2022 InCommon Accomplishments

April 12, 2023

Document Title: 2022 InCommon Accomplishments
Repository ID: TI.167.1
Persistent URL: http://doi.org/10.26869/TI.167.1

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

Publication Date: April 12, 2023

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

© 2023 Internet2. This work is licensed under a Creative Commons Attribution 4.0 International License.

Table of Contents

About InCommon 3
Executive Summary 5
InCommon Academy 7
Top-Notch Training Offered Online and In-Person 7
Software Training 9
InCommon Collaboration Success Program 10
IAM Online 11
InCommon Federation 13
Maturation of Identity and Access Standards 13
Improving Trust and Security Among Federation Participants 13
Research Engagement 15
InCommon Trusted Access Platform 17
Access to Experts 17
Key Accomplishments in 2022 18
InCommon Certificate Service 21
Increased Engagement with Subscribers 22
eduroam 23
eduroam Support Organizations (eSOs) 24
Engaging the Community 26
Governance and Advisory Groups 26
Catalyst Program 33
Supporting the Community 35
Major Initiatives 35

About InCommon

GET ACCESS MANAGEMENT DONE. FASTER. BETTER. TOGETHER.

InCommon is a community that provides integrated service and software solutions to address identity and access management (IAM), single sign-on, access to the cloud and local services, and seamless global collaboration for students, faculty, staff, and researchers. Members of our community benefit from specialized resources tailored to help facilitate their entire organizations' access to:

User Lifecycle	**InCommon Trusted Access Platform** IAM Solutions	Manage people and their access
Academic Collaboration	**InCommon Federation** Community Access Framework	Connect your users across educational institutions
Security	**InCommon Certificates** Automated Certificate Lifecycle Management	Govern, manage, and automate the life cycles of digital certificates
Network Access	**eduroam** Secure Access to Wireless at 10,000+ Global Hotspots	Provide your users with simple, secure connectivity
Workforce Development	**InCommon Academy** Best in Class Tools and Training	Enhance your understanding of IAM
Expertise & Support	**InCommon Catalysts** Trusted Partners Offering IAM Expertise	Accelerate implementation and protect your investment

BY THE NUMBERS

1000+ INCOMMON PARTICIPATING ORGANIZATIONS.

THESE ARE YOUR PEOPLE.

THEY SHARE YOUR EXPERIENCE AND CHALLENGES IN MAKING ACCESS TO SERVICES EASIER.

InCommon®

20 YEARS OF EXPERIENCE HELPING ORGANIZATIONS FUTURIZE THEIR ACCESS MANAGEMENT STRATEGIES

2800+ eDUROAM HOTSPOTS ACROSS THE US

eduroam

2300+ VOLUNTEER HOURS CONTRIBUTED ANNUALLY TO DRIVE THE WORK

InCommon® COMMUNITY

Executive Summary

“On the road again/Just can't wait to get on the road again/The life I love is making music with my friends.”

—Willie Nelson

This iconic musical refrain aptly sums up our 2022. When the COVID-19 pandemic offered a reprieve, we took the opportunity to connect with members of the InCommon community face to face. From TNC in Trieste to EDUCAUSE in Denver, we were back on the road again.

Our year-long road trip concluded at Campus Architecture and Middleware Planning (CAMP) Week, held during Internet2’s Technology Exchange. We were able to get the band back together while welcoming new voices to the chorus as well. The harmony we witnessed as members of the community shared ideas and exchanged “war stories” about their common challenges felt a lot like making music with our friends, old and new.

Seeing so many of you last year energized and inspired our team in immeasurable ways that we believe you’ll see reflected in the work we do together in the near future. Join us for a quick look at our “travel journal” as we highlight our 2022 accomplishments.

Highlights

- **InCommon Academy** reached many hundreds of community members with both breadth and depth. Whether going wide or deep, participants unambiguously placed high value (an average 4.5/5 rating across all activities) on how IA assists in their professional development.

- The **InCommon Federation** infrastructure got better last year. The Federation is of higher quality, more trustworthy, and more secure. Baseline Expectations and the Sirtfi tabletop exercise were major contributors to these improvements.

- Organizational IAM infrastructures and services are constantly changing to meet institutional objectives. The **InCommon Trusted Access Platform**

demonstrated how it can also rapidly adapt to help take on these demands. For example, there were more than 100 new features added to Grouper last year.

