2021 InCommon Accomplishments

March 22, 2022

Document Title:	2021 InCommon Accomplishments
Repository ID:	TI.161.1
Persistent URL:	http://doi.org/10.26869/TI.161.1

Authors:

Apryl Motley	
Ann West	https://orcid.org/0000-0001-5484-6827
Kevin Morooney	https://orcid.org/0000-0001-9058-3921

Publication Date: March 22, 2022

Sponsor: Internet2 Vice President, Trust and Identity and NET+

Table of Contents

About InCommon

InCommon grew out of Internet2's work in trusted access to resources, which has been underway since 1998. In 2000, Internet2 received the first of what would become 10 federal agency awards, with Internet Hall of Fame Inductee Ken Klingenstein as principal investigator, leading to the creation of the Internet2 Middleware Initiative. InCommon grew out of that program. Through InCommon, Internet2 provides identity and access management (IAM) software and services, allowing the research and education community to work together and solve common problems.

How do we do it?

- **Community drives everything.** We work together with shared passion, directness, respect, and humor.
- **We act locally and think globally.** Our community-built solutions work for collaborations on campus, around the country, and around the world.
- **We have standards.** Our innovative and trusted technology is built on standards and tailored for research and education.
- **The developers use their own stuff.** Our community-designed software solutions are developed and built by the same people who make use of them every day.

Our IAM solutions solve problems related to:

- **Managing access** – Simplifying access control with single sign-on and using groups for provisioning.
- **Facilitating scholarly collaborations** – Providing scholars and students access to collaboration tools worldwide without the need for IT intervention.
- **Coordinating guest systems** –Allowing guests (e.g., alumni, prospective students, visiting faculty) to bring their own ID and access appropriate resources.
- **Implementing identity lifecycle management** –Automating identity and policy decisions and access control.

Here are the services we provide:

- **The InCommon Academy** – Expert-led component training, implementation support, introductory workshops, and community-oriented conferences.
- **The InCommon Federation** – Privacy-preserving single sign-on access to services – locally and around the globe.
- **The InCommon Trusted Access Platform** – Community-developed IAM software and services.
- **The InCommon Certificate Service** – Unlimited server and user certificates for one annual fee.
- **eduroam** – Managing Internet2's U.S. node for the eduroam global Wi-Fi network for research and education.

Executive Summary

InCommon® INSIGHT

"Extreme collaboration...the opportunity to receive guidance from those who have walked the path before you as well as the opportunity to help those on the path behind you"
—2021 CAMP Attendee

This is how one attendee described participating in Campus Architecture and Middleware Planning (CAMP) Week. In many ways, these sentiments sum up 2021 for us. Working together with you, our team was extremely focused on leveraging existing resources to bring our community more of everything: more eduroam connections, more opportunities to collaborate with peers, and more identity and access management (IAM) resources.

Last year was definitely better than the year before, and the path forward looks positive because of our shared commitment to collaboration and willingness to help each other along the way. As we continue to walk this walk together, we reflect on what we have accomplished and move ahead in anticipation of what's next. Now more than ever, our greatest opportunities lie in continuing to build upon what we have InCommon. All paths lead here. Take a quick walk with us down memory lane as we highlight our 2021 accomplishments.

Highlights

- **Ken Klingenstein was inducted into the Internet Hall of Fame.** He was recognized for his pioneering work in the development of the internet's identity and trust layers, envisioning and facilitating the widespread, consistent internet identity infrastructure for research and education. Under Ken's leadership, the Internet2 Middleware Initiative led the successful development of Shibboleth, the community-developed, open-source software that has enabled the growth of privacy-preserving federations; the OASIS security assertion markup language (SAML) standard, which Shibboleth uses to exchange identity data between federated partners; other key identity management software, Grouper and COmanage, part of the InCommon Trusted Access Platform; and the InCommon Federation, the U.S. research and education identity management federation. All this work was funded in part by Ken's awards from the National Science Foundation.

- **National Institutes of Health continued to leverage support for the InCommon Federation.** Driven by needing to widen access to and secure critical research, NIH worked with InCommon to help more than 135 campuses support multi-factor access to electronic Research Administration.

- **eduroam moved to the cloud to support the next 1,000 organizations.** Responding to new needs and growth of the service as more higher education and research institutions continue to use the service, Internet2 moved the eduroam service to the cloud to enable scaling and new functionality.

- **Arizona's SunCorridor Network and Network Nebraska became the second and third eduroam Support Organizations.** The new **eduroam Support Organization Program** will facilitate more rapid eduroam deployment across K-12, museums, and libraries in those states. The new cloud-forward architecture will support this expansion into these new communities too.

- **InCommon Baseline Expectations expanded to include security requirements.** The community adopted Baseline Expectations Version 2 in 2020 and exceeded the goal of 80 percent adherence by December 2021**.**

- **InCommon Academy Community Engagement increased at our CAMP-related events.** Our introductory BaseCAMP workshop and the annual technical community CAMP and Advance CAMP (ACAMP) meetings were offered online again in 2021. Attendance increased by 9% compared to previous virtual meetings.

- **InCommon Catalyst Program kicked off.** Following up on community requests for corporate integration help and support options, Internet2 partnered with eight trusted corporate and not-for-profit organizations that have participated in the community for at least a year to announce the InCommon Catalyst Program.

The Path to Training: InCommon Academy

InCommon ACADEMY
INSIGHT

"BaseCAMP is a must for anyone in higher education, IT, and IAM. The materials presented are clear and concise, and the presenters offer a wealth of experience and humor to guide conversations."
—2021 BaseCAMP Attendee

The InCommon Academy provides:

- Opportunities for the community to convene and discuss common challenges and solutions (InCommon BaseCAMP and CAMP Week)
- Regularly scheduled community-presented webinars (IAM Online)
- Training on community developed InCommon Trusted Access Platform software
- A program to help organizations discover, learn about, prototype, and plan IAM services (InCommon Collaboration Success Program)

Community Convening Continues Online

In the face of the pandemic, InCommon moved its entire CAMP series online, even as planning had begun for in-person meetings.

InCommon BaseCAMP – First was BaseCAMP, a workshop that provides:

- An introduction to identity and access management
- An overview of the InCommon Federation
- Discussions of the InCommon Trusted Access Platform suite of community-built IAM software

Attendance in 2021 increased 37% over the 2020 BaseCAMP, and 90% of attendees who completed the evaluation said they would recommend BaseCAMP to a colleague.

The online meeting took place over five days (four hours per day). BaseCAMP 2021 used the Canvas learning management system to house content, integrated with Zoom for live presentations.

Table 1 – BaseCAMP Attendance

Year	2021	2020	2019
Number of Attendees	108	79	70

InCommon CAMP Week – The international trust and identity community convened for a week (partial days) in October for the annual CAMP and ACAMP meetings. Community members contributed presentations that filled three tracks over two days, then participated in the unconference Advance CAMP for an additional three days. Attendance rivaled that of the traditional in-person meetings, and registrations increased by 9% from 2021.

InCommon ACADEMY INSIGHT

"CAMP is a highly valuable event focusing on a range of IAM related topics that allows you to keep a pulse on important IAM industry trends and what to pay attention to as we look to the future. This is in addition to all the help in solving the complex IAM challenges every higher ed institution faces."
—2021 CAMP Attendee

Software Training

During 2021, InCommon held a combined 10 training sessions for the InCommon Trusted Access Platform community-built identity and access management suite of software. Each course uses pre-configured training environments to enable hands-on labs, coupled with lecture and interactive discussion.

Enrollment increased by 28% over 2020.

