon (https://cilogon.org/), which notes her campus authentication but asks her to release some additional attributes, such as a screen name, as requested by the CI service providers.

Jean then checks on the latest data for a clinical trial she is managing. The data is stored on Jean's local campus and accessible via secured web site, which permits her access based on her previous login. The site presents her with a request for access from a colleague at another institution to collaborate on a paper they are co-authoring. To make the request, the colleague authenticated to that data store with their campus login and approved the release of attributes - campus department and role in this case - to help validate the request. Jean reviews the request, recognizing the collaborator based on their name and attributes, and approves the request, granting access without having to create another username and password for the colleague.

Finally, Jean jumps over to Elsevier (http://www.sciencedirect.com/) to check some recent journals. The site welcomes her back, granting her access based on her status as her campus without knowing her actual identity, and alerts her that three of her watch-list words had been triggered by articles in her chosen journals. Jean sighs, and flags them for later reading.

It has been a busy morning, with a lot of collaboration done, all with a single campus identity.

How much of Jean Blue's story is real today? Every site with a URL is operational today using federated identities; the other scenarios are under active development.

As illustrated by this example, the direct benefit to the researcher is that they can utilize many CI resources without having to create yet another username and password for each. Initially this

expedites obtaining access to CI by removing delays with secure distribution of passwords to these resources. Over the lifetime of the researcher's access, it removes the need for the researcher to manage a separate username and password, reducing the chance of forgetting the password and giving them an existing campus support system for changing the password, resetting it in the event they forget it, etc. This not only means that there is a higher level of security, but also less overall effort since each of these services does not have to repeat a vetting process to ensure that the researcher is who they claim, instead leveraging the effort performed by their institutional identity provider. This is especially important for access to secured resources such as the TeraGrid or sensitive data, such as human subjects data.

In the bigger picture, the utilization of their campus login for access is a key first step to allowing someone to utilize any CI without concern about where it might be located or who is operating it. This allows researchers to focus on science and scientific collaboration without having to worry about what collaborators have accounts where, setting up authentication services, and the like.

For researchers with security concerns about data and other resources they are sharing in their collaboration, the use of campus credentials provides greater assurance, as collaborators will be less inclined to share or otherwise mishandle those credentials as they might a password generated solely for the collaboration. The credentials are also tied to the collaborator's position at an institution, meaning that in the event a researcher loses academic status, and the identity will be revoked and cannot be used for access. This allows service providers to more easily provide trusted access to sensitive data, and administrative processes for study review, like Institutional Review Boards (IRBs) can be undertaken with greater confidence and streamlined.

Finally, funding agencies, such as NIH (see [49]) and NSF, have joined InCommon and are moving towards federated identity as the access mechanism for grant application and administration. Utilization of federated identity for CI will bring uniformity to the authentication mechanism for science in line with the business processes of doing science.

A.3.2. Benefits for the CI project

> "Harvesting the science content from LIGO [Laser Interferometer Gravitational-Wave Observatory] data is a collaborative effort between instrumentalists, data analysts, modelers, and theorists. Efficient collaboration begins with scalable and robust identity management infrastructure that can easily be leveraged and integrated with the wide spectrum of tools LIGO scientists use to collaborate and analyze the LIGO data. Middleware from Internet2, including Shibboleth and Grouper, is enabling more LIGO science through easier collaboration and access to resources." -- Scott Koranda, Senior Scientist at the University of Wisconsin-Milwaukee and lead architect of the LIGO [54] Identity Management effort

A NSF CI project receives many of the same benefits from InCommon as any other InCommon Service Provider. Descriptions of these benefits, including multi-media presentations, can be found at the InCommon for Service Providers web site [32]. We summarize the benefits here and highlight those most applicable to CI projects.

The immediate benefit of federated identity to a project with any sort of access control requirements is that they still control who has access to their resources, but authentication is performed by their researchers' home institutions, getting the project out of the business of creating password databases and distributing passwords (and re-distributing them when they are lost). Initially, this has the benefit of expediting the granting of access to new users since they already possess their passwords. A case study from the Swedish Alliance for Middleware Infrastructure on federated identity addressing costs of the identity vetting process can be found in [55].

In the longer term, federated identity also reduces overhead on the project for managing researchers' passwords – e.g., resetting forgotten passwords, regular expiration – allowing the researcher instead to use already familiar campus processes. This reduction in responsibility can be of particular benefit to smaller, resource-constrained projects and collaborations.

From a security perspective, the use of the campus password for authentication also decreases the chance the researcher shares or otherwise mishandles that password, resulting in increased assurance of the user's identity. Removing the need to distribute passwords reduces risk of password exposure. And expediting researcher access by removing the need for password distribution acts to decrease the motivation for users to share passwords.

Furthermore, access can be based on researcher's attributes; for example, their role as faculty at their campus, either solely or in addition to the user's identifier. This use allows for automatic provisioning and de-provisioning of researcher access without time consuming verification of these attributes by project staff. For example, a service could verify on every use that a researcher remains their position as asserted by their home institution.

From the perspective of adoption, providing researchers access with an existing credential, and one potentially in use by other CI projects, removes one step in setting up the project CI, reducing a barrier to entry and encouraging use.

