2017 Internet2 Trust and Identity Accomplishments

March 13, 2018

Table of Contents

Executive Summary

Support for collaboration, maturing delivery of software and services, and expanding and enhancing community trust were the three overarching themes for the Internet2 Trust and Identity division during 2017.

InCommon: InCommon Federation activities focused on collaboration, security, expansion and maturation. Examples include ramping up support for academic collaboration, supporting a global security incident program (SIRTFI), easing the joining process for research service providers, looking forward to the next generation federation technology, and conducting a pilot in supporting federation for the long-tail of the education sector. Most notably, InCommon began the move towards requiring a baseline of trust across all Participants as defined, developed and promulgated by the new Community Trust and Assurance Board.

Regarding operations, InCommon published the final *InCommon Security Incident Handling Framework*, began production support for community framework for incident response, and significantly modernized the services that support Federation operations.

Software and Services: TIER IAM suite architects and developers planned, designed and implemented a continuous release pipeline and moved to a container approach for software delivery, with an eye toward both simplification and sustainability. One outcome was a reduction in the time required to install the Shibboleth Identity Provider from hours to minutes. The TIER Program conducted a mid-term survey and identified adoption as a key next step, and ten schools volunteered to collaborate with each other on their implementations.

On the services side, the Trust and Identity division addressed key business and sustainability challenges with eduroam federated wireless service, a complementary service to InCommon, by implementing a new subscription-based business model. Finally, the option of having multi-factor secured single sign-on for those organizations with an InCommon identity provider was added to the InCommon Certificate Service.

Engaging the Community: Two new top-level advisory groups were established to advise the vice president for trust and identity: a policy program advisory group, and an architecture advisory group to look across the software and services landscape. Four new InCommon working groups reviewed topics ranging from attribute release to educating new service providers to deployment guidance for new Participants. The TIER working groups spent hundreds of person-hours to continue assessing community needs and refining the software and the develop process. The Campus Success Program involves 10 campuses that will work together to adopt one or more software components in the TIER IAM suite and develop documentation to help others.

Looking ahead to 2018, Internet2 and InCommon will engage the trust and identity community in determining the next steps for the IAM suite development and adoption, implementing Baseline Expectations, and scaling metadata delivery for InCommon.

Introduction

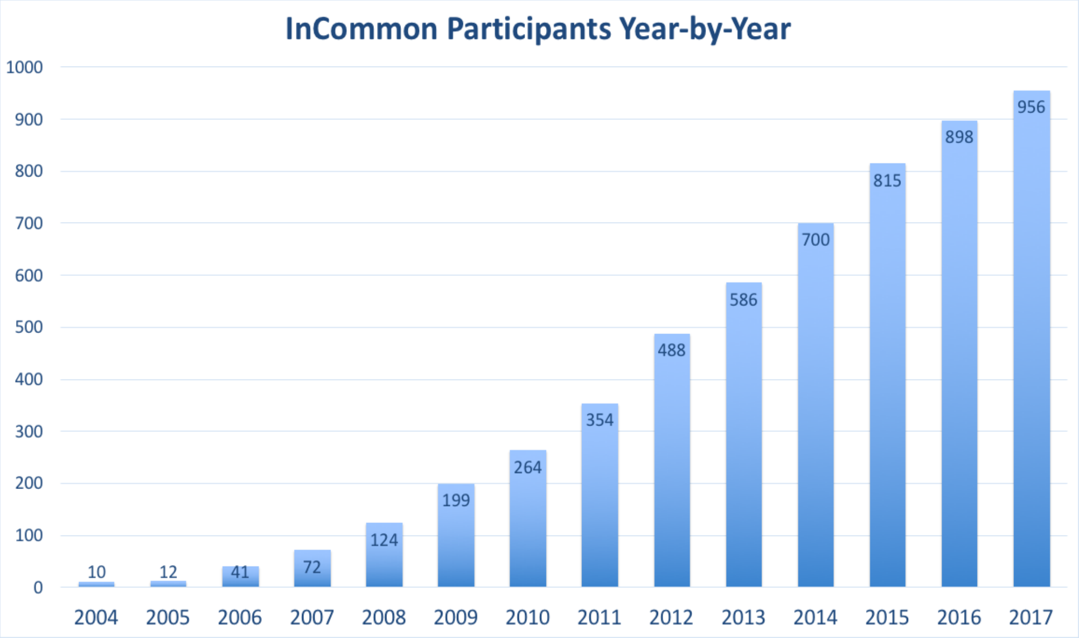
The first full year of the Trust and Identity division at Internet2 (2016) included a significant amount of planning and positioning of services and software development for a sustainable future. In 2017, we began turning those plans into reality.

