2018 Internet2 Trust and Identity Accomplishments

March 28, 2019

Document Title: 2018 Internet2 Trust and Identity Accomplishments
Repository ID: TI.124.1
Persistent URL: http://doi.org/10.26869/TI.124.1
Authors:
Dean Woodbeck https://orcid.org/0000-0002-0996-1719
Ann West https://orcid.org/0000-0002-8215-4913
Kevin Morooney https://orcid.org/0000-0001-9058-3921
Publication Date: March 25, 2019
Sponsor: Vice President, Trust and Identity and NET+

Table of Contents

Executive Summary

The percentage of organizations meeting the Baseline Expectations rose from 13% in February to 95% by mid-January 2019.

The Internet2 Trust and Identity Division convenes the community to develop software and services that make collaborating easier and more secure.

- InCommon Federation enables access to services
- eduroam Federated Global Wireless enables access to global wireless
- InCommon Certificate Services secures it all through enterprise PKI
- Open source Identity and Access Management suite of software – formerly TIER, now the InCommon Trusted Access Platform
- Engaging the community, through all services, to discuss needs, plans, goals, and proposed directions

Here are the key themes from 2018.

Rebooting the InCommon Federation through required practices and information - For the first time, the InCommon community has developed expectations required of all participants, Baseline Expectations for Trust in Federation. The goal is to improve interoperability and ultimately increase the trust that underlies the federation. Through the leadership of the Community Trust and Assurance Board (CTAB), the year-long community effort to implement the first part of Baseline was a success. The percentage of organizations meeting Baseline Expectations rose from 13% in February to 95% by mid-January 2019.

Completing the final objectives for the TIER program - The three-year TIER program (Trust and Identity in Education and Research) came to a close at the end of 2018, paving the way for the InCommon Trusted Access Platform. TIER architects and developers made significant progress in making the software components easier and much less time consuming to install and configure, and developed API connectors to better enable software interoperability. TIER was made possible by 49 institutions that each provided $25,000 per year for three years. The software development will continue under the InCommon umbrella as part of the new InCommon Trusted Access Platform.

Maturing Operations and Security across services - Significant time and effort went into planning for the next phase of service maturity, reliability, and security. As an example, revamping the Federation Manager software (used by

Executive Summary

Federation participants to manage their information and metadata) made it far easier to use, while also supporting the Baseline Expectations program. Operations also focused on service maturity in the design and delivery of InCommon Federation metadata using InCommon's Per-Entity Metadata (MDQ) service and conducted a security review of the eduroam US service in collaboration with our partners at ANYROAM, LLC. This security review will be used as a basis for determining next steps for the service.

Engaging the Community - Two key working groups provided insight and recommendations: 1) one group focused on simplifying the InCommon onboarding process, and 2) the other looked at the barriers to default release of a small number of attributes, as well as ways to expand the InCommon tent. These insights will help guide the community engagement activities around attribute release policies (which directly affect interoperability) and making it easier for service providers to understand the value proposition and the onboarding process.

Looking ahead to 2019 - Three priorities for 2019 come directly from the working groups mentioned above, as well as a white paper published by the Federated Identity Management for Research Collaborations (FIM4R) international collaboration of research communities and infrastructures: 1) continue to work to integrate the software and the federation to make both easier to use and configure, and 2) significantly improve training and workshops to help participants make the most of the software and services, 3) expanding engagement with research communities.

Introduction

The Internet2 Trust and Identity Division convenes the community to develop software and services that make collaborating easier and more secure.

- InCommon Federation enables access to services
- eduroam Federated Global Wireless enables access to global wireless
- InCommon Certificate services secures it all through enterprise PKI
- Engaging the community, through all services, to discuss needs, plans, goals, and proposed directions.
- Open source Identity and Access Management suite of software – formerly TIER, now the InCommon Trusted Access Platform

This document outlines the major accomplishments for the Internet2 Trust and Identity division in 2018.

Key Themes for 2018

1. Rebooting the InCommon Federation through required practices and information.
2. Completing the final objectives for the TIER program.
3. Maturing Operations and Security across services.
4. Engaging the community in discussing needs, outlining plans and goals, and defining the future direction for the services.

InCommon Federation

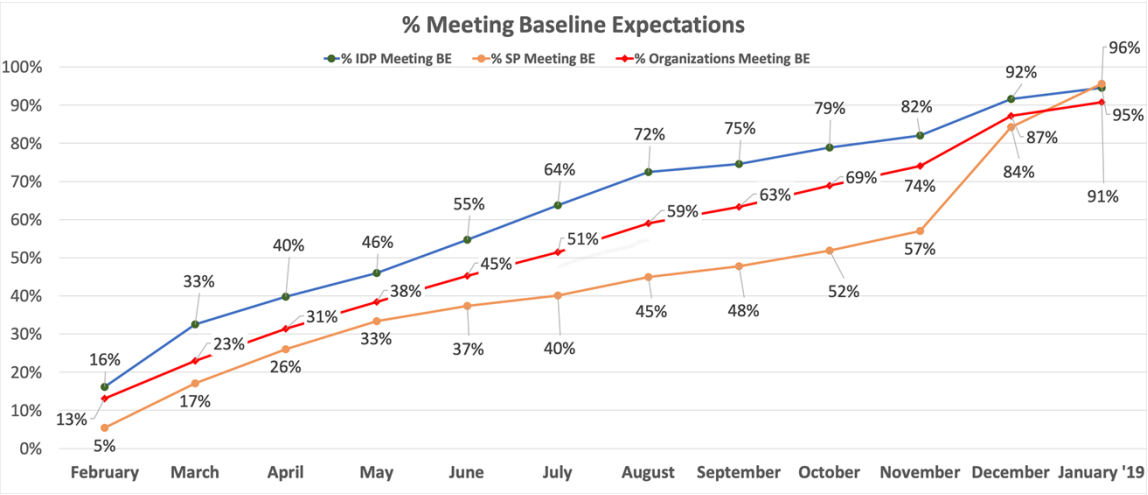
In 2018, Baseline Expectations for Trust in Federation went from an idea to significant adoption.