Table 2 – Trusted Access Platform Software Training Attendance

Course	Courses	Participants	Unique Orgs Attending	Average Rating (Scale 0-5)
COmanage Class	2	34	15	4.7
Grouper School	3	91	40	4.5
midPoint Basics	2	48	19	4.6
Shibboleth Installation	3	84	38	4.3
Totals (across the portfolio)	**10**	**257**	**80**	**4.5**
2020 totals (across the portfolio	*8*	*176*	*91*	*4.6*

InCommon Collaboration Success Program Welcomes Members

Created in 2017 in response to a community survey, the InCommon Collaboration Success Program (CSP) helps organizations develop and meet their IAM goals and work to adopt one or more components of the community developed IAM software suite, the InCommon Trusted Access Platform.

During 2021, the six higher education institutions comprising the third group of CSP participants finished their work. For information on project plans and case studies, see the InCommon wiki.

The 2022 cohort, including another eight research and education organizations, formed in September 2021 and will complete its work in June 2022: Southern Methodist University, University of Arkansas, Clemson University, The University of Texas at Austin, University of Florida, University of North Carolina at Charlotte, SLAC National Accelerator Laboratory, and University of Missouri System.

CSP enables community, campus, and research teams with the chance to work together to address common identity and access management challenges. The program provides:

- Regular engagement, planning, project, and technical sessions to share ideas and learn from others
- Tailored recommendations based on an IAM assessment
- Access to a hosted workbench where you can model your potential solutions
- Eight registrations for InCommon Trusted Access Platform training sessions
- Two registrations for InCommon BaseCAMP and CAMP
- Priority access to advisors, community implementers, and software developers

InCommon ACADEMY INSIGHT

"The name Collaboration Success Program suggests working through challenges together, but the level of insight and detail from other organizations exceeded our expectations."
—2021 CSP Cohort Participant

IAM Online

IAM Online, InCommon's mostly monthly webinar series, concluded its 12th year of providing interactive education about identity and access management topics. IAM Online attendance averages almost 100 per session (including a high of 152 for the Higher Education Community Vendor Assessment Toolkit (HECVAT) collaboration webinar. A list of topics and links to the recordings are included in the appendix of this report. InCommon and GÉANT present past IAM Online sessions (offered in both the U.S. and Europe) on an identity and access management YouTube channel.

The Path to Secure Access: InCommon Federation

InCommon FEDERATION **INSIGHT**

In response to NIH’s call for secure, streamlined federated access, R&S and MFA adoption doubled last year; by the end of 2021, 90% of InCommon Participants had met Baseline Expectations for Trust in Federation Version 2 requirements.

The InCommon Federation provides the US international infrastructure for secure single sign-on access to cloud and local services, and global collaboration tools for the higher education and Research community. The Federation connects millions of users and hundreds of educational institutions, research organizations, and commercial resource providers in the US with even more millions of users and thousands of organizations internationally.

Expanding Identity and Access Standards Adoption

The demand for collaborative research projects increased significantly as the pandemic spread. The National Institutes of Health (NIH) appealed to institutions to improve streamlined and secured federated access to more than 150 services and NIH resources by automating the release of information via the Research & Scholarship (R&S) category and performing multi-factor authentication and signaling using the Research and Education FEDerations (REFEDS) Multi-Factor Authentication (MFA) Profile.

Research & Scholarship (R&S) category – Supporting the R&S category allows for simpler onboarding when a faculty member or researcher joins a collaboration. During 2021, InCommon saw a significant increase in the number of Identity Providers supporting R&S.

Chart 1 – Identity Providers Supporting REFEDS R&S in the InCommon Federation shows the number of InCommon Identity Providers that support R&S, meaning they release a small set of information to all services tagged as "R&S."

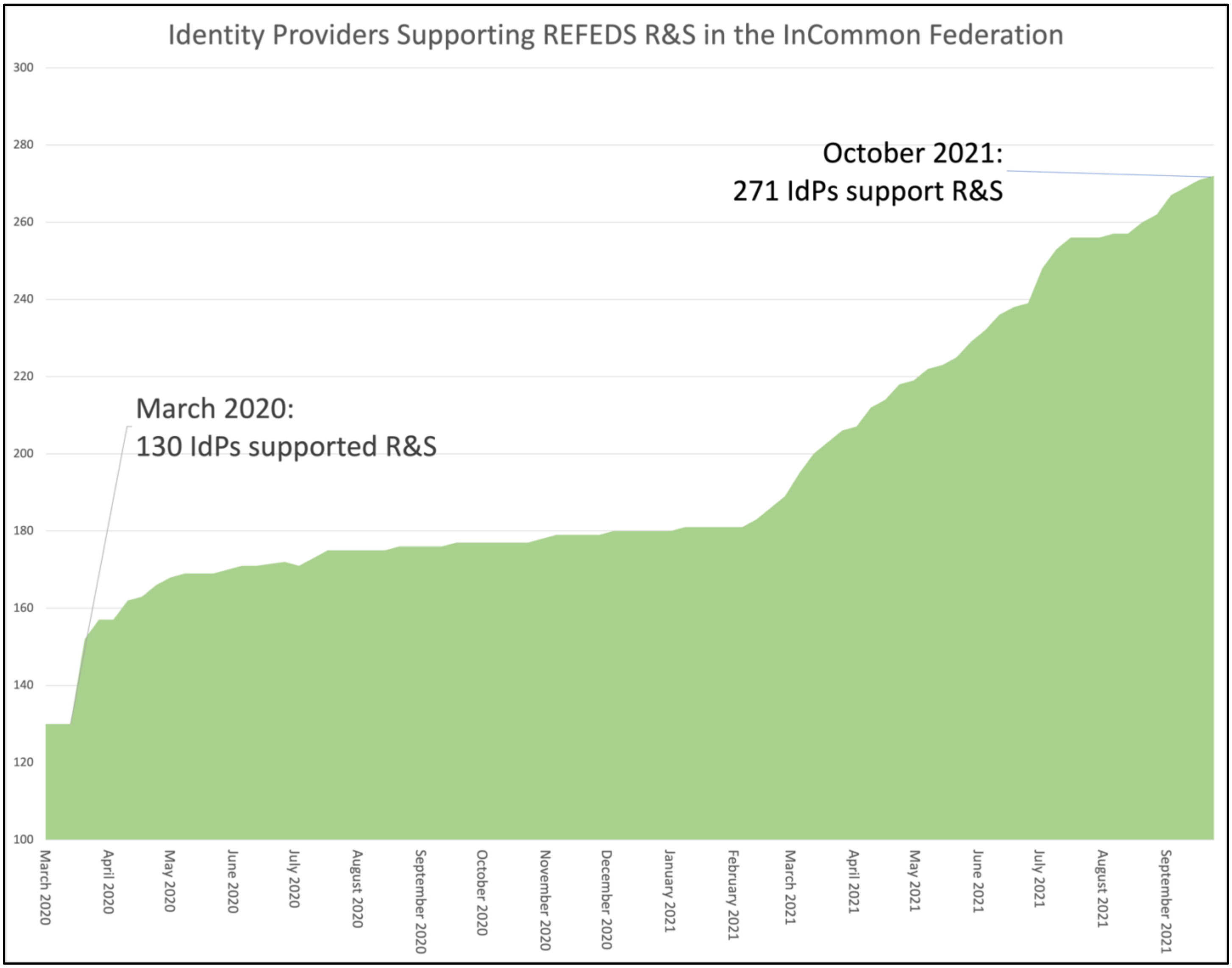
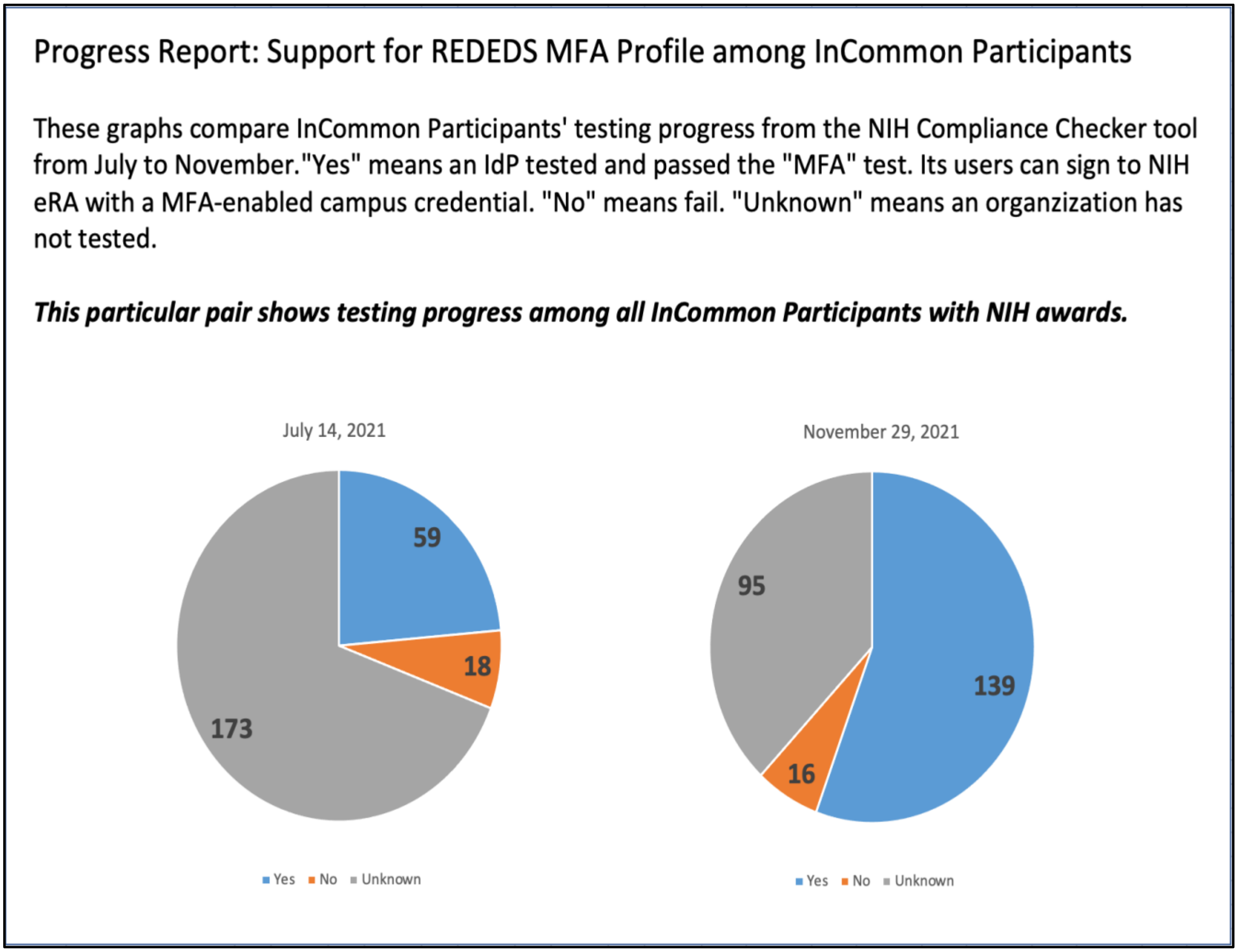