For the InCommon Federation, key priorities included hardening federation operations for sustainability, scaling for increased demand, and maturing the Federation service delivery to key constituencies. An InCommon fee increase, effective in 2017, funded additional staff to focus on scaling and responding to community requirements and needs. The community made substantial progress in raising the trust level and interoperability of the Federation with the introduction of Baseline Expectations for Trust in Federation. This, along with other emphases on improving collaboration readiness (such as the Research & Scholarship category and the SIRTFI program), have positioned InCommon to deliver on the planning priorities identified in 2016.

Key priorities for the TIER program included continued development of the software components in a way that makes them easier to deliver and install, while planning for the next stage of development during this second of a three-year funding commitment by investor universities. In 2017, the community of architects and developers moved to a container-based approach for software delivery, with an eye toward both simplification and sustainability. The TIER investor community also allocated funds for a program to jump-start adoption: the Campus Success Program.

InCommon Federation

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.



Responding to Community Needs

The fee increase allowed InCommon to fill key operational staff roles in security, operational support, and project management, providing for increased attention to security and scaling of the Federation. Community involvement, in the form of working groups and advisory groups, continues to provide a robust foundation for defining and meeting community needs. The Baseline Expectations program, for example, was driven by the Community Trust and Assurance Board, and four InCommon working groups tackled key issues (see Appendix C for working group details).

Ready for Collaboration

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. The following activities conducted in 2017 underscore this need.

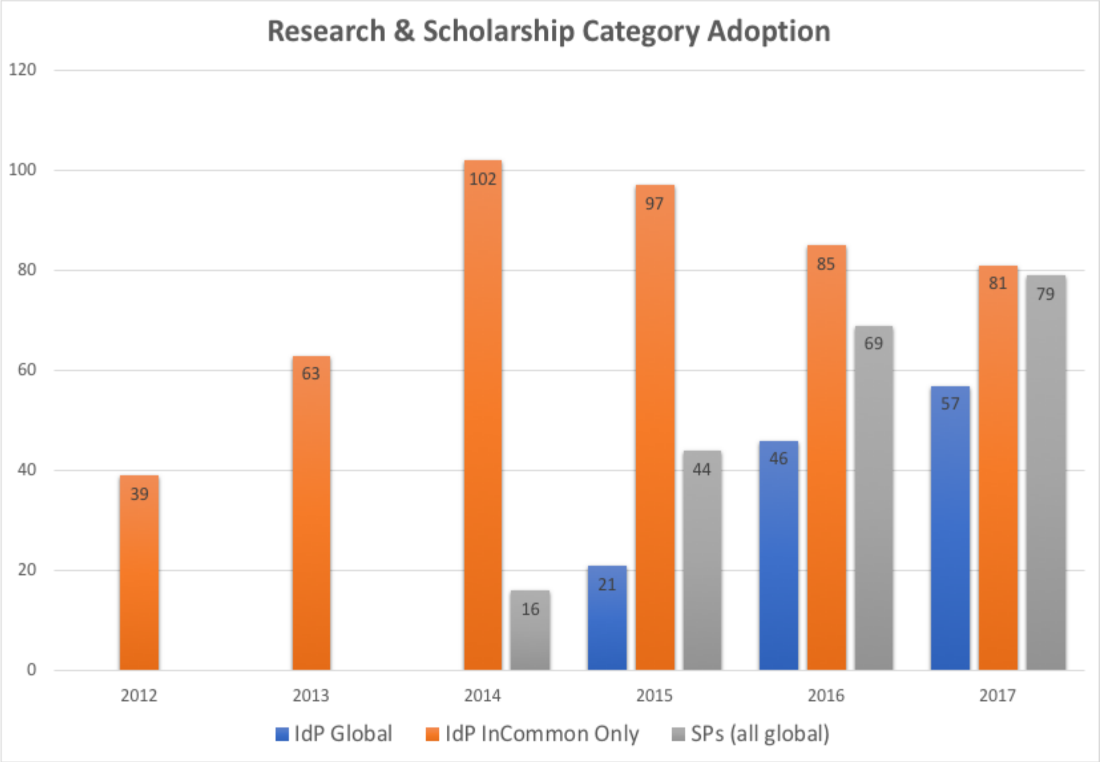
National Science Foundation Requires InCommon for Cyberinfrastructure Plans - One key purpose of the InCommon Federation is to provide seamless access to collaboration tools and services, particularly for faculty, scientists, and researchers. This was reinforced in late 2017, when the **National Science Foundation** included some InCommon requirements in their call for proposals for Campus Cyberinfrastructure program grants.