The InCommon Federation is the U.S. research and education identity federation, providing a common trust infrastructure for shared management of access to online resources. Through InCommon, Identity Providers can give their users national and international single sign-on convenience and privacy protection, while letting online Service Providers focus on controlling access to their protected resources.

Rebooting the Federation: Baseline Expectations for Trust in Federation

In 2018, Baseline Expectations for Trust in Federation went from an idea to significant adoption by InCommon Federation participants. Led by the Community Trust and Assurance Board, with strong support from the InCommon Steering Committee, these requirements for all federation participants will increase trust, improve usability, and provide a better end-user experience.

The community effort and results are nothing short of amazing. Here are the numbers - from just prior to the start of the Baseline Expectations roll-out and then as of the end of January 2019.



Modernizing and Scaling Operations

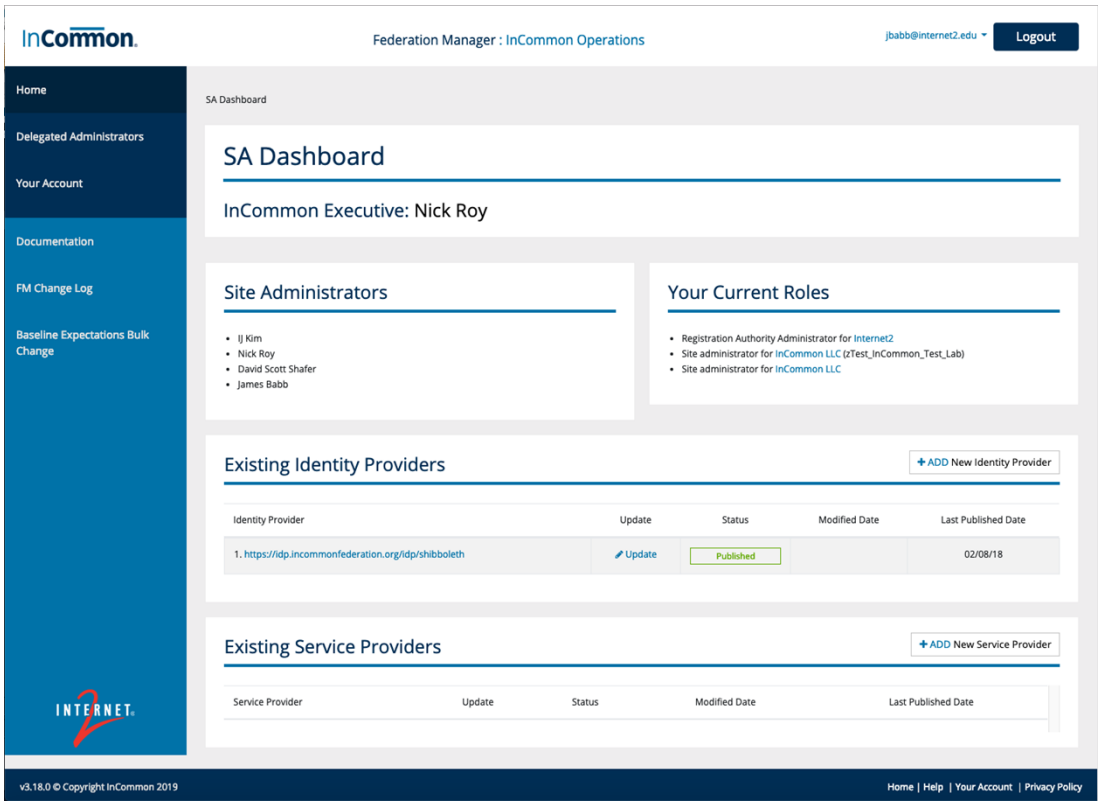
Moving to DevOps and Scaling the Federation

Per the InCommon Operations review of 2015, InCommon made significant progress towards moving the metadata pipeline to using DevOps methodologies. The DevOps approach means that changes and upgrades are deployed as soon as they are ready, rather than waiting for a static release date.

The DevOps process is important, too, in the development of the Per-Entity Metadata project, a new way for scaling the distribution of the trust registry information. Rather than downloading the large metadata aggregate, organizations can query for just the metadata elements that they need. The community requirements for this service are documented in the report from the InCommon Technical Advisory Committee's Per-Entity Working Group report published in December 2016. Since that time, several organizations participated in a pilot, and in 2018 InCommon Operations accomplished the backend work necessary for a production service.

Federation Manager Portal Overhaul

During 2018, InCommon operations made numerous improvements to the Federation Manager portal.



During 2018 InCommon operations made numerous improvements to the Federation Manager portal, the application that site administrators use to keep their metadata up to date:

- A new user interface that is more intuitive and easier to use
- Many changes can now be automatically approved for publication
- Those with multiple service provider entities can do bulk updates of certain metadata elements.