Chart 1 – Identity Providers Supporting REFEDS R&S in the InCommon Federation

Multi-Factor Authentication (MFA) adoption gaining momentum – InCommon and NIH’s combined effort also led to a significant increase in MFA adoption among InCommon Participants. In July 2021, 59 institutions receiving NIH awards had verified their support for the REFEDS MFA Profile, the international standard that federated Service Providers can use to request step-up authentication for Identity Providers. As shown in Chart 2 – Support for REDEDS MFA Profile among InCommon Participants, by the end of November, that number had more than doubled.



Progress Report: Support for REDEDS MFA Profile among InCommon Participants

These graphs compare InCommon Participants' testing progress from the NIH Compliance Checker tool from July to November."Yes" means an IdP tested and passed the "MFA" test. Its users can sign to NIH eRA with a MFA-enabled campus credential. "No" means fail. "Unknown" means an organziation has not tested.

This particular pair shows testing progress among all InCommon Participants with NIH awards.

Chart 2 – Support for REDEDS MFA Profile among InCommon Participants

Improving Trust and Security Among Federation Participants

Baseline Expectations for Trust in Federation Version 2 (BE2) – Continuing the effort to improve trust and interoperability, the Community Trust and Assurance Board, in collaboration with InCommon Operations, spearheaded the rollout of the second iteration of Baseline Expectations for Trust in Federation (BE2). BE2 builds on the original Baseline Expectations by adding three requirements:

1. Identity Providers must include an errorURL in their metadata to facilitate user support connection.
2. All service endpoint encryption must be secured with current and trustworthy transport layer encryption.
3. All entities must comply with the requirements of the Security Incident Response Trust Framework for Federated Identity.

By the end of 2021, 87% of InCommon Participants (90% of Identity Providers and 95% of Service Providers) had met BE2 requirements, as shown in Chart 3 – Baseline Expectations Progress - % Met BE2).