Raising Confidence in the Federation: Baseline Expectations for Trust in Federation - With approval by the InCommon Steering Committee in December 2017, the community has begun adoption of Baseline Expectations for Trust in Federation. The expectations, developed by the Community Trust and Assurance Board (see below), will increase trust among all InCommon Federation participants and will improve usability by ensuring all metadata includes certain elements aimed at a better user experience (orienting logos and privacy policies, for example).

Maintaining Community Trust: Formation of Community Trust and Assurance Board (CTAB) - The Assurance Advisory Committee revised its charter and adopted a new name to reflect the expanded responsibilities. The CTAB worked for more than a year to develop the Baseline Expectations for Trust in Federation and has turned its attention to developing the community consensus process for interpreting the expectations, and the dispute resolution process.

Securing Your Federation: SIRTFI (Security Incident Response Trust Framework for Federated Identity) - During 2017, the InCommon Federation began supporting SIRTFI in production. An upgrade to the Federation Manager portal, used by site administrators, made it more straightforward for an organization to self-assert compliance with SIRTFI. The specification includes all participants having a security contact in metadata. InCommon encourages all participants to adopt the SIRTFI specification, and the Baseline Expectations program requires a security contact in metadata, too.

Collaborating Locally and Around the World: Research & Scholarship Category - The InCommon Federation continues to encourage all Identity Providers to support the Research & Scholarship (R&S) category by releasing a small attribute bundle to the category. Whenever a service is vetted and added to the R&S category, that service automatically receives the appropriate attributes. This significantly increases the usability for faculty and researchers using collaboration tools and services.



Note on chart: "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.). One goal is remove the legacy InCommon Only category to improve interoperability and user experiences.

Helping the Service Providers: Changing to Domain Validation Process - During 2017, the InCommon Federation changed its policy and now accepts a greater number of ways for an organization to prove control of a domain name.

This eases the burden, in particular, on service providers that operate services on behalf of the identity provider. This will reduce the time to register new hosts in the federation, but in particular benefits collaboration and research-related service providers.

Investigating the Next Gen Federation: OIDC/OAuth Survey Working Group Reports Strong Interest - The OIDC/OAuth Survey Working Group surveyed the higher education community to identify use cases and gauge interest in the adoption of this authentication/authorization protocol. In its report, issued in April 2017, the working group confirmed a strong community interest in OIDC/OAuth and recommended that the InCommon Federation and the TIER component architects move toward supporting this technology.

Enabling K12 and Community Colleges to Leverage Federation: InCommon Steward Program Proof of Concept - InCommon and MCNC, the North Carolina research and education network, launched a proof of concept of the InCommon Steward Program in December 2016 with the goal of extending federation to K-14 schools. InCommon and MCNC issued a six-month report in July 2017, documenting the lessons learned thus far and initiating a business development phase. Partnering with the research and education networks enables organizations with little identity support to leverage federation and its benefits.

Maturation and Making Your Federation Stronger

InCommon made significant strides in maturity this year, recognizing that the Federation has become a strategic infrastructure for many participants. During 2017, InCommon added staff in critical roles to make substantial improvements to the Federation Manager portal, to raise the level of trust in Federation infrastructure by actively evaluating security threats, and to start the Baseline Expectations implementation process.