- Digital certificate management can be an unsung hero of a security infrastructure. Rapidly changing standards for certificate management drive organizations toward ever-increasing automation. Sectigo and the **InCommon Certificate Service** have embraced ACME to help organizations with their automation goals. Serving nearly 700 organizations, managing hundreds of thousands of certificates to keep pace with change is challenging, and the certificate service delivered.

- **eduroam** continues its rapid expansion in the U.S. Building on massive changes made to the infrastructure, eduroam is taking root in K-12 through the eduroam Support Organization Program. Utah, Nebraska, Arizona, Oregon, and Connecticut have helped eduroam participation levels zoom past 1,000 subscribers last year, and the growth appears to only be getting started.

- 2022 was another dizzying year of change and growth in Trust and Identity at Internet2. The engine that makes these changes happen are the InCommon community leaders who volunteered 2,000+ hours of their time to help define and achieve a shared future.

InCommon Academy

InCommon ACADEMY INSIGHT

"BaseCAMP offered a refreshing mix of IAM content from high-level discussions to some deep dive examples. Presenters were friendly and knowledgeable and encouraged community engagement."
—2022 Attendee

The InCommon Academy provides:

- Opportunities for the community to convene and discuss common challenges and solutions (InCommon BaseCAMP)
- 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)

Top-Notch Training Offered Online and In-Person

InCommon BaseCAMP

The 2022 BaseCAMP was our largest to date with 137 participants. Our Buy Two, Get One Free promotion was popular and encouraged participation by multiple attendees from the same institution.

- 31 speakers participated.
- 97% of participants stated that all their questions were answered.

Committee Members:

- Tom Jordan, University of Wisconsin-Madison
- Warren Leung, University of California, Irvine
- Ben Rappleyea, Illinois State University
- Summer Scanlan, University of California, Berkeley
- Jeff Williams, University of North Carolina at Greensboro
- Kathy Wright, Clemson University

Table 1 – BaseCAMP Attendance

Year	2022	2021	2020	2019
Number of Attendees	137	108	79	70

InCommon CAMP Week
For the first time since 2019, CAMP Week was held in-person at Internet2's 2022 Technology Exchange in Denver, Dec. 5 - 9. The planning committee developed the IAM track of sessions, which included community presentations, such as case studies, organizations' innovations in identity management, best practices, and other information to help move the community forward. Almost 25% of TechEX attendees indicated IAM as one of their primary areas of interest.

Committee Members:

- Joanne Boomer - University of Missouri (committee co-chair)
- Mike Mays - University of Delaware (committee co-chair)
- Nicole Harris - GÉANT
- Ethan Kromhaut - University of North Carolina at Chapel Hill
- Keith Wessel - University of Illinois at Urbana-Champaign
- Pål Axelsson – SUNET
- Kyle Lewis - Research Data and Communication Technologies
- Charise Arrowood – Unicon
- Jon Miner - University of Wisconsin-Madison

InCommon ACADEMY INSIGHT

"This was an exceptional experience... potentially the most valuable conference I've attended in my career, and I look forward to coming to TechEx regularly in the future."
—2022 CAMP Attendee

Software Training

During 2022, InCommon Academy held a combined 12 training sessions for the InCommon Trusted Access Platform community-built IAM suite of software. Each course uses pre-configured training environments to enable hands-on labs, coupled with lecture and interactive discussion.

Table 2 – Trusted Access Platform Software Training Attendance

Course	Courses	Participants	Unique Orgs Attending	Average Rating (Scale 0-5)
COmanage Class	3	44	21	4.25
Grouper School	4	85	41	4.74
midPoint Basics	2	32	15	4.66
Shibboleth Installation	3	57	36	4.23
2022 Totals YTD (across the portfolio)	**12**	**218**	**84**	**4.48**
2021 Totals (across the portfolio)	10	257	80	4.5
2020 totals (across the portfolio)	*8*	*176*	*91*	*4.6*

InCommon ACADEMY INSIGHT

"This training covered all the basics needed to use Grouper: planning, setup, configuration, and how to find additional information when we need it. I cannot imagine trying to implement Grouper without having gone through this training."
—2022 Training Attendee

InCommon Collaboration Success Program

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. Since then, 28 research and education (R&E) institutions have participated in CSP. The organizations participating in the program joined to take advantage of all that CSP offers to Get IAM Done. Better. Faster. Together.

The class of 2023 formed in September 2022 and will complete its work in May 2023.