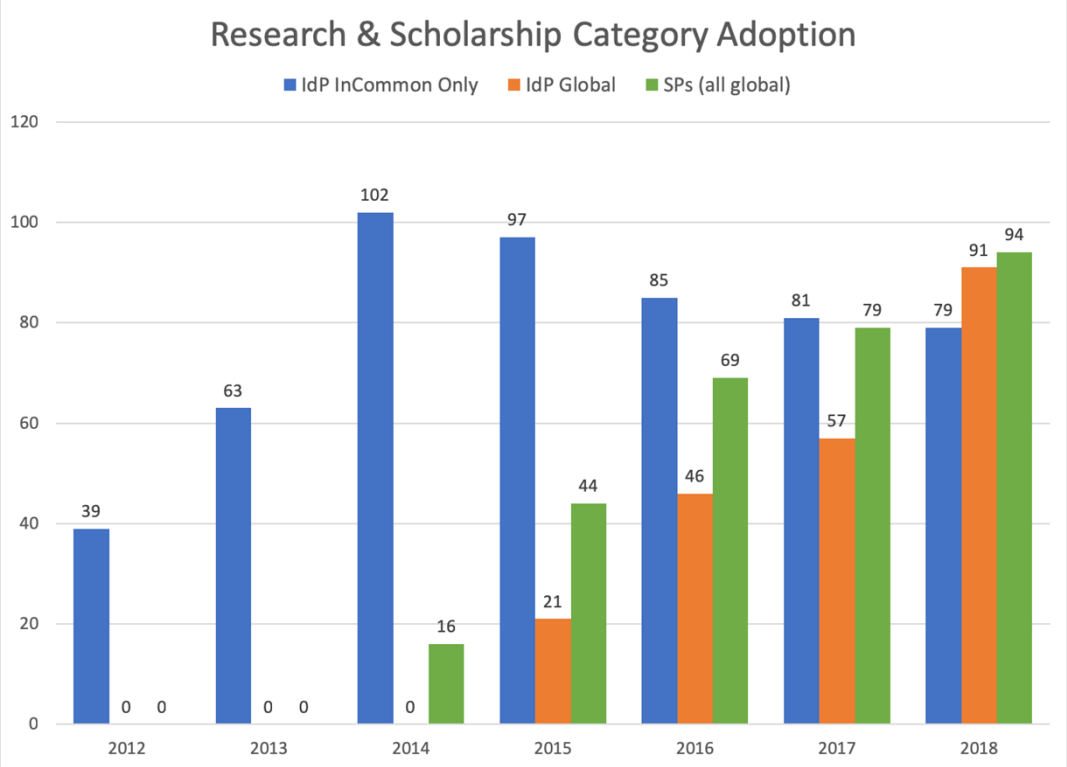
The updated interface also shows site administrators which elements in their metadata do not meet InCommon Baseline Expectations for Trust in Federation, so that they can easily remediate those problems. The Federation Manager also benefits from a DevOps approach, with changes made as they are developed, rather than waiting for a static release date.

Making Collaboration Easier

Using the Research & Scholarship category helps students, faculty, and researchers seamlessly access collaborative and other scholarly resources.

Support for research and academic collaborations is one of the key missions for the InCommon Federation. Toward that end, InCommon continues to strengthen its connections with other research and education federations around the world. The move to Baseline Expectations will provide increased trust and an improved user experience due to the ability to use logos to help users understand the federated login flow.

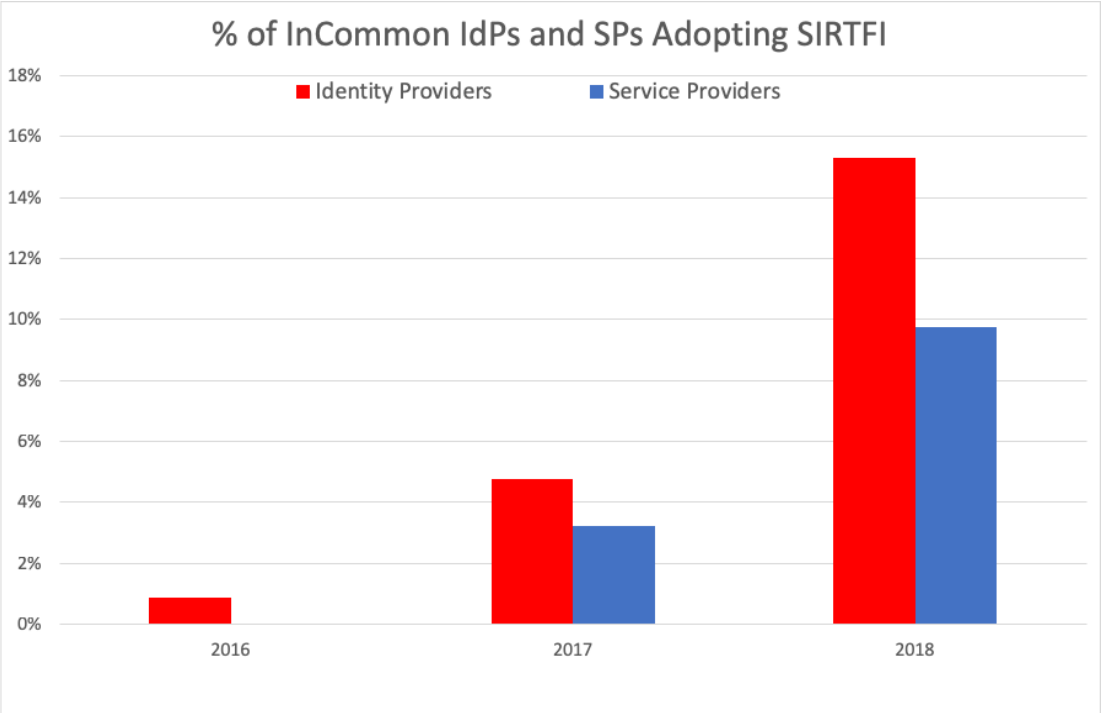
Most federated academic services require a few user attributes to enable login (usually name, email, and an identifier). The REFEDS Research & Scholarship (R&S) entity category was created to meet this need. Federations tag appropriate scholarly services as part of the category, and the identity provider releases the attribute bundle to the entire category. When a new service is added to the category, it automatically receives the needed attributes. This significantly improves the overall user experience and decreases the data release management overhead for IT organizations.



"IdP Global" indicates identity providers that release the R&S attributes to all R&S service providers globally. "IdP InCommon Only" indicates IdPs that release R&S attributes to only R&S service providers registered by InCommon (e.g. in the U.S.).

Securing Your Federation: SIRTFI (Security Incident Response Trust Framework for Federated Identity)

While one requirement of Baseline Expectation is having a security contact in metadata, SIRTFI goes further and provides a framework for coordinating incident response across all federations. The framework covers four areas: operational security, incident response, traceability, and participant responsibilities. It is self-attested by organizations and can serve as a best practices roadmap for secure participation in the federation.