A.3.3. Benefits for the researcher's institution

As in the previous section on benefits to CI projects, campuses receive a number of benefits from the adoption of InCommon and federated identity that are documented by InCommon [28]. We summarize those benefits here and highlight those most applicable to supporting NSF science and engineering CI projects:

- ***Controlled, scalable access to external services.*** Shibboleth and InCommon provide a scalable means of providing controlled access to external services. For example, they can replace current schemes based on IP addresses for controlled access to digital libraries with a scheme based on

the institution's provisioned user base [37]. A complete list of InCommon Sponsored Partners either providing or in the process of providing access via InCommon can be found on the InCommon participants web page [11].

- ***Privacy controls.*** Shibboleth gives the campus and its faculty, staff and students privacy controls with regards to what attributes are released to each service provider. It supports anonymous and pseudonymous authentication, and the ability to receive user consent for the release of attributes, which can be beneficial in addressing legal requirements such as FERPA or HIPAA.
- ***Visibility into CI usage.*** The use of federated identity gives the campus visibility into the use of CI (and other services) by its user community since the campus is now part of the authentication process. This allows for the collection of aggregated, privacy-respecting statistics on what services are used by what types of users, and with what frequency.
- ***Grant competitiveness.*** Supporting federated identity will increasingly be important to grant competitiveness as the grant process moves to InCommon, as science increasingly moves to team science, and as effective collaborations improve science outcomes. InCommon will permit institutional researchers improved, or even preapproved, access to offsite data and analytical resources, allowing them to be more competitive in terms of research.
- ***Uniform authentication mechanism.*** Providing an authentication mechanism usable by both researchers on campus and their external collaborators helps prevent "home-grown" authentication systems being set up by researchers in front of potentially sensitive data (e.g., a collaboration sharing clinical data). In general, providing the same authentication mechanism for internal CI that is used by external CI allows the campus to provide CI locally for researchers and their collaborators that removes a barrier to transitioning between that local CI and regional or national CI.
- ***Internal single sign-on.*** Federated identity provides web single sign-on internal to the campus with the usual benefits of doing so, namely a single password for users, centralized provisioning of accounts, and central auditing.
- ***InCommon certificate service.*** A side benefit to joining InCommon is access to the InCommon Certificate Service [29], providing X.509 certificates (SSL, EV, personal signing, encryption, and code signing) for a fixed annual fee.

A.4. Challenges of Federated Identity

In order to be balanced in our presentation, we discuss here the challenges to deploying and using federated identity and InCommon. In the following section, we discuss some of the alternatives to InCommon and their trade-offs. The authors of this Roadmap believe these challenges are outweighed by the advantages and the approach of this roadmap is at least as good a choice as the alternatives, but we acknowledge that every solution has disadvantages as well as advantages and so include this section in the interest of full disclosure.

A.4.1. Mature Identity Management as a Required Prerequisite

In our discussions with organizations that have deployed Shibboleth and joined InCommon, a consistent prerequisite that came up was the organization having a "mature" identity management system in place before it undertakes federated identity. What constitutes "mature" is somewhat subjective, however the following have emerged as key features:

- ***A centralized user directory infrastructure.*** The organization has a single known, authoritative source for user information (authentication and attributes) with defined interfaces for accessing that information and controls on its modification.
- ***Understood business processes for user enrollment.*** The organization understands how users are enrolled in their identity management system, how their roles are assigned, and how they are removed from the system. This includes an understanding, at least, of what the edge cases are; for example: guest logins, anonymous library users, contractors, incoming students, and incoming faculty.
- ***Automated user provisioning.*** Based on the business processes, user provisioning and de-provisioning in the identity management system (i.e. addition, removal and attribute management of users), should be, at least for a majority of users, automated.

To be clear, an organization doesn't need to have these completely solved (no organization probably does), but more complete solutions lead to easier federated identity deployment and higher levels of trust.

Establishing an identity management system is outside the scope of this document, however some resources for doing so can be found in Section D.2.

A.4.2. Changes to Risk Profile

Federated identity turns what used to be an identity management process that was internal to an organization into a process distributed across multiple organizations. This brings changes to the risk profile of an adopting organization:

- ***Reliance on the external infrastructure.*** For a CI project, the trade-off for reduced workload and interoperability is a reliance on the InCommon federation and federation partners (and interconnecting infrastructure), which entails risks to both reliability and security. Related to this is that in the bigger picture, by increasing the scope of use for a single authentication, we increase the impact if that authentication is fraudulent (put simply, if the researcher's campus password is stolen, it grants illicit access to more services with federated identity). Quantification of these risks is difficult because they depend on the specific set of services used by each individual researcher and a lack of long-term operational data, but is something participants need to be aware of and accept (or identify mitigation strategies for).
- ***Reliance on enabling technologies.*** The use of federated identity involves relying on enabling technologies, for example Shibboleth software. Mitigating this risk is InCommon's use of open standards and Shibboleth's track record as an Internet2 member-supported software project.

- ***Risk of user attribute exposure.*** Shibboleth provides attribute release policies to control, on a service provider by service provider basis, the sharing of user attributes. Nevertheless, there is still a risk of human or software error resulting in inappropriate sharing. Emerging technologies such as uApprove [93] allows users to participate in attribute release and mitigates this risk.

A.4.3. Expenses of InCommon Membership and Shibboleth Deployment

For organizations that chose to deploy Shibboleth and manage the process of joining InCommon themselves, which is a very typical thing to do, the largest cost will be staff time. In the subsequent section (A.4.4) we summarize the effort required for organizations to estimate this cost.