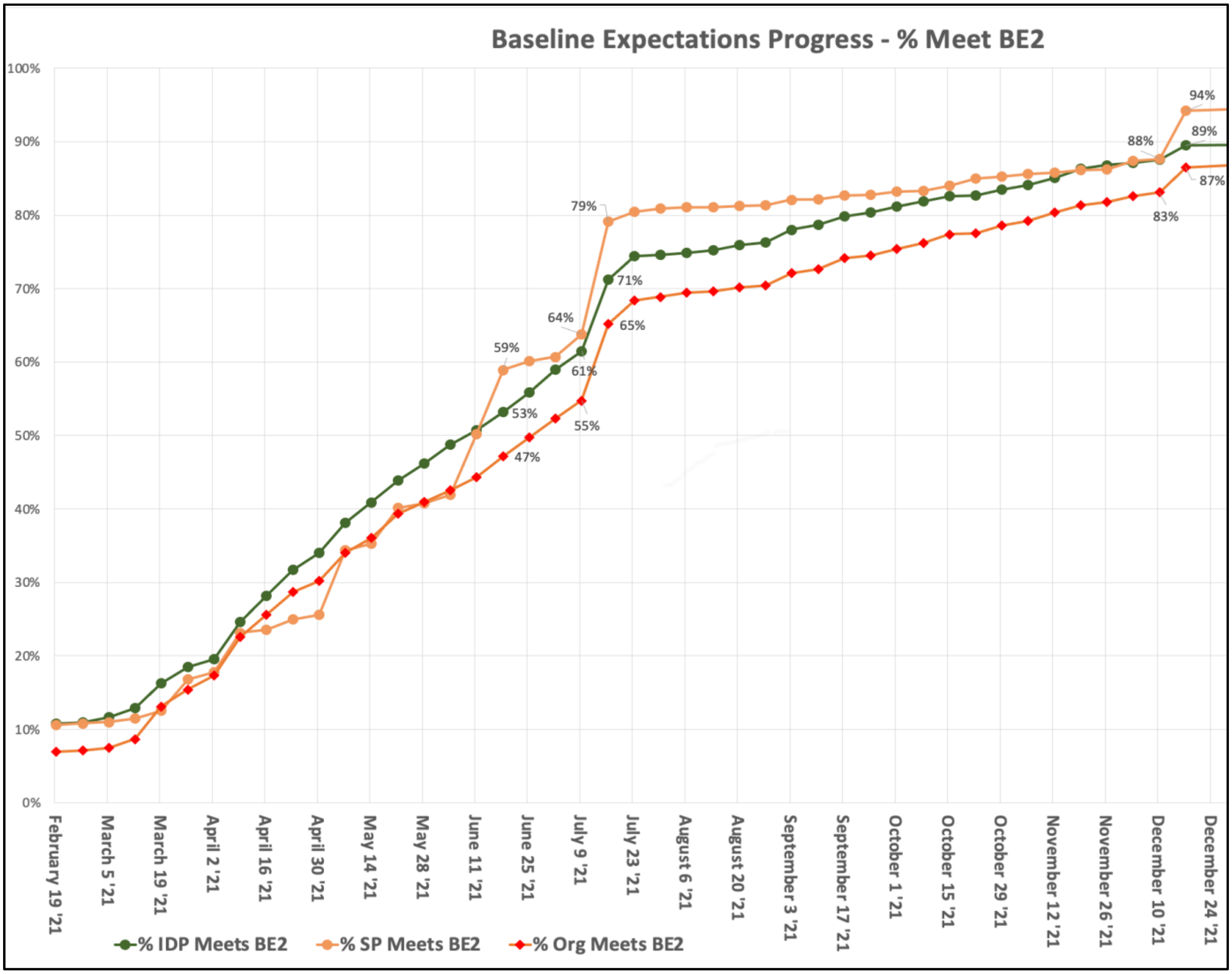


Chart 3 – Baseline Expectations Progress - % Met BE2

Security Incident Response Trust Framework for Federated Identity (SIRTFI) - InCommon supports the international SIRTFI framework, which aims to enable the coordination of incident response across federated organizations. The Community Trust and Assurance Board has added SIRTFI to InCommon's Baseline Expectations to raise it from a best practice to a hallmark of a trustworthy federation. At the end of 2021, 90% of Identity Providers and 95% of Service Providers had indicated support for SIRTFI.

Chart 4 – Percentage of InCommon IdPs and SPs Adopting SIRTFI shows the percentage of InCommon Identity Providers (red) and InCommon Service Providers (blue) that indicate they support SIRTFI. This represents 520 IdPs and 5,122 SPs Providers.

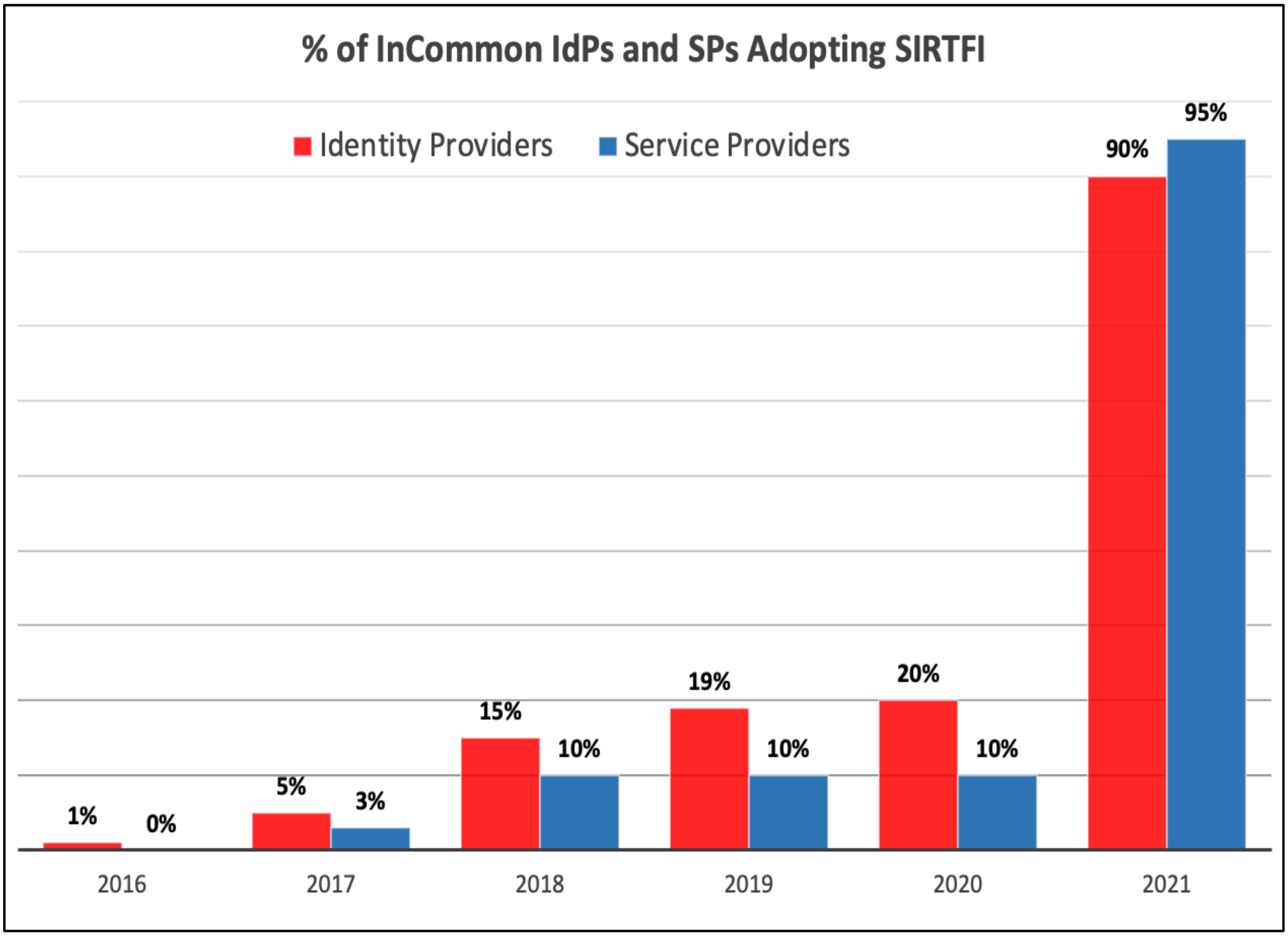


Chart 4 – Percentage of InCommon IdPs and SPs Adopting SIRTFI

Higher Education Community Vendor Assessment Toolkit (HECVAT) – In 2021, members of the InCommon Technical Advisory Committee (TAC) partnered with the Research and Education Network - Information Sharing and Analysis Center (REN-ISAC) and the Higher Education Information Security Council (HEISC) to update the authentication and authorization sections of the HECVAT. This update serves to focus the set of authentication and authorization-related questions on a fewer number of key points, allowing institutions to more readily assess the capabilities and security models vendors are employing in these critical areas.

Research Engagement

National Institutes of Health (NIH) – InCommon and NIH worked throughout 2021 to coordinate the design, implementation, and outreach connected to NIH phasing in MFA and identity assurance requirements for selected NIH services.

- The InCommon Assured Access Working Group was convened to provide guidance for campuses on how to implement support for identity assurance per the REFEDS Assurance Framework.
- A subgroup of the REFEDS Assurance Working Group was convened to improve MFA-associated guidance documentation to address many questions raised when campuses learned that NIH would soon be requiring MFA support from them.
- NIH developed and deployed a diagnostic tool for campus IdP operators to help them see how MFA and/or identity assurance related updates to their IdP actually work with NIH.

InCommon CAMP Week in October 2021 focused on NIH needs and featured several discussions with NIH representatives about balancing the increasing security requirements and higher education capabilities to meet them. Multiple messages were sent to identified groups of campus stakeholders concerning these developments, and multiple online office hours were held to support campus implementation of the new requirements.