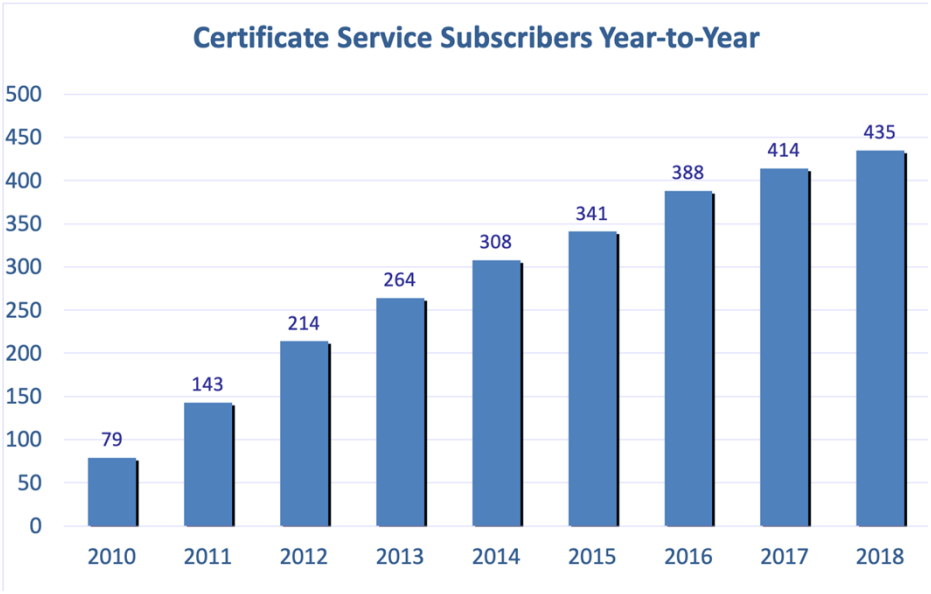
This chart shows the percentage of InCommon identity providers and service providers self-asserting their adherence to SIRTFI (Security Incident Response Trust Framework for Federated Identity) since the framework's release in 2016.

InCommon Certificate Service

The InCommon Certificate Service provides unlimited certificates (SSL, EV, client, and others) for one annual fee. Toward the end of the year, the underlying certificate vendor, Comodo, underwent a reorganization and renaming process and is now Sectigo.

Key accomplishments in 2018 for the Certificate Service are listed below. The work is driven, in part, by a bi-annual Certificate Service survey, which attracted 164 responses in 2018.

- Subscribers to the service are now able to authenticate using **SAML-based SSO**. In addition, organizational administrators are required to use multi-factor authentication (MFA) when logging in using SSO.
- Sectigo implemented a **dedicated validation support queue** for InCommon subscribers (ccmvalidation@sectigo.com).
- There is now a **status page** for monitoring the Sectigo Certificate Manager system.
- A **stronger Service Level Agreement**, including incentive money for achieving the stated goals, was implemented in the latest contract renewal with Sectigo.



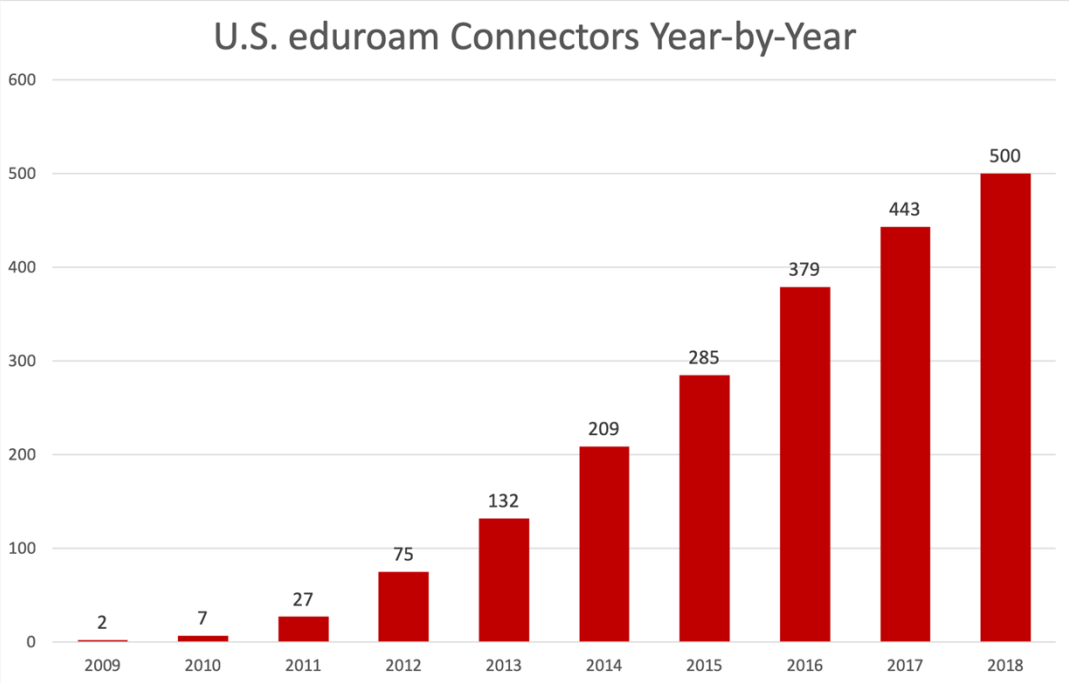
eduroam: Global Federated WiFi

During 2018, Internet2 and ANYROAM rolled out new eduroam hardware and moved to continue to improve operations.

eduroam is a secure global wifi roaming service for the international research and education community, operated by GÉANT. Internet2 is the U.S. node for the service (serving more than 600 organizations). eduroam allows individuals to use their home institutional credentials to connect to wireless at all other eduroam institutions.

During 2018, Internet2 with its partner ANYROAM:

- rolled out new hardware for eduroam operations and conducted a security assessment.
- developed a comprehensive service definition to clarify roles and responsibilities as the next step in improving and enhancing the service.
- completed a service survey of the community of eduroam connectors, which will inform our plans as we continue to grow the service.