In addition to staff time other expenses include:

- InCommon Participant Fees: Currently $1000-$3000 annually depending on the size of the organization plus a $700 one-time fee. Please see the InCommon web site [31] for details and changes since the writing of this document.
- Web certificates for identity and service providers. As with any other secure web server, these services need web server certificates. (Note that organizations could use the InCommon Cert Service as described in Section A.3.3 for these certificates.)

Alternatively, organizations can choose, as discussed in Section A.5, to outsource portions of the Shibboleth deployment - from design consultation to service hosting. This obviously shifts internal effort re-allocation to out-of-pocket expenses, and while organizations may choose this route, it does not appear to be a requirement for most organizations capable of running their own identity management systems. Outsourcing identity management services can also create additional risks, such as an outside entity having possession of institutional credential information.

A.4.4. Effort Required for InCommon Membership and Shibboleth Deployment

Most organizations choose to deploy Shibboleth (or an alternative) and manage joining InCommon themselves. As discussed in the previous section on expenses, staff time is the largest expense of this approach. It is difficult to give a quantified effort level for participating in federated identity as processes, expertise, culture and other factors vary between organizations and projects. We instead break down in Table 1 the effort required for deploying and maintaining federated identity and InCommon membership into a set of equivalencies to other common activities in terms of required effort and skills. The expectation is that the reader can judge the effort that these equivalent activities would require for their organization or project, and translate that into a quantified estimate for participation in InCommon.

Note that we provide only a summary of the tasks in this section, focusing on the effort level rather than "how to" details; for details on accomplishing the tasks, please see the subsequent Roadmap sections on Technical Issues, and Policy and Business Process Issues.

InCommon Membership Activity	Roughly Equivalent Activity/Effort
Leadership for process of joining	Requires CIO or delegate with support of campus leadership.
Policy and business process documentation and modification	Major authentication policy change, e.g., establishing a new minimum password strength.
Signing InCommon membership agreement	Contract signing.
Deployment of Shibboleth Identity Provider software	Deployment of a web single sign-on system (e.g., CAS [5]).
Deployment of Shibboleth Service Provider software	Deployment of a web application protected by web single sign-on; varies greatly by application.
Addition of a federated partner	Technically is a minor configuration change. From a policy perspective varies based on partner's requirements; having well defined process in place eases this.
Software/service maintenance	Maintaining a web single sign-on service. A few additional activities are minor overhead.

Table 1: Activities involved in joining and maintain membership in InCommon and rough estimates of the effort required based on equivalent activities.

A.5. Alternatives to InCommon and Shibboleth

We briefly describe some alternatives to the InCommon and Shibboleth approach highlighted in this Roadmap, and discuss their trade-offs.

- ***Bilateral agreements without InCommon.*** It is possible, at least in theory, to forgo a federation and use a set of bilateral agreements to support a federated identity fabric. Given the relatively low cost of supporting InCommon, the time costs of establishing similar bilateral agreement would seem to quickly outpace any savings.
- ***Using social networking identities.*** Instead of InCommon, an organization or project could utilize identities as asserted by social networking sites (e.g., Facebook, Google, Yahoo) using technologies such as OAuth [68] and OpenID [96]. The advantages and disadvantages of this approach is an area of some debate currently. On the side of social networking is that social networking sites absorb the costs of providing identities and users tend to already have such accounts. On the other hand, social networking identities tend to be self-asserted by the users (e.g., see [17]). There is no institutional authority behind them, thus InCommon has the potential for higher strength of authentication. InCommon has the advantage of greater stability provided by higher education institutions, as opposed to commercial entities, which may change their practices due to business concerns. InCommon also has the ability to include attributes from the user's home institution. It is also not an either-or situation, use cases are emerging [50] where these technologies are complementary: Shibboleth is used to provide

stronger authentication for employees and students, and OpenID is used for guest accounts to access less-sensitive resources.

- ***Projects can establish their own identity management system.*** CI projects can establish their own identity management systems, even utilizing single sign-on solutions to achieve some benefits of federated identity (such as the Earth Systems Grid [88] has done). This approach brings the benefit of being more of a known approach and keeps the project in control of their destiny, at the cost operating their own authentication infrastructure and a lack of interoperability.
- ***Alternative SAML implementations.*** There exist a number of open source and proprietary implementation alternatives to Shibboleth. We do not try to capture a list of such implementations here due to the fact it would be quickly out of date, but the list of InCommon affiliates [26] would be a good starting point for researching these alternatives. Organizations may want to explore these options, as it is certainly possible that while Shibboleth serves many organizations well, an alternative may serve a particular organization better. For example, an organization heavily using Microsoft products should explore federated identity products offered by Microsoft.
- ***Utilize a third-party identity provider.*** There exist commercial parties that can provide federated identity provider services that interoperate with InCommon for an organization that does not want to deploy their own service. Based on discussions, we believe a decision to pursue such an option is based more on an organization's culture than any technical or effort consideration. The list of InCommon affiliates [26] and sponsored partners [11] are good places to start exploring options.

A.6. Section Conclusion

This concludes the first section of the Roadmap for using NSF Cyberinfrastructure with InCommon. We hope that it has provided a good overview of InCommon, federated identity, and the advantages, disadvantages and challenges of deploying a federated identity system to support collaborative research and enable better science outcomes.