Thank you: InCommon Reports on Use of 2017 Fee Increase - Improved security, enhancement of the Federation Manager portal, and increased service desk support are some of the results of an InCommon fee increase, which began with the 2017 calendar year. An August blog post listed some of the developments supported by the revenue.

New Staff to Fill Gaps - The fee increase enabled InCommon Operations to hire a DevOps Manager, Security Lead, Project Manager, and Service Desk

Associate to fill significant gaps in the support of the portfolio. A part-time Research Liaison was also hired to increase the dialogue with this important community.

Modernizing Our Tools for You: Federation Manager Moving to DevOps Model - The Federation Manager - the portal used by participants to maintain their metadata - has undergone a number of changes during 2017. The changes include upgrades to the user interface, making things clearer and easier, and developing a DevOps process for regular ongoing tweaks and improvements.

Security Requires Communications: Federation Publishes Final Security Incident Handling Framework - InCommon Operations published the *InCommon Security Incident Handling Framework*, which documents how Operations responds to security-related threats targeting the InCommon Federation infrastructure, and to those related to participants' federating systems. The framework and description of the security incidents addressed thus far are available on the InCommon wiki.

Making it Easier to Find Things: Document Stewardship Process Implemented - Internet2 Trust and Identity has adopted a document stewardship process to provide a permanent location for important information and build a historical record of documents and policies. The process formalizes the manner in which standards, policies, guidelines, recommendations, and other informational documents are drafted, proposed, vetted, approved for use, and published for open access. It is intended to address any documents that are products of work sponsored by the Internet2 Trust and Identity division or one of its community advisory groups. This process makes it easier for readers to find documents of interest, tracks authors and stages of document review, and clarifies the status of every document germane to community software and services development.

The InCommon Model: Explaining Trust and Trusted Relationships - The InCommon Federation published this high-level introduction to the model for trusted relationships within the Federation. It is intended as a resource for executives and business managers with responsibility for policy, legal, and technical aspects of identity and access management at their organizations.

Software and Service Delivery

Key software and service delivery needs of the Trust and Identity community include software developed by and for research and education that is affordable and provides dependable services.

TIER: Supporting Good IdM Practices and InCommon

The TIER (Trust and Identity in Education and Research) program is a community-driven effort, coordinated by Internet2, to develop a consistent approach to identity and access management (IAM) that simplifies campus processes and advances inter-institutional collaboration and research. That includes an IAM software suite.

In 2017, the program was focused on instituting a continuous release pipeline, simplifying software installation and configuration, and encouraging adoption. Community working groups comprised of dozens of member organizations collectively spent thousands of hours working on the IAM suite and related processes. For additional information about the working groups and their work, see Appendix C.