Identity and Trust Software Development

The three-year TIER effort successfully concluded at the end of 2018, having significantly reduced the time and effort to install and configure the IAM software suite.

This year marked the successful conclusion of the three-year effort to mature, modernize and sustain the community-developed open-source software solutions (Shibboleth, Grouper and COmanage - with some others joining along the way). Results of the TIER (Trust and Identity in Education and Research) program include:

- Containerizing the software components, significantly reducing the time and effort needed for installation, configuration, and upgrades
- Developing APIs and other tools to improve the interoperability among the components
- Creating reference implementations of combined components to provide a baseline for other implementations
- Developing a Grouper Deployment Guide and a Grouper Training Environment
- Developing a graphical user interface for the Shibboleth Identity Provider software
- Developing of the Campus Success Program (see below) to accelerate adoption

Community members and Internet2 staff provided thousands of hours, and 49 schools each provided $25,000 per year for three years, to make the effort successful.

The TIER progress led to the development of the new InCommon Trusted Access Platform, an IAM suite meeting the specific needs of research and education.

Adoption: Campus Success Program

Through the TIER (Trust and Identity in Education and Research) Campus Success Program (CSP), 10 higher education institutions significantly accelerated the adoption path for the TIER IAM suite. The campuses formulated work plans, met regularly with subject-matter experts to implement those plans, and worked together to address issues along the way. These schools' documented experiences will help the rest of the trust and identity community with adoption and implementation.

Identity and Trust Software Development

By engaging in face-to-face meetings and with TIER working groups, CSP participants uncovered issues and shared best practices. As a result, solutions could be implemented much faster than working alone.

Several campuses moved all (or a portion of) their project plans into production, others landed in a test environment, and some progressed to a point of better understanding of requirements and necessary resources to bring plans to fruition. Universally, the cohort agreed that one of the most valuable outcomes was the underlying community of practice that developed during the program.

The CSP concluded at TechEx 2018, when participants shared the outcomes of their project plans and lessons learned during the inaugural program. The final report, along with campus case studies are on the wiki.

The program provided guidance on a variety of education and engagement opportunities that could help others in adopting the software. It will serve as a key piece of the next generation education and adoption programs.

Engaging the Community

Trust and Identity convenes the community to develop requirements, specifications, and program activities in the form of working groups and advisory groups.

Document Stewardship Framework

The higher education trust and identity community has produced a wealth of helpful documents over the past two decades. As websites and wikis evolve and working groups complete their work, sometimes those documents became challenging to locate and revisions confusing to track. One priority in 2018 was development of a document repository to help solve this problem.

Community Recommendations and Reports of Note

Several working group reports were completed in 2018, the results of which are being complied and integrated into the InCommon work plan where appropriate. For a complete listing of all working groups, see the next section and Appendix B:

International Research Requirements can be found in the FIM4RV2 Assessment for Internet2 Trust and Identity written by Community Architecture Committee for Trust and Identity, the standing architecture group that advises the VP for Trust and Identity. This document is a gap-fit analysis of the international Federated Identity Management for Research document which reflects the efforts of more than 20 Research Communities from around the world that have collaborated over the last year to define a common vision for the future of Federated Identity Management for Research.

Attributes for Federation and Collaboration - This working group was co-chartered by InCommon Steering and its two advisory committees to explore the slower-than-expected adoption of the Research & Scholarship Entity Category. The category is intended to simplify collaboration access for faculty and researchers. The working group surveyed and interviewed more than 130 organizations and explored the reasons that R&S-compatible attribute release policies are not in place at most campuses, identified a number of concerns, and the final report made several recommendations to address the problem of attribute release.

Streamlining Service Provider Onboarding - This working group was chartered by the InCommon Technical Advisory Committee to examine the onboarding process for service providers and made recommendations to streamline the process. The group's approach was to make the onboarding material more readable, easier to navigate, and organized in the form of an onboarding walkthrough. You can read a summary from working group chair Garrett King, and/or read the group's final report.

Working Groups

Appendix B includes a list of the working groups, their charters, links to wiki pages and reports, and a summary of their work in 2018.

InCommon and TIER Working Groups

InCommon Working Group	Chair	Working Group Materials
OIDC/OAuth Deployment Working Group	Nathan Dors, University of Washington	https://spaces.internet2.edu/x/jJiTBg
Deployment Profile Working Group	Keith Wessel, University of Illinois Urbana-Champaign	https://spaces.internet2.edu/x/WoIQBg
Streamlining SP Onboarding Working Group	Tommy Roberson, Baylor University; and Garrett King, Carnegie Mellon University	https://spaces.internet2.edu/x/iJiTBg
Attributes for Collaboration and Federation Working Group	Brad Christ, Eastern Washington University	https://spaces.internet2.edu/x/ipiTBg

TIER Working Group	Chair	Working Group Materials
TIER Data Structures and APIs Working Group	Keith Hazelton, University of Wisconsin-Madison	https://spaces.internet2.edu/x/SgFwBQ
TIER Packaging Working Group	Jim Jokl, University of Virginia	https://spaces.internet2.edu/x/JYV4BQ
TIER Entity Registry Working Group	Warren Curry, University of Florida Benn Oshrin, Spherical Cow Group	https://spaces.internet2.edu/x/gYKeBQ
TIER Component Architects Working Group	Steve Zoppi, Internet2	https://spaces.internet2.edu/x/RAFwBQ
Big Ten Academic Alliance and TIER Collaboration on Provisioning and De-provisioning	Keith Wessel, University of Illinois at Urbana-Champaign	https://spaces.internet2.edu/x/DANhBg

Governance and Advisory Groups

Trust and Identity Division

Trust and Identity Program Advisory Group - The Trust and Identity Program Advisory Group (PAG) provides community management-level input and guidance to the Vice President for Trust and Identity and NET+ for the creation and direction of division programs and services including, but not limited to, InCommon Federation and Certificate Services, the TIER program, and eduroam.