Two versions of this Roadmap are distributed: A complete version and, mainly intended for print, an abbreviated version. The complete version has two subsequent sections: one on Technical matters and one on Policy and Business Processes that go into more depth on addressing the challenges involved in joining InCommon and using it to support NSF cyberinfrastructure. The abbreviated version does not include these two sections. Both versions be may found online at:

http://www.incommon.org/nsfroadmap.html

B. Glossary of Terms

For the reader's convenience, we provide here a set of terms relevant to federated identity used throughout this document. We thank the InCommon organization as many of these definitions are taken from the InCommon glossary [33] and reproduced with the permission of InCommon.

- **Administrator** - In the context of InCommon, the Administrator serves as the participating organization's primary registrar. The Administrator is responsible for registering and maintaining the policies and technical data related to the organization's participation in the InCommon Federation, including the submission of the URL of the Participant's POP and any Identity Provider and/or Service Provider metadata and associated certificates. The participating organization's designated Executive assigns the Administrator.
- **Assertion** - The identity information provided by an Identity Provider to a Service Provider.
- **Attribute** - A single piece of information associated with an electronic identity database record. Some attributes are general; others are personal. Some subset of all attributes defines a unique individual. Examples of an attribute are name, phone number, and group affiliation.
- **Attribute Assertion** - A mechanism for associating specific attributes with a user.
- **Attribute Authority (AA)** - The Shibboleth software service that asserts the requesting individual's attributes by creating an attribute assertion and then digitally signing it. The receiving online Service Provider must be able to validate this signature.
- **Attribute Release Policy (ARP)** - Rules that an AA follows when deciding whether or not to release an attribute and its value(s)
- **Audit** - An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.
- **Authentication (AuthN)** - The security measure by which a person transmits and validates his or her association with an electronic identifier. An example of authentication is submitting a password that is associated with a user account name.
- **Authorization (AuthZ)** - The process for determining a specific person's eligibility to gain access to a resource or service, a right or permission granted to access an online system.
- **Boarding Process** – the term used to describe the process a service provider goes through on joining a federation to arrange receiving the attributes it requires from the identity providers.
- **Billing Contact** - In the context of InCommon, the Billing Contact is responsible for executing and maintaining all of the Participant's financial transactions associated with its InCommon federation participation, including any necessary communication with its internal Executive and Administrative Contacts, and externally with federation accounting staff.
- **Directory** - A directory is a specialized database that may contain information about an institution's membership, groups, roles, devices, systems, services, locations, and other resources.

- **eduPerson** - An LDAP object class authored and promoted by the EDUCAUSE/Internet2 eduPerson Task Force to facilitate the development of inter-institutional applications. The eduPerson object class focuses on the attributes of individuals. Current documentation on the eduPerson object class is available at http://www.educause.edu/eduperson/.
- **Electronic identifier** - A string of characters or structured data that may be used to reference an electronic identity. Examples include an email address, a user account name, a campus NetID, an employee or student ID, or a PKI certificate.
- **Electronic identity** - A set of information that is maintained about an individual, typically in campus electronic identity databases. May include roles and privileges as well as personal information. The information must be authoritative to the applications for which it will be used.
- **Enterprise directory** - An enterprise directory is a core middleware architecture that may provide common authentication, authorization, and attribute services to electronic services offered by an institution.
- **Executive** – In the context of InCommon, the Executive represents the participant organization regarding all decisions and delegations of authority for the responsibilities of InCommon Participants, including but not limited to payment of invoices, and assigning any person in the trusted Administrator role who submits Certificate Signing Requests, metadata, or Certificate Revocation Requests, and other administrative duties as described herein. The Executive is authorized as such in the InCommon participation agreement or by succession from the originally named Executive. The Executive role will typically be filled by a CIO, VP of IT, or other senior administrative officer responsible for the organization's information technology assets.
- **Federated identity** - The management of identity information between members of a federation.
- **Federation** - A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.
- **Identity** - Identity is the set of information associated with a specific physical person or other entity. Usually not all identity attributes are relevant in any given situation. Typically an Identity Provider will be authoritative for only a subset of a person's identity information.
- **Identity credential** - An electronic identifier and corresponding personal secret associated with an electronic identity. An identity credential typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access.
- **Identity database** - A structured collection of information pertaining to a given individual. Sometimes referred to as an "enterprise directory." Typically includes name, address, email

address, affiliation, and electronic identifier(s). Many technologies can be used to create an identity database or set of linked relational databases.