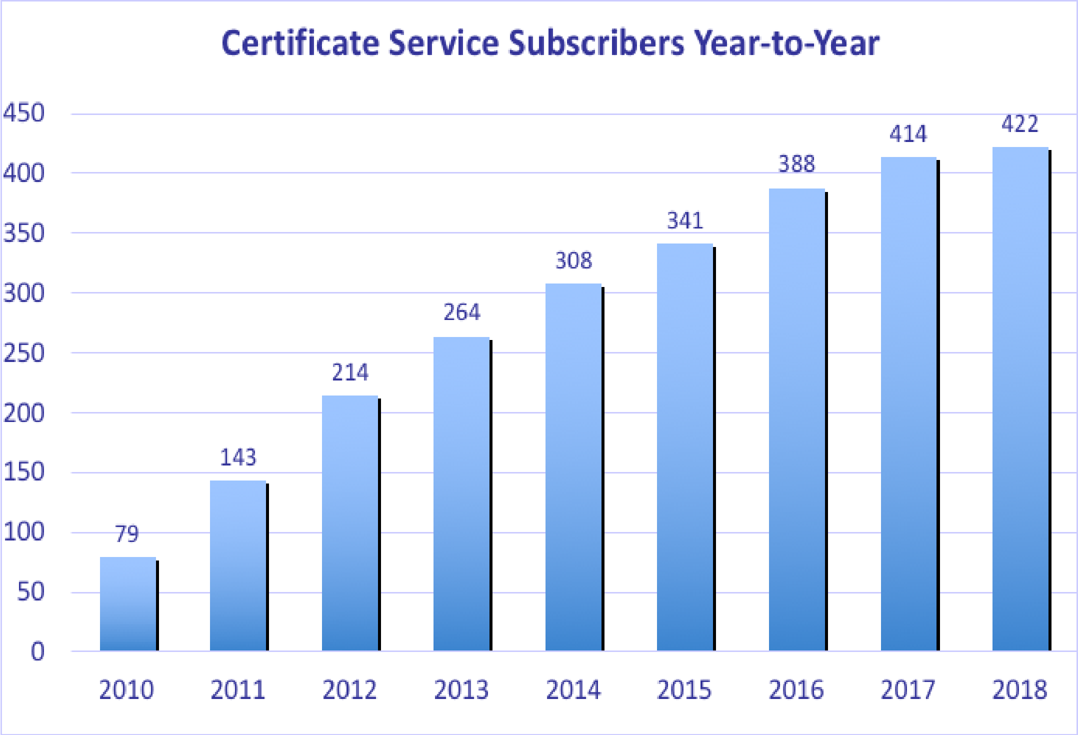
Continuous Release Pipeline and Software Development - Working groups developed and refined the continuous release pipeline, with updates incorporated into the software as soon as they are ready for production. They also improved the installation and basic configuration time for the Shibboleth Identity Provider component from potentially several hours to less than 10 minutes. Developers also packaged the Shibboleth IdP into a Docker container and continued work on containerizing the other software components. midPoint, a registry and provisioning tool designed to work with LDAP infrastructure, was added as a component during 2017.

TIER Demos - The developers and architects again offered live presentations and demos at the 2017 Internet2 Technology Exchange. These well-received demonstrations provided community members with insight into the IAM suite, development efforts, and how the software can help their institutions manage IAM challenges.

Mid-term Investor Survey - Halfway through the three-year funding cycle, the TIER Community Investor Council conducted a survey of the 49 investor schools to gather feedback and direction for the last year of the project. The results showed heavy use of Shibboleth (90%) and an increasing use of Grouper (60%). A registry was the most-requested missing component, with COmanage deployed in only 5% of investor schools. Since the survey, midPoint has been added to the suite of components. The survey also identified that most investor schools need help with adoption of the IAM suite, with requests for roadmaps, requirements mapping, and consulting services. Support and support services are also key needs.

Campus Success Program - As part of the effort to support adoption, a diverse group of ten campuses joined the TIER Campus Success Program to adopt and deploy one or more of the TIER software components (Shibboleth, Grouper, COmanage, and midPoint). The campuses meet bi-weekly to share experiences and provide regular updates on their efforts, and have access to subject-matter experts and discounted training to help reduce the time to adoption. The schools are also developing different forms of documentation—deployment guidance, presentations, project reports—to help jump-start and accelerate adoption by other campuses. This effort will run through mid-October 2018.

InCommon Certificate Service



Single Sign-on and Multifactor Authentication Available - Nine Certificate Service subscribers successfully completed a pilot testing the use of single sign-on (SSO) and multifactor authentication (MFA) to log in to the Comodo Certificate Manager (Comodo is the certificate provider behind the InCommon service). This long-requested feature is now available for any Certificate Service subscriber that also operates an Identity Provider in the InCommon Federation. Those who administer certificates on campuses can now use their InCommon federated credentials for single sign-on and use their local multifactor authentication deployments.

Enhancing Your Certificate Service: InCommon Certificate Service Work Plan - Coming out of the 2016 InCommon Certificate Service Survey, Internet2 worked with Comodo to develop a 2017 work plan with items highlighted by the community. You can view the progress on the wiki.

eduroam: Federated WiFi

Sustaining eduroam: Rolling Out Business Model to the Community - The global eduroam service has been operating in the U.S. since 2012, with Internet2 serving as the U.S. hub. To sustain the service, the Trust and Identity division engaged the almost 600 connecting organizations about continuing the service and completing the eduroam connector agreement, which outlines roles and responsibilities for the services. Also included was a pricing model vetted by the community in 2014.