Key topics discussed in 2018 include:

- The transition from the completion of the TIER program to the next steps for the continued development and funding of the containerized open-source software.
- Related to the bullet above, feedback on the development of the InCommon fee change proposal.
- Expanding the scope of the PAG for 2019.

Community Architecture Committee for Trust and Identity (CACTI) - CACTI (Community Architecture Committee for Trust and Identity) is an architecture strategy group of community members to advise the Vice President for Trust and Identity and NET+. CACTI provides strategic architectural input for trust and identity, and manages and evolves community standards, among other duties.

Key work included developing a comparison between requirements in FIM4Rv2 (see above) and current policies, practices, and initiatives within Internet2 Trust and Identity Services; and recommended courses of action to provide better alignment.

InCommon Federation

InCommon Steering Committee - The InCommon Steering Committee is responsible for managing the business affairs of InCommon, including oversight and recommendations on issues arising from the operation and management of InCommon. Policies and practices approved by the Steering Committee are available on the policies page of the InCommon website.

Key topics discussed in 2018 include:

- With the completion of the TIER program, moving the funding source for the IAM suite to InCommon.
- Development of a proposed fee change to support the ongoing development of the IAM suite and provide Shibboleth support for InCommon participants.
- Approving the necessary changes to the InCommon Participation Agreement to enable the Baseline Expectations for Trust in Federation, which saw significant adoption during 2018.
- Chartering and supporting the recommendations of the Attributes for Collaboration and Federation Working Group, which was charged with looking at ways to improve interoperability.

Engaging the Community

InCommon Community Trust and Assurance Board - The Community Trust and Assurance Board (CTAB) represents the InCommon community with issues and programs related to trust and assurance. The CTAB is an advisory body to the InCommon Steering Committee.

> **During 2018,** CTAB rolled out the Baseline Expectations for Trust in Federation program, which it had developed over the preceding year. As noted elsewhere above, adoption of Baseline Expectations was very successful, with the percentage of organizations meeting Baseline rising from 13% to more than 90% during 2018.

InCommon Technical Advisory Committee - The InCommon Technical Advisory Committee (TAC) supports InCommon's mission "to create and support a common framework for trustworthy shared management of access to online resources." It is an advisory body to the InCommon Steering Committee and provides advice on operational roadmap.

> **Four major TAC working groups** operated during 2018:
>
> - OIDC-OAuth Deployment Working Group - bringing together community members to develop and propose standard deployment practices (see Appendix B below).
> - Deployment Profile Working Group - developing a deployment profile that describes required and recommended practices for IdPs and SPs operating in the higher education and research community (see Appendix B below).
> - Streamlining SP Onboarding Working Group - This group delivered these items: an InCommon Service Provider Onboarding criteria document, an SP Onboarding questionnaire, and a primer that describes core concepts involved in participating in InCommon.
> - Attributes for Collaboration and Federation Working Group – This group did an extensive review of the reasons why default attribute release policies are not in place at man campuses (that is, why they are not releasing directory information) and explored other ways to improve interoperability.

Software Development

TIER Community Investor Council (TCIC) - In 2015, 49 colleges and universities made a three-year financial commitment for TIER and formed the TIER Community Investor Council (TCIC) to guide planning, development, and priority-setting. The funding began in 2015 and ended in December 2018 and the TCIC disbanded.

TIER Component Architects - This group includes the lead developers and working group chairs involved in the TIER program. Advisory to the Internet2 associate vice president of integration and architecture, this team develops specifications through the convening of working groups, then ensures those are included in the software.

TIER Working Groups – A report delivered at the end of 2017 demonstrates the sheer amount of community time and effort that drove TIER, with an extensive list of software improvements and development plans. See Appendix B for a summary of the TIER working groups and their work in 2018.

Education Programs

The Trust and Identity division offers several opportunities to learn more and engage with your community peers.

IAM Online Webinar Series - The monthly IAM Online webinar series marked its ninth year of operation in 2018. Appendix C includes a list of topics and speakers. In a partnership with GÉANT, archived sessions are available on an IAM Online YouTube channel.

InCommon Shibboleth Installation Workshops - The InCommon Shibboleth Installation Workshops marked the ninth year of operation. Three workshops took place in 2018 with a total attendance of 88 participants. See Appendix D for details.

2018 Internet2 Global Summit - The 2018 Internet2 Global Summit, held in San Diego, California, featured a series of showcase sessions featuring the work of the Campus Success Program schools, an overview "Trust and Identity at Internet2: Delivering Services and Software for Access and Collaboration," and a series of bird-of-a-feather and working group meetings.

2018 Internet2 Technology Exchange - In its fifth year, the Internet2 Technology Exchange (TechEx) is an important technical meeting for trust and identity in research and education in the U.S., with a significant global component and attendance. The trust and identity community combined three focused meetings into the 2018 TechEx: REFEDS, the conference for research and education identity federations worldwide; Advance CAMP, the unconference meeting that explores just-in-time issues and challenges of community-wide interest or concern; and two tracks of Trust and Identity sessions, with campus-focused sessions comprised of community proposals. Approximately 200 trust and identity professionals attended the meeting.

Conclusion and Looking Ahead

The Baseline Expectations for Trust in Federation effort demonstrated that the community values the Federation and the trust it provides. The first phase introduced in 2018 focused on required elements in the InCommon metadata. For 2019, the Community Trust and Assurance Board will focus on those organizations that do not yet meet the Baseline metadata requirements. CTAB is also developing a roadmap for the next phase of Baseline, which may include error URLs, and configuring of multi-factor authentication so that it will work in federated use cases.

Other priorities for 2019 come directly from CACTI's response to the research FIM4R report, the Streamlining SP Onboarding Working Group and the Attributes for Collaboration and Federation Working Group. In general, all focused on ways to make Federation easier - from the onboarding process to encouraging attribute release policies that make collaboration seamless.

Other key findings, reinforced by the results of the TIER program, are to continue work to integrate the TIER software (now known as the InCommon Trusted Access Platform) and make it easier to use and configure.