Eastern Regional Network (ERN) – InCommon participated in regular meetings of the Eastern Regional Network's Architecture & Federation Working Group to help develop ERN's architecture and provide input to its Policy Working Group.

NASA – NASA invited InCommon to lead a discussion with technical representatives from each of its main facilities on how federated access can work within a Zero Trust security architecture. The discussion was well received, and a variety of artifacts were provided to help NASA technical staff prepare associated plans for approval.

The Path to IAM: InCommon Trusted Access Platform

InCommon
TRUSTED ACCESS
PLATFORM
INSIGHT

Last year, there were approximately 85 packaging releases of Trusted Access Platform, making various software components more portable and easier to implement.

The InCommon Trusted Access Platform is a community-built identity and access management (IAM) services and software for research and education. It is built to integrate with existing systems and is packaged in containers to simplify installation and configuration. The major components are Shibboleth, Grouper, COmanage, and midPoint. The first three were developed with support from the National Science Foundation.

The suite helps solve common IAM challenges, including

- Single sign-on across, local-to-global academic collaboration, library and software-as-as-a service applications and resources
- Managing access to shared and secured resources
- Managing access to and the participants in scholarly collaborations
- Enabling guest access from individuals with social to federated credentials.
- Supporting the organizational identity lifecycle, provisioning and deprovisioning, guest systems, and others.

Key accomplishments in 2021 include:

Across all the components, the Log4j security issue was fixed, and new packaged containers were released. InCommon Academy Training was also updated to reflect new features highlighted below.

InCommon
TRUSTED ACCESS
PLATFORM
INSIGHT

“We invested substantial effort in building supply-chain protection for our Maven build process, something virtually no other Java projects have addressed. We believe it is our responsibility to do all we can reasonably do to prevent the sorts of attacks now affecting the whole software industry.”
–Scott Cantor, Developer Associate, Shibboleth Consortium

Shibboleth Federating Software – Originally developed by the Internet2 community, the ongoing enhancement of Shibboleth is carried out by the international Shibboleth Consortium. In 2021, the Consortium released major changes to the identity provider software, including easier upgrades and configurations, the first OpenId Foundation certified OIDC plugin, substantial supply-chain protection for their Mavin build process, and design work for new Service Provider software.

Internet2's role as part of the Trusted Access Platform includes:

- **Testing and packaging of the Consortium releases** to make it easier for organizations to manage and operate the software. Internet2 released 26 Shibboleth component packages in 2021.
- **Engaging Unicon to support and develop a Shibboleth Graphical User Interface (GUI)** to further ease operations and configuration. In 2021, Unicon worked with the community to enable the GUI to support delegation of system management to other departments as well as better integration with existing SSO systems, and support of modern metadata distribution methods (MDQ).
- **Serving on the international Shibboleth Consortium board** as an advocate for the InCommon community and to ensure sustainability.

InCommon TRUSTED ACCESS PLATFORM INSIGHT

"There is a new and much enhanced provisioning framework with a handful of supported targets standardized for how Grouper keeps authorization data in sync in external systems."
–Chris Hyzer, Grouper Lead, Internet2

Grouper Access Management Software – Internet2 funds the community development team for Grouper as well as packages the software for easier operations. In 2021, activity focused on improving the provisioning framework to ensure data integrity between Grouper and externally provisioned systems. For detailed information about releases in 2021, see the Grouper Working Group wiki.

InCommon TRUSTED ACCESS PLATFORM INSIGHT

"Currently in release candidate status, Match v1.0.0 was designed in direct response to community requirements."
– Benjamin Oshrin, Spherical Cow Consulting

COmanage Registry Software – Internet2 funds most of the core project development for COmanage, and the COmanage development team handles packaging of the software. In 2021, Registry v4.0.0 was released, bringing out several new features, in direct response to community deployer use cases, supporting both research organizations and campus IT. The project team also adjusted the cadence of feature development to support more timely releases. Significant new features include:

- Identity Match 1.0 candidate released with direct support for COmanage Registry to enable inbound record cross-system matching and de-duplication.
- A much-improved user interface and set of group models for better useability and group membership management
- Significant provisioning support for asynchronous (queue-based) provisioning, an API provisioning plug-in (suitable for message queue and other integration patterns)
- Improved voPersonToken support in the LDAP provisioner, a Jira provisioning plug-in

For more information on recent releases, see the COmanage wiki.

InCommon TRUSTED ACCESS PLATFORM INSIGHT

"With the release of version 4.3, we improved performance, scalability, and password management as well as making diagnostic and visibility enhancements."
– Slavek Licehammer, Evolveum

midPoint Registry and Provisioning Software – midPoint is primarily funded and developed by Evolveum with support for InCommon community feature development and collaboration from Internet2. In 2021 the adoption of midPoint by the InCommon community accelerated and several new versions were released to improve performance, scalability, diagnostics, and automated user interface testing. In addition, an InCommon midPoint Working Group was established to meet regularly to address community needs. Several webinars about new features of midPoint were organized and promoted in the InCommon community. Recordings from the webinars are publicly available. For information about midPoint releases, see the Evolveum Docs site.

The Path to Centralization: InCommon Certificate Service

InCommon® CERTIFICATES INSIGHT

At the end of 2021, there were 240,000 active certificates across 676 organizations.

The InCommon Certificate Service provides unlimited certificates (SSL, EV, client, and others) for one annual fee. The work is driven, in part, by a biannual survey of Certificate Service subscribers. As of December 31, 2021, we had approximately 240,000 active certificates across 676 organizations.

Sectigo, InCommon's partner in the InCommon Certificate Service, has added the Automated Certificate Management Environment (ACME) Service for subscribers. The last regular survey of InCommon Certificate Service subscribers showed overwhelming interest in ACME.

Chart 5 – Certificate Subscribers Year-to-Year shows subscriptions to the InCommon Certificate Service as of December 31 of each year. During 2020, we started including the individual campuses that are part of a system-wide licenses that previously were not listed individually.

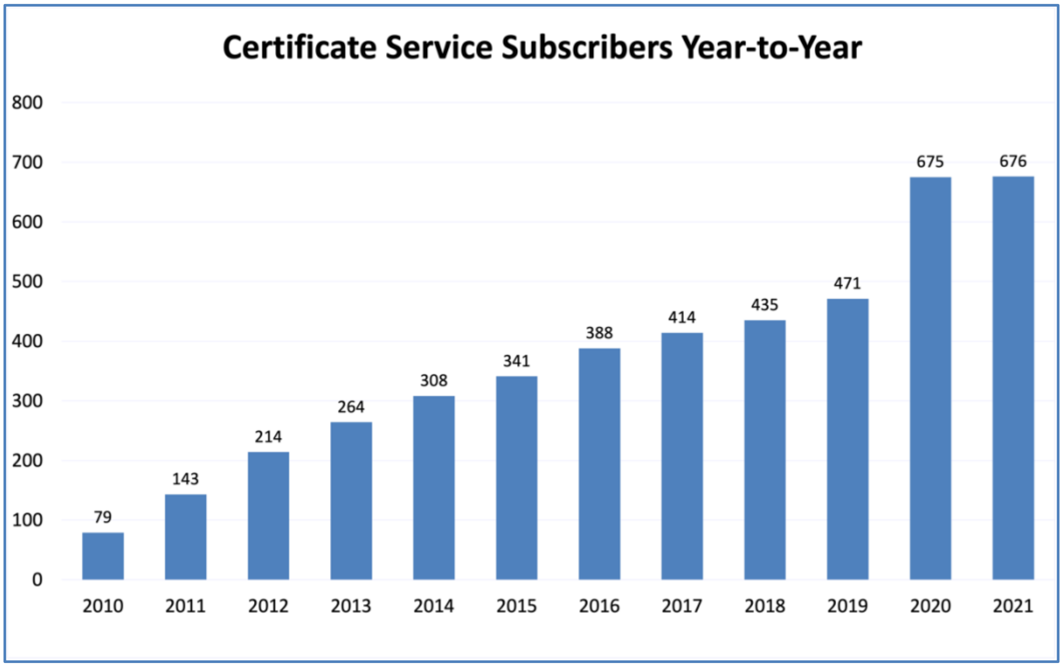


Chart 5 – Certificate Subscribers Year-to-Year

The Path to Collaboration: eduroam

INSIGHT

eduroam is available in more than 100 countries, including more than 1,000 universities and non-profits in the U.S.