- **Identity Management System** - A set of standards, procedures and technologies that provide electronic credentials to individuals and maintain authoritative information about the holders of those credentials.
- **Identity Provider (IdP)** - The originating location for a user. Previously called the Origin Site in the Shibboleth software implementation. For InCommon, an IdP is a campus or other organization that manages and operates an identity management system and offers information about members of its community to other InCommon participants.
- **InCommon federation** - InCommon is a formal federation of organizations focused on creating a common framework for trust in support of research and education. The primary purpose of the InCommon federation is to facilitate collaboration through the sharing of protected network-accessible resources by means of an agreed-upon common trust fabric. InCommon participation is separate from membership in Internet2.
- **InCommon Technical Advisory Committee** - Group of individuals that provide technical guidance and direction for InCommon.
- **Level of Assurance (LoA)** - A level of assurance with respect to identity management is used convey the amount of trust one can have in an asserted identity. This is a complicated issue, covering, among other things, vetting practices of the institution making the assertion, the technical specifics of the authentication process, and institutional policies regarding password changing. For more detail, the reader is directed to NIST Special Publication 800-63 [62].
- **Metadata** - Data about data, or information known about an object in order to provide access to the object. Usually includes information about intellectual content, digital representation data, and security or rights management information.
- **Participant** - An organization accepted into the InCommon Federation that has met all the criteria for participation as either a higher education institution or a Sponsored Partner.
- **Participant Agreement (PA)** - This is the "contract" that a potential Participant signs when they are accepted by the Federation. This document outlines information such as fees, and responsibilities to participate in InCommon.
- **Participant Operating Practices (POP)** - This document describes how InCommon Participants need to describe their credential and identity management system.
- **Persistent Identifier** – A user identifier than is reused across multiple sessions. Such an identifier allows a service to maintain state about a user, for example, their ownership of data or personalization preferences.
- **Privacy Policy** - A statement to users of what information is collected and what will be done with the information after it has been collected.

- **Pseudonymous authentication** - Authentication with an identifier that remains consistent across sessions, but doesn't expose any personal information in itself, for example, a pseudonym one might create on an Internet forum.
- **Service Provider (SP)** - Previously called the Target Site in the Shibboleth software implementation. For InCommon, an SP is a campus or other organization that makes online resources available to users based in part on information about them that it receives from other InCommon participants.
- **Shibboleth®** - Software developed by Internet2 to enable the sharing of web resources that are subject to access controls such as user IDs and passwords. Shibboleth leverages institutional sign-on and directory systems to work among organizations by locally authenticating users and then passing information about them to the resource site to enable that site to make an informed authorization decision. The Shibboleth architecture protects privacy by letting institutions and individuals set policies that control what information about a user can be released to each destination. For more information on Shibboleth please visit: http://shibboleth.internet2.edu/uses.html.
- **Sponsored Partner** - A business partner that provides resources to a higher education institution, and is sponsored for participation in InCommon by a participating higher education institution.
- **Technical Contact** - The Technical Contact for InCommon serves as the primary point of contact for all technical issues for the organization participating in InCommon. The technical contact communicates with federation technical staff to ensure smooth operation of the federation's infrastructure.

C. References

1. Accrediting Agencies Recognized by InCommon. http://www.incommonfederation.org/accrediting.html
2. Administrative Interface for Internet2 Services. https://service1.internet2.edu/siteadmin/manage/
3. Barton, Tom, Jim Basney, Tim Freeman, Tom Scavo, Frank Siebenlist, Von Welch, Rachana Ananthakrishnan, Bill Baker, Monte Goode and Kate Keahey. Identity Federation and Attribute- based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy. 5th Annual PKI R&D Workshop, 2006.
4. Basney, Jim, Terry Fleury and Von Welch. Federated Login to TeraGrid. 9th Symposium on Identity and Trust on the Internet, 2010. http://www.ncsa.illinois.edu/~jbasney/tgfed.pdf
5. Central Authentication Service. Jasig. http://www.jasig.org/cas/
6. CIC InCommon Silver Project: Phase 1 Report. July, 2010. http://www.cic.net/Libraries/Technology/IdM_InCommonSilverPhase1.sflb.ashx
7. CILogon Portal Delegation. http://www.cilogon.org/portal-delegation/
8. CILogon Service. https://cilogon.org/
9. COmanage: Collaborative Organization Management. http://www.internet2.edu/comanage/
10. Configuring Shibboleth Delegation for a Portal. https://spaces.internet2.edu/x/n4Sg/
11. Current InCommon Participants. http://www.incommonfederation.org/participants/
12. DataONE. https://www.dataone.org/
13. Developing a Coherent Cyberinfrastructure from Local Campus to National Facilities: Challenges and Strategies. A Workshop Report and Recommendations. EDUCAUSE Campus Cyberinfrastructure Working Group and Coalition for Academic Scientific Computation. February 2009. http://www.casc.org/papers/CASC-CCI_Workshop_Report_and_Recommendations.pdf
14. EDUCAUSE FedId Resources. http://www.educause.edu/Resources/Browse/FederatedIdentityManagement/31075/
15. eduPerson and eduOrg Object Classes. http://middleware.internet2.edu/eduperson/
16. Family Educational Rights and Privacy Act (FERPA). http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
17. Goodin, Dan. Interpol chief impersonated on Facebook. The Register. September 20, 2010. http://www.theregister.co.uk/2010/09/20/interpol_chief_impersonated/
18. IdPAddAttribute. https://spaces.internet2.edu/display/SHIB2/IdPAddAttribute/
19. IdPAddAttributeFilter. https://spaces.internet2.edu/display/SHIB2/IdPAddAttributeFilter/