The three-year TIER program has come to a close at the end of 2018, but the work will continue. Community developers and subject matter experts made significant progress in making the software components easier to install and configure, and developed API connectors to better enable software interoperability.

While the three-year program has ended, it provides a solid foundation for continued work on the open-source IAM suite. The software moves under the InCommon umbrella as the InCommon Trusted Access Platform. As part of its commitment to sustaining the software and accelerating adoption, InCommon will significantly expand learning and support opportunities, including development of online components, to help participants make the most of the software and services.

Appendix A: Newsletters and Reports

Trust and Identity Newsletters

February 2018
March 2018
April 2018
June 2018
August 2018
September 2018
November/December 2018

Campus Success Program Case Studies and Final Report

- Colorado School of Mines
- Colorado State
- Georgia Tech
- Lafayette College
- Oregon State University
- Rice University
- University of California-Merced
- University of Illinois
- University of Maryland Baltimore County
- University of Michigan
- Program Final Report

Appendix B: 2018 Active Working Groups

InCommon OIDC/OAuth Deployment Working Group
Chartered by: InCommon Technical Advisory Committee
Chair: Nathan Dors, University of Washington
Wiki: https://spaces.internet2.edu/x/jJiTBg

A survey confirmed that there is already substantial use of the OIDC/OAuth2 protocols by campuses. Using these protocols is substantially less mature in the higher education environment than the SAML protocols that have been used for the last 15 years. This working group brings together current users to develop and propose standard deployment practices in order to improve the likelihood of interoperation "just working."

InCommon Deployment Profile Working Group
Chartered by: InCommon Technical Advisory Committee
Chair: Keith Wessel, University of Illinois, Urbana-Champaign
Wiki: https://spaces.internet2.edu/x/WoIQBg

This working group was chartered to develop a deployment profile that describes required and recommended practices for IdPs and SPs operating in the higher education and research community. The working group developed a profile to update the SAML V2.0 Interoperability Deployment Profile (SAML2-int) and is completing its final report.

InCommon Streamlining SP Onboarding Working Group
Chartered by: InCommon Technical Advisory Committee
Chairs: Tommy Roberson, Baylor University; Garrett King, Carnegie Mellon University
Wiki: https://spaces.internet2.edu/x/iJiTBg

The working group delivered its final report in August 2018 with three deliverables: an InCommon Service Provider Onboarding criteria document, an SP Onboarding questionnaire, and a primer that describes core concepts involved in participating in InCommon.

Appendix B: 2018 Active Working Groups

Attributes for Collaboration and Federation Working Group
Chartered by: InCommon Steering Committee
Chair: Brad Christ, Eastern Washington University
Wiki: https://spaces.internet2.edu/x/ipiTBg

This working group delivered its final report in August 2018. The group surveyed and interviewed more than 130 organizations examining participation or planned participation with the Research & Scholarship Category of Service Providers. “Participation” among identity providers involves releasing a small number of attributes (directory information) to all services in the R&S category (which are vetted by InCommon or other federations). The working group explored the reasons that such default attribute release policies are not in place at most campuses. The group identified a number of concerns and made several recommendations to address the problem of attribute release.

TIER Data Structures and APIs Working Group
Chair: Keith Hazelton, University of Wisconsin-Madison
Wiki: https://spaces.internet2.edu/x/SgFwBQ

TIER Entity Registry Working Group
Chairs: Warren Curry, University of Florida; Benn Oshrin, Spherical Cow Group
Wiki: https://spaces.internet2.edu/x/gYKeBQ

During 2018, the TIER Data Structures & API Working Group and TIER Entity Registry Working Group focused on provisioning/de-provisioning, de-duplication of identities, and a number of other priorities to complete the work set forth in the TIER Accomplishments by Thematic Groups. Some of the specifics include:

- Supporting the development of the Grouper Training Environment
- Providing demonstrations at the Global Summit Trust and Identity Showcase sessions
- Supporting the TIER Campus Success Program
- Collaborating with the Big Ten Academic Alliance on the TIER Provisioning Fit/Gap
- Developing a TIER-style container for messaging between software components
- Developing guidance and architectural considerations for Grouper and midPoint integrations

Appendix B: 2018 Active Working Groups

TIER Packaging Working Group

Chair: Jim Jokl, University of Virginia
Wiki: https://spaces.internet2.edu/x/JYV4BQ

During 2018 the TIER Packaging working group focused on refining the packaging for the software containers to further streamline and simplify the TIER components. Specifics include:

- Completing specification for the design of TIER-compatible Docker containers
- Developed the TIER Grouper container with associated documentation
- Worked with the Shibboleth UI development team on a container for that application
- Worked with Evolveum to develop a TIER midPoint container
- Developed logging standards for TIER containers
- Developed a RabbitMQ container specification for messaging between TIER components
- Supported the TIER Campus Success Program in understanding and working with the TIER packages

Big Ten Academic Alliance and TIER Collaboration on Provisioning and De-provisioning

Chair: Keith Wessel, University of Illinois
Wiki: https://spaces.internet2.edu/x/DANhBg

The Big Ten Academic Alliance developed a survey to collect information on products specializing in provisioning and de-provisioning for comparison and evaluation. The results will help create best practices and provide a product comparison for those getting ready to implement a provisioning solution.

- Developed a product evaluation template that also summarizes current evaluations
- Supported the TIER Campus Success Program by completing a set of use cases for a bulk provisioning API.
- Created a GitHub repository for collecting System for Cross-domain Identity Management (SCIM) schema requirements, which contains a JavaScript Object Notation (JSON) version of the SCIM core schema.

Appendix C: IAM Online Topics

IAM Online is a monthly series delivering interactive education on Identity and Access Management (IAM), sponsored by InCommon, Internet2, and the EDUCAUSE Higher Education Information Security Council. An archive of IAM Online presentations is available on the IAM Online YouTube channel.