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.

Governance and Advisory Groups

Trust and Identity Division

Trust and Identity Program Advisory Group - The Trust and Identity Program Advisory Group (PAG), created in 2017, provides community management-level input and guidance to the VP of Trust and Identity 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. The PAG includes representatives from the InCommon Steering Committee, the Internet2 TIER Community Investor Council, and the Community Architecture Committee for Trust and Identity (CACTI).

Community Architecture Committee for Trust and Identity (CACTI) - CACTI (Community Architecture Committee for Trust and Identity) was formed in 2017 as an architecture strategy group of community members to advise the vice president of trust and identity. CACTI provides strategic architectural input for trust and identity, and manages and evolves community standards, among other duties. CACTI includes members from the national and international research and education community, including key trust and identity organizations. Details are included in the CACTI charter.

InCommon

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.

InCommon Assurance Advisory Committee/Community Trust and Assurance Board - The Assurance Advisory Committee (AAC) transitioned to the Community Trust and Assurance Board (CTAB) with a revised charter and expanded role - primarily in developing and shepherding the Baseline

Expectations for Trust in Federation program. The CTAB is an advisory body to the InCommon Steering Committee.

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.

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 will end in December 2018. Internet2 provides the day-to-day management and staffing of TIER software development, support for community working groups, and development of community practices.

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. The group published a status update on TIER development, documenting the established community requirements and the work needed in 2018 to meet those expectations.

Education Programs

IAM Online Webinar Series - The monthly IAM Online webinar series marked its eighth year of operation in 2017. Appendix D includes a list of topics and speakers. In 2017, Internet2 partnered with GÉANT on an IAM Online YouTube channel.

InCommon Shibboleth Installation Workshops - The InCommon Shibboleth Installation Workshops marked the eighth year of operation. Four workshops took place in 2017 with a total attendance of 88 participants. Internet2 began using the TIER distribution of Shibboleth during the last workshop with good results. See Appendix E for details.

2017 Internet2 Global Summit - The 2017 Internet2 Global Summit, held in Washington, D.C., featured a plenary talk by Ian Glazer, senior director for identity at Salesforce. Ian spoke on “The Changing Face/Fate of Identity,” sharing important insights with the community as it grows its trust and identity practices and defines future needs. Other Global Summit highlights included a Great Identity Debate (moderated by Nicole Harris of GÉANT), a Kantara assurance working meeting, a session on Trust and Identity Governance and Sustainability (with Kevin Morooney, Klara Jelinkova and John O’Keefe), and sessions highlighting the progress of the TIER program.

2017 Internet2 Technology Exchange - In its fourth year, the Internet2 Technology Exchange (TechEx) is now established as 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 2017 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. More than 200 trust and identity professionals attended the meeting.

Working Groups

Appendix C includes a list of the working groups, chairs, links to wiki pages, and a summary of their charters and any reports or other results.

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

InCommon and TIER Working Groups

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
Grouper Deployment Guide	Bill Thompson, Lafayette College	https://spaces.internet2.edu/x/mgAZBg

Conclusion and Looking Ahead

2017 marked a watershed year for the Trust and Identity division of Internet2.

- The community saw the results of the first year of the increased InCommon fees, which included maturation and scaling operations in a way that sets the service on a good path toward sustainability.
- Through the Baseline Expectations program, the InCommon Federation is shifting from no effective requirements to effective processes that move all Participants to support a common set of practices that improve the Federation’s strategic value for research and education.
- New support for engaging researchers and scholars, and acknowledgement by the National Science Foundation of the importance of federation to their funded work, reinforced the important role for InCommon in support of research and academic collaborations.
- TIER community IAM architects and developers moved to a container approach for software delivery, with an eye toward both simplification and sustainability.
- TIER adoption efforts began with ten schools committed to working together to help each other and their peers from the community.
- Implementing a business process and fee structure addresses key sustainability challenges for the eduroam federated wireless service, a sister and complimentary service to InCommon.