20. IdP Clustering Configuration. https://spaces.internet2.edu/display/SHIB2/IdPClusterIntro/
21. IdPInstall. https://spaces.internet2.edu/display/SHIB2/IdPInstall/
22. IdPLogging. https://spaces.internet2.edu/display/SHIB2/IdPLogging/
23. IdPMetadataProvider. https://spaces.internet2.edu/display/SHIB2/IdPMetadataProvider/
24. IdPUserAuthn. https://spaces.internet2.edu/display/SHIB2/IdPUserAuthn/
25. InCommon: About InCommon. http://www.incommon.org/about.html
26. InCommon Affiliates. http://www.incommonfederation.org/affiliate/
27. InCommon Basics and Participating in InCommon: A Summary of Resources. https://spaces.internet2.edu/download/attachments/2815/resources_booklet.pdf?version=3
28. InCommon Benefits. http://www.incommonfederation.org/benefits.cfm
29. InCommon Cert Service. http://www.incommonfederation.org/cert/
30. InCommon Education and Training. http://www.incommonfederation.org/educate/
31. InCommon Fee Structure. http://www.incommonfederation.org/fees.html
32. InCommon for Service Providers. http://www.incommon.org/partners/
33. InCommon Glossary. http://www.incommonfederation.org/glossary.cfm
34. InCommon IAM Online Presentations http://www.incommonfederation.org/iamonline/
35. InCommon Identity Assurance. http://www.incommonfederation.org/assurance/
36. InCommon Introductory Presentation https://spaces.internet2.edu/download/attachments/2815/InC_Overview_v2.ppt?version=1
37. InCommon Library Collaboration. http://www.incommonfederation.org/library/
38. InCommon Metadata Consumption. https://spaces.internet2.edu/display/InCCollaborate/Metadata+Consumption/
39. InCommon Policies and Practices. http://www.incommonfederation.org/policies.html
40. InCommon Sponsored Partners. http://www.incommonfederation.org/sponsor.html
41. InCommon Shibboleth Metadata Configuration. https://spaces.internet2.edu/display/InCCollaborate/Shibboleth+Metadata+Config/
42. InCommon Technical Guide https://spaces.internet2.edu/display/InCCollaborate/Technical+Guide/
43. Indiana Clinical and Translational Sciences Institute (CTSI). http://www.indianactsi.org/
44. Information from InCommon. https://spaces.internet2.edu/display/InCCollaborate/Information+from+InCommon/
45. Install Shibboleth to protect Java Servlets. https://spaces.internet2.edu/display/SHIB2/NativeSPJavaInstall/

46. Internet2: Boarding Process. https://spaces.internet2.edu/display/fedapp/Boarding+Process/
47. Internet2 Events. http://events.internet2.edu/
48. Internet2: FedApps Working Group. https://spaces.internet2.edu/display/fedapp/Home/
49. Internet2: NIH Federation InCommon Wiki. https://spaces.internet2.edu/display/InCNIH/InC-NIH/
50. Inernet2: OpenID Use Cases. https://spaces.internet2.edu/display/OpenID/Use+Cases/
51. JISC Idm Toolkit. https://gabriel.lse.ac.uk/twiki/bin/view/Projects/IdMToolkit/Toolkit/
52. Johnson, H. and P. Caskey. Introduction to Shibboleth Attribute Delivery. Educause CAMP, June 2007. http://www.educause.edu/Resources/IntroductiontoShibbolethAttrib/161780/
53. Join InCommon. http://www.incommonfederation.org/join.cfm
54. Laser Interferometer Gavitational-Wave Observatory (LIGO). http://www.ligo.caltech.edu/
55. Leve, Kristina and Valter Nordth. Lowering costs of identity proofing by federated identity management. http://www.incommonfederation.org/docs/other/SWAMI_federated_idm_roi.pdf
56. Metadata. https://spaces.internet2.edu/display/SHIB2/Metadata/
57. Morgan, R. L. "Bob", Scott Cantor, Steven Carmody, Walter Hoehn, and Ken Klingenstein. "Federated Security: The Shibboleth Approach." Educause Quarterly, Volume 27, Number 4, 2004. http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/FederatedSecurityTheShibboleth/157315/
58. National Science Foundation and Penn State InCommon Pilot Now Underway. November 17, 2010. https://iam.psu.edu/national-science-foundation-and-penn-state-incommon-pilot-now-underway/
59. National Science Foundation Cyberinfrastructure Council. Cyberinfrastructure Vision for 21st Century Discovery. March 2007. http://www.nsf.gov/pubs/2007/nsf0728/nsf0728.pdf
60. NativeSPClustering. https://spaces.internet2.edu/display/SHIB2/NativeSPClustering/
61. NativeSPMetadataProvider. https://spaces.internet2.edu/display/SHIB2/NativeSPMetadataProvider/
62. NIST Special Publication 800-63: Electronic Authentication Guideline. Version 1.0.2. April, 2006.
63. NITLE Shib and FedId Roadmap for Smaller Colleges and Universities. http://cnx.org/content/m31491/latest/
64. NSF Cooperative Agreement: Supplemental Financial/Administrative Terms and Conditions--Large Facilities. September 25, 2006