InCommon/Internet2 operates the U.S. node for the global eduroam roaming Wi-Fi network for research and education. eduroam is available in more than 100 countries, including more than 1,000 universities and non-profits in the U.S. Individuals use their campus credentials to use the service no matter where they are.

eduroam Support Organizations – Network Nebraska and Arizona's Sun Corridor Network joined the Utah Education and Telehealth Network (UETN) as eduroam Support Organizations, committed to deploying eduroam to the K-12s, libraries, and museums in their states. During a pilot, UETN deployed eduroam to 38 K-12 school districts in Utah as well as numerous libraries and museums, and on public transit around the state.

The Support Organizations promote eduroam among their constituents and work with InCommon/Internet2 to:

- Onboard new K-12, library, and museum constituents in their area
- Provide first-level support for constituents
- Participate in collaborative meetings with other program participants

eduroam Infrastructure Upgrade – After a year's worth of work and a great team effort, the Internet2 team and community partners have rebuilt the eduroam administrative portal, as well as transitioned the backend RADIUS service to the cloud. This significant upgrade places eduroam on strong footing for continuing to scale the service to add constituencies and communities in the future.

Community Working Group Reports on Guest Access and End User Onboarding – The eduroam Advisory Committee (eAC) sponsored two working groups in 2021: one addressing access to eduroam for guests who are not affiliated with another eduroam organization, and the other addressing shortcomings in the ease of adoption of eduroam by end users. Both working groups returned reports by the end of the year and have concluded their comment periods.

Chart 6 – US eduroam Subscribers by Year shows subscriptions to the eduroam (U.S.) service as of December 31 of each year. During 2020, we started including the individual campuses that are part of a system-wide license, so previously they were not listed individually. In 2021, we have included Service Provider/Hot Spot subscribers as well.

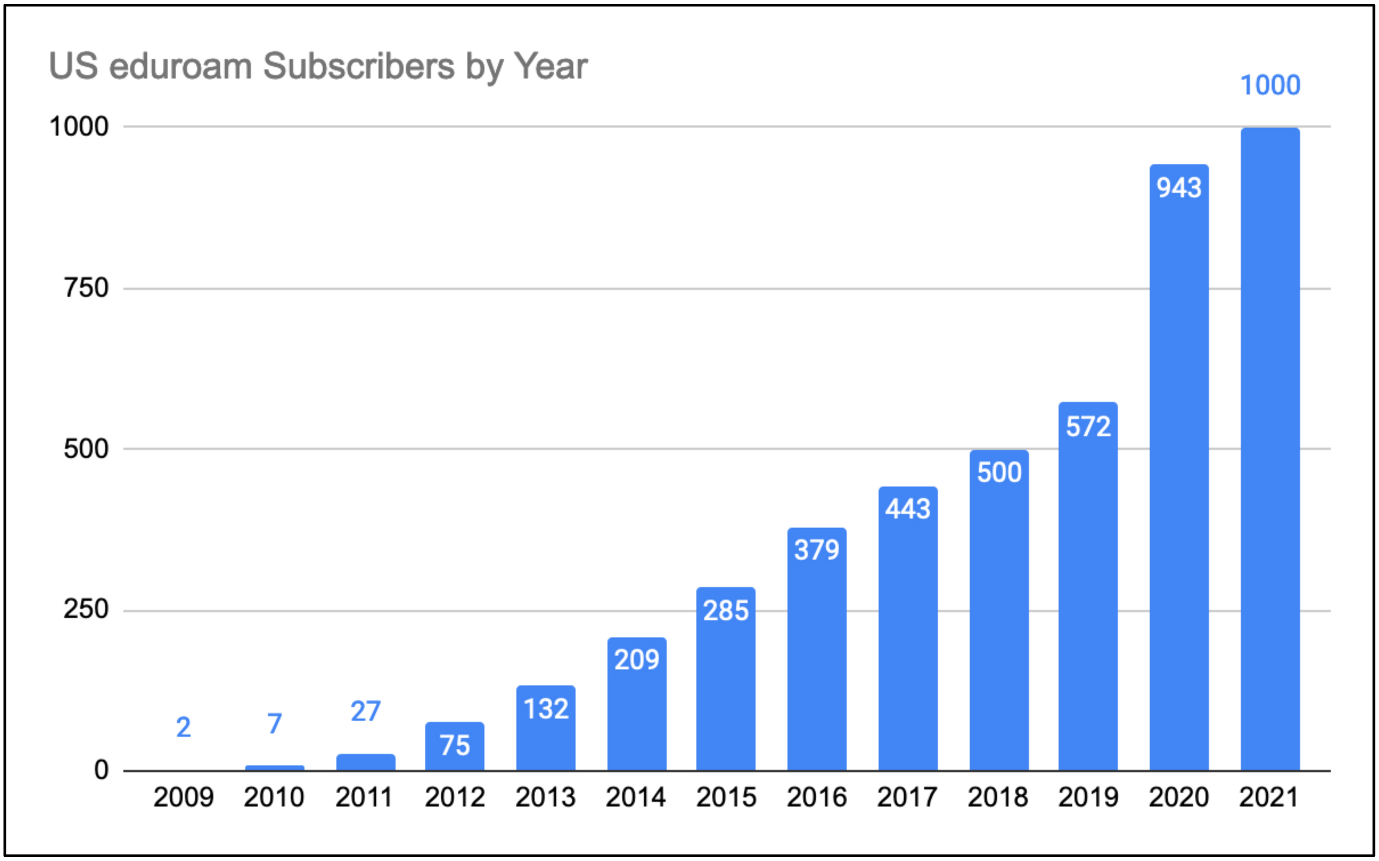


Chart 6 – US eduroam Subscribers by Year

eduroam

INSIGHT

"I truly believe we were able to move the needle in making eduroam more broadly available and easier to deploy."
– eduroam-US Advisory Committee Member

The Path to Peer Support: Engaging the Community

InCommon® COMMUNITY INSIGHT

Engaged volunteers contributed 2,343 hours to help move the community forward.

Through its advisory committees and working groups, InCommon convenes the community to develop requirements, specifications, and program activities. Collectively, engaged participants contributed 2,343 hours to help move the IAM community forward.

Governance and Advisory Groups

Trust and Identity Program Advisory Group

The Trust and Identity Program Advisory Group (PAG) provides community executive input and guidance to the Vice President for Trust and Identity and NET+.

Key topics discussed in 2021 included:

- Relationship and overlap between the PAG and InCommon Steering Committee
- The pandemic and trust and identity services, including eduroam, making collaboration easier, and community engagement
- OpenRoaming (guest access for enterprises) and eduroam (federated Wi-Fi for research and education)
- Browser changes and the impacts on Federated Identity
- Starting a global CEO forum working group

The PAG convened for a cumulative 30 community hours of work.