Looking ahead to 2018, the Trust and Identity division will engage the community on developing next steps for the IAM Suite development and adoption, implementing Baseline Expectations, and scaling metadata delivery for InCommon. In the background, the division staff will work to enhance service delivery and software development, and will focus on community engagement in planning for future goals and direction.

Appendix A: Statistics

New Research and Scholarship Service Providers in 2017

1. Gravitational-wave Candidate Event Database Test
2. Big Ten Academic Alliance Reciprocal Borrowing (Staging)
3. Big Ten Academic Alliance Reciprocal Borrowing
4. *Unity
5. Center for Open Science - Open Science Framework
6. Internet2 Visible Network
7. Internet2 Analytics
8. Internet2 Collaboration Login
9. Big Ten Academic Alliance
10. Simien Mountains Gelada Research Project
11. CLIC-CTSA
12. WV Aquavit Research Collaboration
13. Mass Open Cloud

Appendix B: Newsletters and Reports

Trust and Identity Newsletters

In July 2017, the InCommon Update and TIER newsletter were retired in favor of a new Trust and Identity newsletter.

December 2017
October 2017
August 2017
July 2017

InCommon Update Newsletters

InCommon published five monthly newsletters during 2017:

May 2017
April 2017
March 2017
February 2017
January 2017

TIER Newsletters

The TIER program published five newsletters during 2017:

May/June 2017
April 2017
March 2017
February 2017
January 2017

TIER Quarterly Reports

2017 Quarter 1
2017 Quarter 2
2017 Quarter 3

Case Study

Gravitational Wave Research Boosted by Seamless Virtual Identity and Access Management

Appendix C: Working Group Summaries

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. If necessary and desirable, this working group will facilitate an effort to further evolve the current SAML2int profile. It will also identify which of these standards could be tested by InCommon if the federation wanted to ensure full profile compliance by participants.

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 has identified and begun documenting standards for Service Provider operation within the InCommon Federation using the CIC Cloud Services Cookbook as a starting point. Having standards available that help SPs onboard will add to the value proposition for SPs in the InCommon Federation and reduce variance in configuration and increase interoperability.

The target audience for the working group is organizations that are running, or want to run, an SP.

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 includes participants from the key stakeholder groups that need/use common attributes used in federated access exchanges. The working group explored the reasons that default attribute release policies are not in place at most campuses and will propose a default list of attributes for InCommon Identity Provider operators. The group aims to develop and execute a roadmap for adoption of the Research and Scholarship Category of Service Providers as well as a default attribute release policy. In addition, the group will review and enhance online content for Identity Provider administrators, so they have a clear set of steps to follow to implement the desired approach.

TIER Data Structures and APIs Working Group

Chair: Keith Hazelton, University of Wisconsin-Madison
Wiki: https://spaces.internet2.edu/x/SgFwBQ

This working group developed demonstrations for the 2017 Global Summit and the 2017 Technology Exchange related to provisioning identities and their attributes into common commercial applications. The group also worked with other working groups to release the TIER Grouper Deployment Guide and to develop the TIER Beacon instrumentation (which will help understand deployment patterns and adoption). Members also worked with the Big Ten Academic Alliance to analyze provisioning among COmanage, Grouper, and midPoint. At the end of the year, the group identified priorities for 2018.

TIER Packaging Working Group

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

The Packaging Working Group spent the early part of the year refining the base packages and configurations for TIER's initial Shibboleth, Grouper, and COmanage components to make them as easy to deploy and test as possible. Based on community input, the working group developed a continuous integration pipeline for stand-alone Docker containers for each component. The pipeline enabled a rapid evolution in the component/container development with roughly 50 builds over the spring and summer. The working group also spend time reviewing the adoption of an additional TIER component, midPoint. The working group also focused on developing packaging for midPoint and the development of a graphical user interface tool for managing metadata for Shibboleth administrators.

TIER Entity Registry Working Group

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

This working group developed and published a formal proposal for a TIER Thin Registry as a baseline for campus adoption. The group also worked with the TIER Data Structures and API working group to investigate and evaluate midPoint and begin development of an event messaging architecture around RabbitMQ/AMQP. The group also expanded the TIER reference architecture to confirm direction on storage/access of identity information from the viewpoint of applications for minimal person registry identity data, affiliation (group/role) data, additional person information, and an “information switchboard” capability.