65. NSF Dear Colleague Letter: Cyberinfrastructure Framework for 21st Center Science and Engineering (CF21). http://www.nsf.gov/pubs/2010/nsf10015/nsf10015.pdf
66. NSF Resource Allocations Policies. https://www.teragrid.org/web/user-support/allocations_policy/
67. OASIS Security Services (SAML) Technical Committee. http://www.oasis-open.org/committees/security/
68. OAuth: Introduction. http://oauth.net/about/
69. Ocean Observatory Initiative (OOI). http://www.oceanleadership.org/programs-and-partnerships/ocean-observing/ooi/
70. Open Science Grid. http://www.opensciencegrid.org/
71. OSG Registration Authority. https://twiki.grid.iu.edu/twiki/bin/viewauth/OSGRA/
72. Project Moonshot. http://www.project-moonshot.org/
73. ProtectNetwork. http://www.protectnetwork.org/
74. REFEDS: Research and Education Federations. http://www.terena.org/activities/refeds/
75. Science Gateways Home. https://www.teragrid.org/web/science-gateways/
76. Shib Enabled. Internet2. https://spaces.internet2.edu/pages/viewpage.action?pageId=11484
77. Shibboleth 2 Identity Provider Configuration. Internet2. https://spaces.internet2.edu/display/SHIB2/IdPConfiguration/
78. Shibboleth: About http://shibboleth.internet2.edu/about.html
79. Shibboleth: Communicating with a Service Provider. https://spaces.internet2.edu/display/SHIB2/IdPSPCommunicate/
80. Shibboleth Deployment Checklist http://shibboleth.internet2.edu/shib-checklist-final-website.html
81. Shibboleth Getting Started http://shibboleth.internet2.edu/get-started.html
82. Shibboleth Installation. https://spaces.internet2.edu/display/SHIB2/Installation/
83. Shibboleth Mailing Lists. http://shibboleth.internet2.edu/lists.html
84. Shibboleth Support Documentation http://shibboleth.internet2.edu/support.html
85. Shibboleth: Talk to a New IdP. https://spaces.internet2.edu/display/SHIB2/NativeSPAddIdP/
86. Shibboleth Technical Deployers Info Center http://shibboleth.internet2.edu/deployers.html
87. Shibboleth Technical Manager Info Center http://shibboleth.internet2.edu/adopters.html

88. Siebenlist, F., R. Ananthakrishnan, D. E. Bernholdt, L. Cinquini, I. T. Foster, D. E. Middleton, N. Miller, and D. N. Williams, "Enhancing the Earth System Grid Security Infrastructure through Single Sign-On and Autoprovisioning," Proceedings of the 5th Grid Computing Environments Workshop, Portland, Oregon, USA, ACM, 2009. http://www.mcs.anl.gov/uploads/cels/papers/P1683.pdf.

89. Support. http://shibboleth.internet2.edu/support.html

90. SWITCH AAI Demo. http://www.switch.ch/aai/demo/

91. TeraGrid: Campus Champions. https://www.teragrid.org/web/eot/campus_champions/

92. TeraGrid User Portal. https://portal.teragrid.org/

93. uApprove. SWITCH. http://www.switch.ch/aai/support/tools/uApprove.html

94. Welch, Von, Tom Barton, Kate Keahey and Frank Siebenlist. Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration. 4th Annual PKI R&D Workshop, 2005

95. Welch, V., Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman and Steven Tuecke. Security for Grid Services. Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), 2003.

96. What is OpenID? http://openid.net/get-an-openid/what-is-openid/

97. X.509 Certificates in Metadata. Internet2. https://spaces.internet2.edu/display/InCCollaborate/X.509+Certificates+in+Metadata/

D. Additional Resources

D.1. Future Resources

In this section we briefly discuss technologies and other services that are not available today, but are expected to be available in the next future and which may bring benefit to NSF CI projects and institutions that house NSF researchers. These technologies are listed in no particular order.

D.1.1. UApprove

uApprove [93] is a software extension to a Shibboleth IdP which allows the user to make attribute release decisions instead of relying on the Shibboleth IdP administrator and organization policy. Many organizations are hoping that by putting the decision into the hands of the users, it will ease concerns around FERPA [16].

D.1.2. Federated SSH Work

A current limitation of InCommon and Shibboleth is a lack of support for applications other than web browsers. As we discussed in the Guide to Technical Deployment, CILogon exists to bridge from InCommon to PKI credentials, used by many command line grid applications.

Two future developments that are working to address adding federating identity support to a broader range of non-web application are Project MoonShot [72] and the Federated SSH work as part of the COmanage project [9].

D.1.3. FedApps Working Group

Internet2 is starting a working group to investigate issues involved with making applications available via federated identity. This working group, entitled "FedApps" [48], is in the process of forming at the time of this writing.

D.2. Identity Management Resources

Establishing an identity management system is outside the scope of this document, some resources for doing are:

- The NMI-Edit web site: http://www.nmi-edit.org/started/index.cfm
- InCommon IAM Online: http://www.incommon.org/iamonline/
- Educause Federated Identity Management Resources: http://www.educause.edu/Resources/Browse/FederatedIdentityManagement/31075/
- Jansson, Eric. NITLE Shibboleth and Federated Identity Management Roadmap for Smaller Colleges and Universities. Connexions. August 20, 2009. http://cnx.org/content/m31491/latest/
- JISC. The Identity Management Toolkit. https://gabriel.lse.ac.uk/twiki/bin/view/Projects/IdMToolkit/Toolkit/