Community Architecture Committee for Trust and Identity

Chair: Robert Carter, Duke University
Vice Chair: Les LaCroix, Carleton College

The Community Architecture Committee for Trust and Identity (CACTI) is the architecture strategy group of community members that provides strategic architectural input for trust and identity, and manages and evolves community standards, among other duties.

The committee spent significant time looking at issues in the security space, such as software supply-chain security. It conducted two webinars – one on the aforementioned supply-chain issue and one in partnership with other committee chairs on getting involved in governance.

Key topics discussed in 2021 included:

- Broadening the InCommon reach to include people and places from which we historically have not had participation in our meetings
- Establishing two long-standing CACTI working groups
    - midPoint Working Group
    - PeopleSoft Integration Working Group
- Continuing to sponsor the long-standing eduroam advisory committee (eAC)
- Investigating security in new operating environments, such as infrastructure-as-a-service and DevSecOps.

CACTI convened for a cumulative 380 community hours of work.

InCommon®
COMMUNITY
INSIGHT

"Serving on the CACTI committee was a rewarding and enriching experience for me in both representing the needs of my community (research facilities) and in the many new technologies and people I met during the process."
– 2021 CACTI Committee Member

InCommon Steering Committee
Chair: Brad Christ, Eastern Washington University
Vice-Chair: Marc Wallman, Dakota State University

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. In addition to monthly meetings, they also committed to four two-hour retreats in 2021.

Key topics discussed in 2021 included:

- The business case for identity and access management
- IdP-as-a-Service working group report
- The blending of the committee and T&I PAG
- The value proposition of the InCommon Trusted Access Platform

- Engaging and supporting research communities
- Moving to an Internet2-operated infrastructure for eduroam
- Community engagement strategies
- Baseline Expectations for Trust in Federation Version 2

The Steering Committee convened for a cumulative 320 community hours of work.

InCommon Community Trust and Assurance Board
Chair: David Bantz, University of Alaska
Vice-Chair: Brett Bieber, University of Nebraska

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.

Key projects in 2021 included:

- Spearheading the rollout of the second iteration of Baseline Expectations for Trust in Federation (in collaboration with InCommon Operations).
- Working closely with InCommon and international stakeholders to develop implementation guidance to help participants meet NIH's requirements for supporting:
  - REFEDS multi-factor (REFEDS MFA Profile),
  - identity assurance (REFEDS Assurance Framework), and
  - user information exchange (REFEDS Research & Scholarship category) standards.
- Chartering the Assured Access Working Group

Between attending committee meetings, hosting office hours, and participating in working groups, CTAB members collectively contributed an estimated 621 hours of effort in 2021.

InCommon® COMMUNITY INSIGHT

"My favorite part about working on InCommon's advisory committees is being able to work with others to advance the security and trust in our shared infrastructure—something that is bigger than myself or my own campus."
– 2021 CTAB Member

InCommon Technical Advisory Committee
Chair: Keith Wessel, University of Illinois Urbana-Champaign

Vice-Chair: Heather Flanagan, Spherical Cow Consulting

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 the Federation's operational roadmap. Highlights from TAC's 2021 Work Plan included:

- **Adopting the SAML Deployment Profile –** In 2021, TAC developed a recommendation for InCommon to formally adopt the Kantara SAML Deployment Profile for Federated Identity. The InCommon Steering Committee accepted the recommendation. Rollout will begin in 2022.
- **SeamlessAccess (Future of Identity Provider Discovery Service) –**TAC, in collaboration with InCommon Operations, assessed scaling and sustainability issues around the InCommon Discovery Service while evaluating SeamlessAccess as a potential solution. TAC is finalizing its recommendation and will be submitting it to InCommon Steering in spring 2022.
- **Browser Technology Changes –** To safeguard user privacy, browser developers are making changes to the way user tracking works in web browsers. Unfortunately, changes to these tracking mechanisms (cookies, link decorations, etc.) also significantly impact federated single sign-on. TAC began actively tracking developments in this area in 2021.

TAC members collectively contributed an estimated 402 hours of effort in 2021.

InCommon® COMMUNITY INSIGHT

> *"The InCommon community is something special. It is inclusive and collaborative, makes hard work fun, and imparts deep knowledge of trust and identity."*
> *– 2021 TAC Member*

InCommon eduroam-US Advisory Committee (eAC)
Chair: Jeremy Livingston, Stevens University
Vice-Chair: Jeff Egly, University of Utah

The eduroam Advisory Committee (eAC) helps formulate strategies and practices for US and global research and education roaming networks, reports any findings, and makes recommendations to CACTI and Internet2, the eduroam-US operator.

Key projects in 2021 included:

- Completing work on the eduroam Best Practices Guide and promoting it during community webinars
- Forming working groups to develop requirements for additional eduroam related services

  - The eduroam User/Guest Onboarding Working Group created a requirements document for a user and device onboarding service for eduroam
  - The eduroam Guest Access Working Group created a requirements document for a guest access service for eduroam.
- Offering feedback during the transition to the new eduroam infrastructure
- Providing early testing for the new eduroam infrastructure
- Providing beta testing for eduroam Federation Manager

eAC convened for a cumulative 590 community hours, including working group and committee contributions.

Working Groups

InCommon Trusted Access Platform Software Integration Working Group

Chair: Keith Hazelton, Independent Consultant
Co-Chair: Ethan Kromhout, University of North Carolina Chapel Hill
Wiki: https://spaces.at.internet2.edu/x/SgFwBQ

Multiple systems of record may have information about an individual. It is crucial to link all the disparate information under a single digital identity. The InCommon Trusted Access Platform Software Integration Working Group is helping define a common ID Match capability not just for integration with the TAP components COmanage, midPoint, and Grouper, but for campuses with other person identity registry solutions as well.

The group continued to develop a knowledge base and guidance on various methods to integrate the various components of the IAM infrastructure with each other and with the rest of the systems that make up the campus IT environment.

By sharing knowledge and experience, we improved our collective ability to successfully provision to Active Directory (AD) and Azure. This is one case among many where experts building up Internet2's own IAM infrastructure contributed to the community through their participation in the working group. This group served to initiate planning and preparation for a new midPoint User's Group which got off to a strong start this year.

As adoptions of COmanage, Grouper, and midPoint got underway, the group investigated and reported on how provisioning and deprovisioning can be accomplished with each component or with some combination of the three.

This group also spent time noting different factors that bear on the choice of identifier(s) with the aim of documenting good practices. In a quest for a better framework for comparison of IAM solutions, planned or deployed, the group developed a high-level functional taxonomy for IAM to provide a common language for evaluating how and whether a solution provides needed capabilities.

InCommon midPoint Working Group

Chair: Slavek Licehammer, Evolveum
Wiki: https://spaces.at.internet2.edu/x/DIlgCw

This working group was commissioned by CACTI early in 2021 based on the growing demand for and adoption of midPoint. Presentations and discussions relevant to midPoint features took place in 2021, and feedback is being gathered from the community with the goal of helping to shape the new features based on real requirements from the broader community.

The working group also began to analyze community use cases and produce recommendations for how each use case can be solved using midPoint, which includes possible integration of midPoint with other tools, especially other Trusted Access Platform components.

Component Architects Working Group

Chair: Steve Zoppi, Internet2

This group meets regularly to support the advancement and better consolidation of documentation, training, and common support channels for the InCommon Trusted Access Platform software. Regular attendance of software component leads and IAM architects was expanded to include a midPoint lead as well as several InCommon Catalyst partners to help expand discussions around community adoption of the software.

The group worked to further define key IAM architectural patterns for the integration of the software components into the five most predominant use cases thought to be common among institutions looking to adopt the software to build or improve their IAM systems. The definition of these use cases is now being used to help inform plans for more specific training and support for adopters, such as CSP members and those attending BaseCAMP, to learn more about IAM.