At the midpoint of the (CSP), all members of the 2022-23 cohort presented a deep dive of their IAM plans. This activity was highly valued by participants; it provides a key opportunity for them to share their in-progress plan and receive feedback from subject matter experts and peer institutions from the current and past CSP cohorts. Deep dive presentations also serve as the starting point for future case studies that will be shared with the community later this year.

The second half of CSP is designed to help institutions accelerate their progress toward their goals. It consists of customized connections of participants to experts, office hours topics driven by the cohort participants, continued training opportunities, and an opportunity for a facilitated peer discussion among the senior IT teams at the CSP cohort institutions. These activities are highly customized to the needs expressed by participants, yielding a unique experience each cohort year.

InCommon ACADEMY INSIGHT

"In the program, we're exchanging ideas about what's worked and what hasn't worked. That directness and honesty along with the feeling of community and collaboration, there is nothing else quite like it in terms of the value it gives."
—2022 CSP Cohort Participant

IAM Online

Last year InCommon hosted six webinars. As of Dec. 31, 2022, more than 700 people had registered for IAM Online, which continues to grow and serve as an important vehicle for outreach to build the InCommon community. The table below outlines the topics, speakers, and attendance for the year.

Table 3 – IAM Online 2022 Lineup

Month	Topic	Speakers	Attendance
Mar.	Where Innovation Meets Experience: The CIO Perspective on IAM	Bernie Gulachek (University of Minnesota), Dave Robinson (Grinnell College), and Kevin Morooney, Moderator (Internet2)	111
Apr.	The Collaboration Success Program: Getting IAM Done, Together.	Grady Bailey (University of Texas at Austin), Bruce Vincent (Stanford Linear Accelerator Center), Lacey Vickery (University of North Carolina at Charlotte), and Erin Murtha, Moderator (Internet2)	73
Jul.	Hello Passkey. Goodbye Passwords!	Tim Cappalli (Microsoft Identity) and Heather Flanagan, Moderator (Spherical Cow Consulting)	180

Month	Topic	Speakers	Attendance
Sept.	eduroam: What's New for You	Romy Bolton (Internet2), Amanda Molinari and Jeff Egly (UETN), Ben Nelson and Brett Bieber (Network Nebraska), and Mike Zawacki, Moderator (Internet2)	67
Oct.	Going Password-Free at UNC: Design, Decisions, and Development	Tariq Wilson (University of North Carolina at Chapel Hill) and Steven Zoppi, Moderator (Internet2)	160
Nov.	Extending IAM to the Cloud: It's Still Your Program.	Margaret Cullen (Painless Security), Kevin Hickey (University of Detroit Mercy), and Rob Carter, Moderator (Duke University)	97

InCommon Federation

More than 98% of identity providers and service providers registered in InCommon now meet Baseline Expectations for Trust in Federation Version 2 requirements.

The InCommon Federation provides the U.S. 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 U.S. with even more millions of users and thousands of organizations internationally.

Maturation of Identity and Access Standards

Increased adoption of multi-factor authentication (MFA) and identity assurance practices, spurred by the needs of the National Institutes of Health (NIH) and similar activities in Europe, produced increased field experience with the international standards underlying them. This experience highlighted areas of those standards in need of revision. InCommon staff and community members participated in revising the REFEDS MFA Profile and the REFEDS Assurance Framework. REFEDS is the international organization of Research & Education FEDerationS, to which InCommon and 70+ other national R&E federations belong. The revision addressed common questions arising in MFA deployments and facilitated an overhaul of the identity proofing material to make it easier for readers to determine what is required for each identity proofing level and to define criteria that are suited to the international R&E environment.