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

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

Early in 2017 the Big Ten Academic Alliance joined forces with TIER Working Groups in an effort to advance standards for campus identities to access and operate the growing number of on-campus and cloud services. The goal is to gather and document the standards that are available and propose additional development for provisioning and de-provisioning. Some areas of interest are communicating group and role information, standardizing attribute release and mapping, and choosing the right method and protocol to communicate this information. Phase 1 will involve creating a functional model that is mapped to the relevant standards and protocols. Phase II will propose a roadmap to address areas where current standards do not meet today’s challenges in an effort to attain the next level of provisioning/de-provisioning.

Appendix D: 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 during 2017, plus other trust and identity webinars, are available on the IAM Online YouTube channel.

Identities are People, Too: IAM Tooling that Works (Dec. 13, 2017)
Presenter: Mary McKee, Senior IT Manager, Duke University

Taking a Fresh Look at IAM at Your Institution: Two Case Studies (October 11, 2017)
Presenters: Tom Dugas, Director, Information Security/New Initiatives, Duquesne University; Sharon Pitt, Associate Vice President and CIO, Binghamton University

Identity and Access Management with Globus (September 13, 2017)
Presenter: Steve Tuecke, Globus Co-Founder and Project Lead; Moderator: Tom Barton, University of Chicago and Internet2.

Baseline Expectations for Trust in Federation (July 19, 2017)
Presenters: Brett Bieber, University of Nebraska Lincoln, InCommon AAC Chair; Tom Barton, University of Chicago and Internet2

“Free the Attributes!” “No - Minimize Identity Exposure!” How about “Let the individual decide?” (June 2017)
Presenters: Rob Carter, Duke University; Ken Klingenstein, Internet2

The Shibboleth Consortium: Sustainability and Future Directions? (May 10, 2017)
Presenters: Scott Cantor, Sr. Systems Developer, The Ohio State University; Shibboleth Developer and Board member; Justin Knight, Project Manager at Jisc (which manages the Shibboleth Consortium); Kevin Morooney, Vice President, Trust and Identity, Internet2, Shibboleth Board member; Steve Zoppi, Associate Vice President, Services Integration and Architecture, Internet2

MFA: Duo and Google 2-Step Deployments Compared (April 12, 2017)
Presenter: Rich Graves, shared information security officer for both Carleton College and St. Olaf College

Appendix D: IAM Online Topics

InCommon Technical Advisory Committee Work Plan (March 22, 2017)
Presenter: Mark Scheible, MCNC and chair, InCommon TAC

Making Federation Easier: Default Attribute Release and User Consent (Feb. 8, 2017)
Presenters: Liam Hoekenga, University of Michigan; Mark Scheible, MCNC; Keith Wessel, University of Illinois at Urbana-Champaign

What is TIER and What Does it Mean to Me? (Jan. 25, 2017)
Presenters: Kevin Morooney, Vice President for Trust and Identity Services, Internet2; Ann West, Associate Vice President, Trust and Identity, Internet2; Steve Zoppi, Associate Vice President, Services Integration and Architecture, Internet2

Appendix E: InCommon Shibboleth Installation Workshops

2017	Host	Attendees (max = 40)
April	University of Michigan Ann Arbor	36
June	University of Denver	20
July	Lafayette College	15
November	National Institute for Allergies and Infectious Diseases	27
Total		88

Appendix F - 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/

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. The CTAB was formerly known as the Assurance Advisory Committee (AAC). CTAB membership includes representatives from higher education, other research and scholarly communities, internal auditors, and other key constituents. See www.incommon.org/ctab.

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.

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 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.

Steward Program - InCommon Steward Program - The InCommon Steward Program extends the benefits of federated identity management to K-12 school districts and community colleges. The Steward (a state or regional network) manages the implementation and InCommon provides the infrastructure and operational experience. See www.incommon.org/steward

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

TCIC - TIER Community Investor Council - This group guides the planning and development of TIER, representing the TIER investor schools. See https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/about-tier/

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

TIER Campus Success Program - 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

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