Additional work was launched to further describe the details of the five use cases by providing specific examples, including architectural diagrams. The team is using this work to expand on the overall Trusted Platform Reference Architecture originally developed during the Trust and Identity in Education and Research (TIER) initiative.

The addition of several Catalyst partners to the group helped expand discussions on use cases and integration patterns to include the real-work experiences of the partners to help institutions develop and integrate IAM systems that included connections to a variety of commercial software products. These discussions are driving the group's development of overlays to the core reference architecture to include different commercial components common to higher education, such as HR, SIS, and ERP systems.

The Trusted Access Platform workbench was introduced as a set of operational instances of the software to be used by CSP members to gain immediate hands-on access prior to having to set up their own versions. The team reviewed and discussed the composition of the workbench to help recommend improvements as well as to inform those who work as subject matter experts (SMEs) in supporting the community. The team also discussed ways to attract new talent into the IAM world of higher education and research to help expand the pool of resources available to institutions.

Assured Access Working Group

Chairs: Brett Bieber, University of Nebraska
Wiki: https://spaces.at.internet2.edu/x/XImeCg

In June 2021, the Assured Access Working Group published its REFEDS Assurance Framework Implementation Guidance for InCommon Participants. This detailed report helps InCommon Participants understand the REFEDS Assurance Framework and how to implement it in a way that meets NIH's requirements for identity assurance.

Catalyst Program

In 2021, Internet2 announced the successful launch of the InCommon Catalyst Program, aimed at supporting higher education institutions, research organizations, and sponsored partners with better security, access to services, and user experience.

The program kicked off with eight organizations specializing in a wide range of IAM support services. These organizations are Alfa Jango, CILogon, Cirrus Identity, Evolveum, RDCT, Spherical Cow Group, Unicon and West Arete.

All InCommon Catalysts are Internet2 members who contribute to the research and education IAM community and work together to solve technology challenges and develop solutions that enable the academic mission. InCommon Catalysts made significant contributions to the trust and identity community in 2021.

Examples of projects that InCommon Catalysts support include integrating InCommon Trusted Access Platform components with an institution's existing IAM infrastructure; assisting research, higher education, and their industry partners in joining the InCommon Federation; providing expertise in designing IAM systems that are efficient and extensible; integrating IAM components or developing a purpose-built system; and advising on outsourcing IAM tasks or systems through hosted services.

The Path to Engagement: Supporting the Community

InCommon® INSIGHT

Last year InCommon Operations supported close to 12,000 help desk tickets.

InCommon Operations supported major initiatives within the trust and identity services community through its service infrastructure design and development workstreams.

- Notably, we worked with the community to identify reasonable benchmarks for transport layer security (TLS) grades required of SAML endpoints for the Baseline Expectations for Trust in Federation Version 2 program. We developed a solution that allows us to use open-source TLS grading software to enumerate TLS grades for all SAML endpoints registered by InCommon and then report to the InCommon site administrators and staff, executives, and CTAB on the specifics and trends of this critical security infrastructure.

- Further, InCommon Operations was key in the move of the eduroam U.S. service infrastructure (the eduroam Federation Manager) and community from a legacy platform into its new home alongside the existing SAML Federation Manager component.

- We also moved all InCommon's service infrastructure for both the SAML federation and eduroam into a new cloud-based DevOps environment, a major undertaking.

- In addition, InCommon Operations was part of a team of community members from the InCommon TAC which helped to overhaul the authentication and authorization components of the HECVAT. This group was led by Mary McKee (Duke University), Steven Premeau (University of Maine System), and Mark Rank (Cirrus Identity).

InCommon Operations supported almost 12,000 new requests for technical assistance in 2021 through our help@incommon.org help desk. That's approximately 50 tickets each workday related to the Federation, Certificate, and eduroam services. We're here to help and did we ever!

Appendix A: IAM Online Topics

IAM Online is a webinar series delivering interactive education on identity and access management (IAM), sponsored by InCommon and Internet2. Archived presentations are on the IAM Online YouTube channel.

NSF and Campus Cyberinfrastructure Plans: Enabling Access for Academic Collaborations (January 2021)
Presenters: Klara Jelinkova (Rice University), Marc Wallman (North Dakota State University), Tom Barton (University of Chicago and Internet2)

Growing an IAM Team (February 2021)
Presenters: Christopher Bongaarts, KT Cragg, and Bernard Gulachek (all at University of Minnesota), Kevin Morooney, Moderator (Internet2)

eduroam (US) Best Practices Guide (March 2021)
Presenters: Andrew Buker (University of Nebraska), Jeff Egly (Utah Education and Telehealth Network), Rob Gorrell (University of North Carolina at Greensboro), Neil Johnson (University of Iowa), Kim Owen (North Dakota State University), Mike Zawacki, Moderator (Internet2)

National Institutes of Health and Identity Management Requirements (April 2021)
Presenters: Ann West (InCommon/Internet2), Jeff Erickson (National Institutes of Health), Brett Bieber (University of Nebraska and InCommon Assured Access Working Group)

Increasing Identity Assurance and Improving NIH Readiness (May 2021)
Presenters: Brett Bieber, Chair, Assured Access Working Group (U of Nebraska); Tom Barton, Host (UChicago/Internet2)

One Opportunity, Three IAM Approaches (June 2021)
Presenters: Tommy Doan (Southern Methodist University), Erin Murtha (Internet2), Lacey Vickery (University of North Carolina at Charlotte), Keith Wessel (University of Illinois at Urbana-Champaign)

CILogon: Enabling Federated Access to Cyberinfrastructure (July 2021)
Presenters: Jim Basney (University of Illinois at Urbana-Champaign/NCSA), Scott Koranda (University of Illinois at Urbana-Champaign/NCSA)

Secrets, Supply Chains, and Securing Trust in the New Normal (August 2021)
Presenters: Rob Carter, 2021 CACTI Chair (Duke University), Matthew Economou (Research Data and Communication Technologies), Carl Waldbieser (Lafayette College), Nicole Roy (InCommon)

You're the Boss! Getting Involved with InCommon Community Groups (September 2021)
Presenters: Brad Christ (Eastern Washington University), Rob Carter (Duke University), David Bantz (University of Alaska), Keith Wessel (University of Illinois), Keith Hazelton and Ethan Kromhout (Trusted Access Platform Software Integration Working Group)

Watch Featured Videos from CAMP and ACAMP 2021 (October 2021)
We provided sessions from CAMP Week held Oct. 4-8, 2021. Videos were available for viewing in lieu of live programming.

Browser Changes and the Impact on Federated Identity (November 2021)
Presenter: Heather Flanagan (Spherical Cow Consulting)

HECVAT 3.0 Launches … to Outer Space? Plus, Updated IAM Questions (December 2021)
Presenters: Jon Allen (Baylor University), Josh Callahan (Humboldt State University), Charlie Escue (Indiana University), Brian Kelly (EDUCAUSE), Nick Lewis (NET+ Cloud Services/Internet2), Mary McKee (Duke University)

Appendix B: Glossary of Terms and Acronyms

Baseline Expectations – Baseline Expectations for Trust in Federation: A set of common expectations that all InCommon 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 – Collaboration Success Program: A diverse group of higher education institutions committed to adopting and deploying the Trusted Access Platform software components and helping to accelerate adoption for the rest of the 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.

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

InCommon Trusted Access Platform: The InCommon Trusted Access Platform is an identity and access management suite of services and software designed to integrate with existing systems, so it's easy to get started.

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 - to verify identity and gain access to resources.

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, which is an open standard for access delegation. 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://internet2.edu/community/about-us/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.

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