D.3. Resources for Federated Identity Deployment

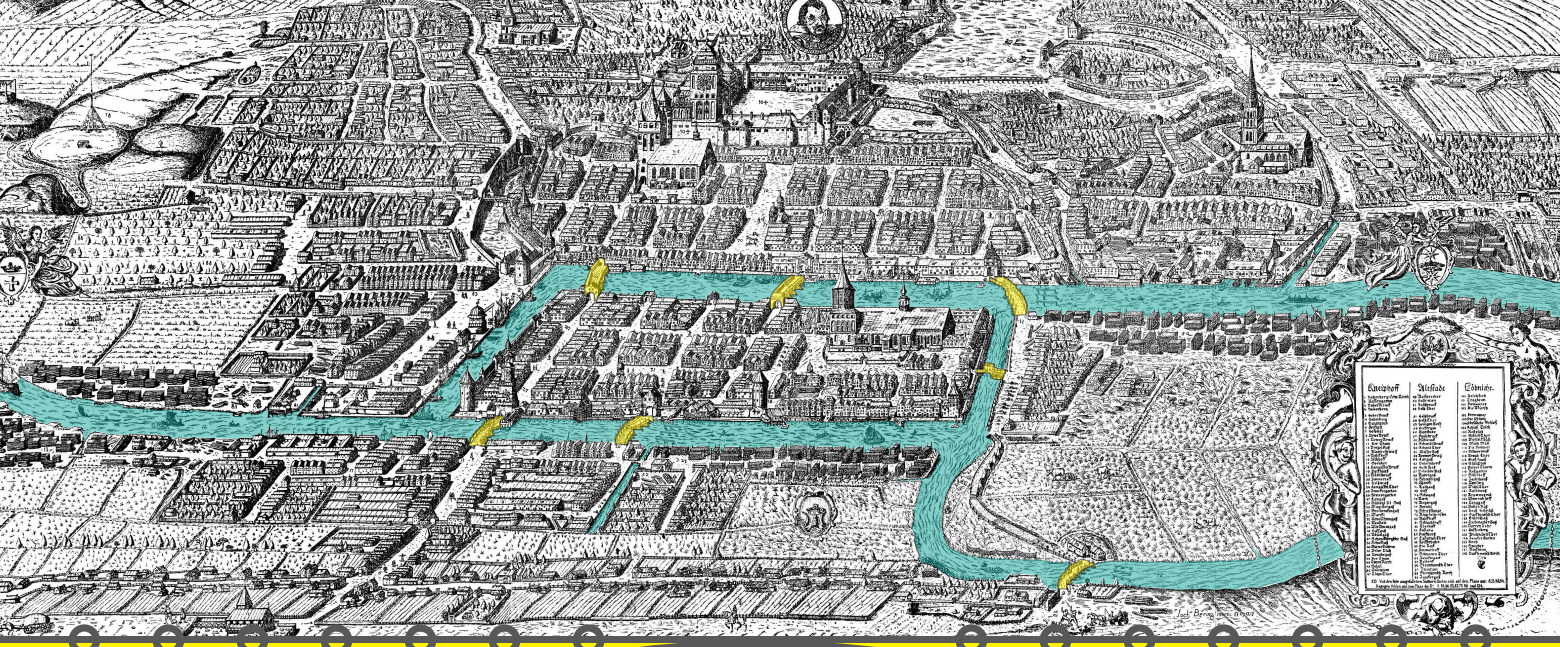
D.3.1. Examples of Deployments

In this section we list some examples of deployments to provide the reader with some real-world experience from institutions that may approximate their own:

- EDUCAUSE presentation describing experiences at UCLA, Penn State and New Castle (UK): http://www.educause.edu/Resources/ShibbolethCaseStudies/161773/
- Deploying Shibboleth: Technical Requirements, Policy Issues, and Case Studies (presentations from USC, Penn State, MIT): http://www.educause.edu/Resources/DeployingShibbolethTechnicalRe/169205/
- Shibboleth In Use, a collection of use cases on the Shibboleth web site: http://shibboleth.internet2.edu/shib-in-use.html
- InCommon Case Studies: http://www.incommonfederation.org/cases.html
- USC Case Study by NMI-EDIT: http://www.nmi-edit.org/case_studies/usc-shibpubc.pdf
- Implementing a production Shibboleth IdP service at Cardiff University (presentation slides): http://www.slideshare.net/JISC.AM/cardiff-jisc-fam-aston-may07/
- InCommon … Now That's the Ticket. Lafayette provides students with SSO ticketing convenience. http://www.incommonfederation.org/docs/eg/InC_CaseStudy_UTix_Lafayette_2009.pdf

D.3.2. InCommon Training Opportunities

The best place to look for an up to date list of training opportunities is the InCommon Education and Training web site [30], which includes both a list of in-person workshops and online seminars.



The cover image is based on Joachim Bering's etching of the city of Königsberg, Prussia as of 1613 (now Kaliningrad, Russia). Seven bridges connect two islands in the Pregal River and the portions of the city on the bank. The mathematical problem of the Seven Bridges of Königsberg is to find a path through the city that crosses each bridge once and only once. Euler proved in 1736 that no solution to this problem exists or could exist. This image appears on the cover of each of the Campus Bridging Workshop reports.

Campus bridging is the integrated use of cyberinfrastructure operated by a scientist or engineer, other cyberinfrastructure on the scientist's campus, at other campuses, the regional, national, and international levels in a seamless manner as if they were proximate to the scientist and when working within the context of a Virtual Organization make the 'virtual' aspect of the organization irrelevant (or helpful) to the work of the VO. The challenges of effective bridging of campus cyberinfrastructure are real and challenging – but not insolvable if the US open science and engineering research community works together with focus on the greater good of the US and the global community. Other materials related to campus bridging may be found at: https://pti.iu.edu/campusbridging/