OpenID Connect and OAuth in the R&S Community (December 12, 2018)
Moderator: Nathan Dors, University of Washington. Presenters: Rachana Ananthakrishnan, Globus; Roland Hedberg, Catalogix; David Vaghetti, Consortium GARR; Albert Wu, InCommon/Internet2

IAM Access Governance and Grouper 2.4 (September 12, 2018)
Moderator: Michael Gettes, University of Florida. Presenters: Chris Hyzer, University of Pennsylvania; Bill Thompson, Lafayette College

Identity Matching: How to Know Who's Who (or, Will the Real John Smith Please Stand Up?) (August 8, 2018)
Moderator: Keith Wessel, University of Illinois at Urbana-Champaign. Presenters: Benn Oshrin, Spherical Cow Group; Summer Scanlan, University of California, Berkeley

Managing Affiliate, Alumni, and Other Identities with COmanage (April 18, 2018)
Moderator: Benn Oshrin, Spherical Cow Group. Presenters: Jeff Ruch, Colorado State University; Janemarie Duh, Lafayette College

Managing IAM Roles and User Access: How to Herd Cats (February 14, 2018)
Moderator: Keith Wessel, University of Illinois at Urbana-Champaign. Presenters: Brett Bieber, University of Nebraska-Lincoln; Ester Cha, University of Illinois at Urbana-Champaign; DePriest Dockins, University of Michigan

Campus Cyberinfrastructure Plans and Enabling Access for Academic Collaborations (January 9, 2018)
Moderator: Ann West, InCommon/Internet2. Presenters: Tom Barton, University of Chicago; Melissa Woo, Stony Brook University

Appendix D: InCommon Shibboleth Installation Workshops

2018	Host	Attendees (max = 40)
May	Unicon	20
July	University of Pittsburgh	30
November	Brown University	38
Total		88

Appendix E - Glossary of Terms and Acronyms

AAC - Assurance Advisory Committee - Now succeeded by the CTAB (see below), the AAC provided leadership and oversight of the InCommon assurance program. See www.incommon.org/assurance.

Baseline Expectations - Baseline Expectations for Trust in Federation - A set of common expectations that all Participants meet, intended to make collaboration more predictable and improve the user experience. See www.incommon.org/federation/baseline/

CACTI - Community Architecture Committee for Trust and Identity - CACTI is an architecture strategy group of community members to advise the Vice President for Trust and Identity and NET+.

CSP - Campus Success Program (2018); Collaboration Success Partners (2019) - A diverse group of higher education institutions committed to adopting and deploying the TIER software components and helping to accelerate adoption for the rest of the trust and identity community. See https://spaces.internet2.edu/x/oQrABg. Transitioning to Collaboration Success Partners in 2019.

CTAB - Community Trust and Assurance Board - CTAB represents the InCommon community in InCommon's trust and assurance related programs and initiatives. It is advisory to the InCommon Steering Committee.

Certificate Service - InCommon Certificate Service - A program offering enterprise-scale server and other certificates. Subscribers receive unlimited certificates for one annual fee, including all domains owned or controlled by the institution. Available to US higher education institutions and not-for-profit research and education networks. See www.incommon.org/certificates

Docker Container - A lightweight, stand-alone, executable package of a piece of software that includes everything needed to run the software. It operates regardless of the environment. The TIER program is packaging all components in Docker containers to simplify installation and configuration.

eduGAIN - An interconnection of identity federations around the world, simplifying access to content, services and resources for the global research

and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorization. See www.incommon.org/edugain.

eduroam - A global wireless network access service developed for the international research and education community. eduroam allows students, researchers, faculty, and staff secure seamless wireless access at all participating institutions. See www.incommon.org/eduroam.

IAM - **Identity and Access Management** - IAM refers to a framework of policies and technologies for ensuring that the proper people in an enterprise or virtual organization have the appropriate access to the right technology resources.

IdP - Identity Provider - The originating location for a user. For InCommon, an IdP is a campus or other organization that manages and operates an identity management system, including single sign-on that allows members of its community to access protected resources.

MFA - Multifactor Authentication - A security system in which a user must provide at least two methods for authentication - say, something you know and something you have - in order to verify identity and gain access to resources.

OAuth - OAuth is an open standard for access delegation. See https://en.wikipedia.org/wiki/OAuth

OIDC - Open ID Connect - OIDC is an identity layer that allows for the verification of an end-user's identity. It sits on top of the OAuth protocol. See openid.net/connect/

PAG - Program Advisory Group - An Internet2 Program Advisory Group (PAG) provide community input to advise and guide the creation and direction of Internet2 programs and services. The Trust and Identity PAG advises the Vice President of Trust and Identity Services. See https://www.internet2.edu/vision-initiatives/governance/program-advisory-groups/

R&S - Research & Scholarship Category of Service Providers - The Research and Scholarship Entity Category (R&S) is an international specification that provides a simple and scalable way for Identity Providers to release a small set of attributes, or information, to an entire group of Service

Appendix E - Glossary of Terms and Acronyms

Providers serving the Research and Scholarship Community. Service Providers are vetted prior to being added to the category. See refeds.org/research-and-scholarship.

REFEDS - Research and Education FEDerations - REFEDS is a voice that articulates the mutual needs of research and education identity federations worldwide. See refeds.org for more information.

SIRTFI - Security Incident Response Trust Framework for Federated Identity - Enables the coordination of incident response across federated organizations. This framework comprises a list of assertions to which an organization can attest. See refeds.org/sirtfi.

SP - 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.

SP - Service Provider - An InCommon Service Provider is a campus, research organization, or commercial organization that makes online resources available to users via federated identity.

TAC - InCommon Technical Advisory Committee - An advisory body to the InCommon Steering Committee providing advice on InCommon's operational processes and practices, strategies, capabilities, and roadmap. See https://spaces.internet2.edu/x/Swk

TIER - Trust and Identity in Education and Research - Internet2's Trust and Identity in Education and Research (TIER) program is a community-driven, consistent approach to identity and access management. TIER aims to simplify campus processes and advance inter-institutional collaboration and research. See www.internet2.edu/tier

VM - Virtual Machine - An emulation of a computer system; in this case providing the ability to execute programs in a platform-independent environment.