Improving Trust and Security Among Federation Participants

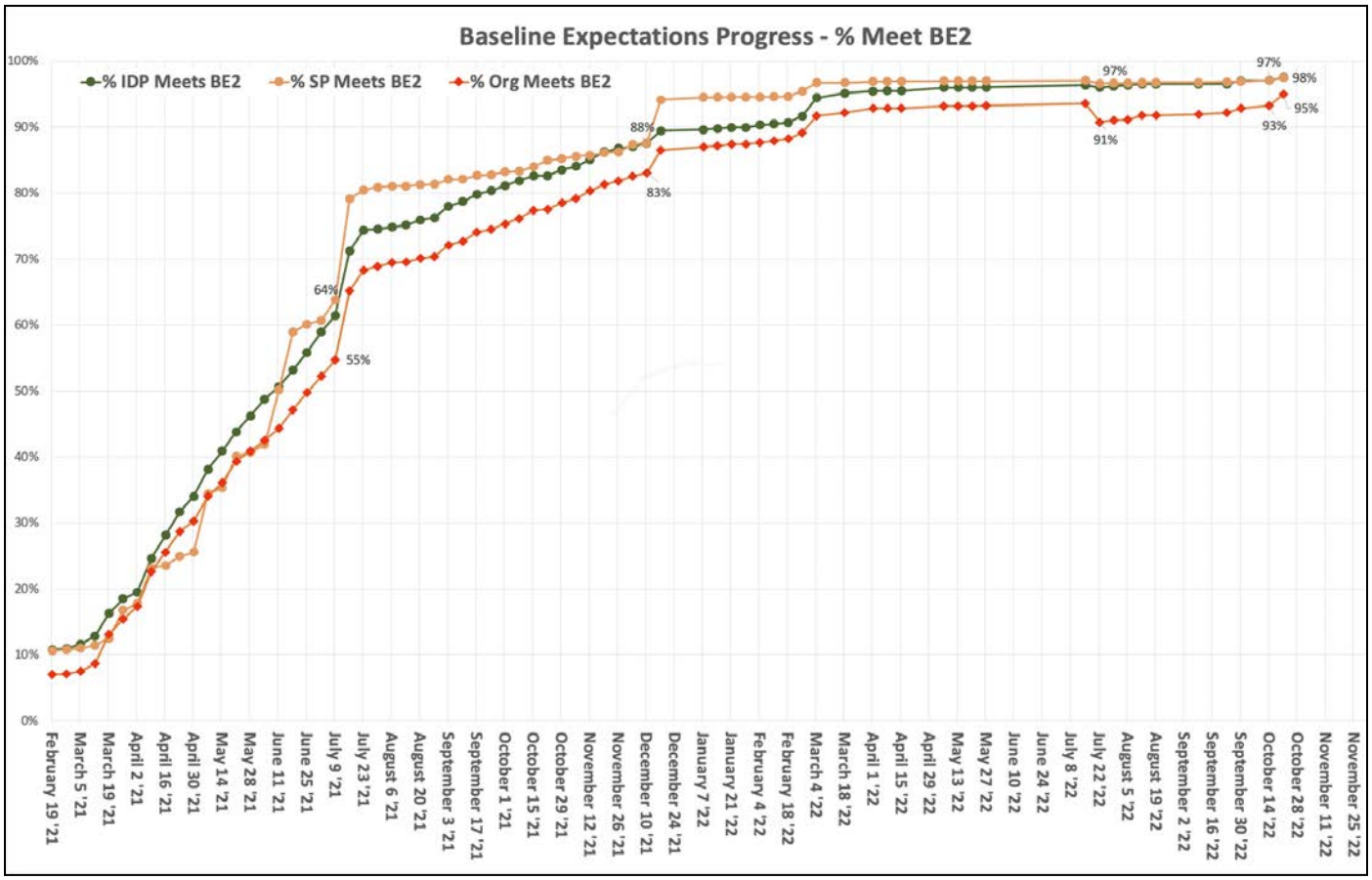
Baseline Expectations for Trust in Federation Version 2 (BE2)

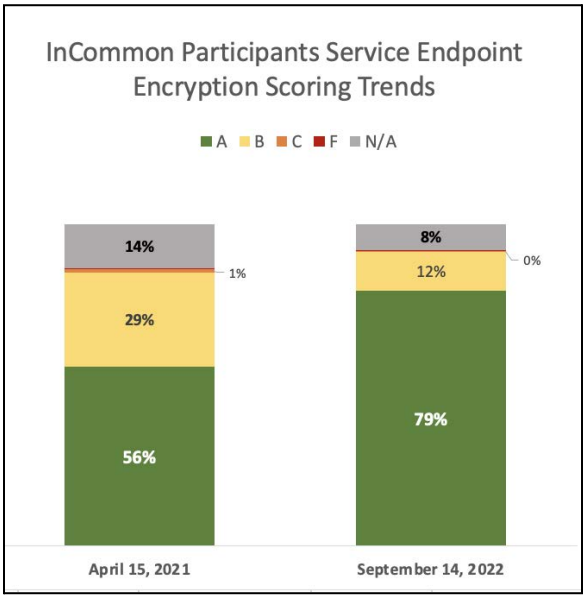
Continuing Baseline Expectations policy's goal to improve trust and security among Federation Participants, Baseline Expectations 2 introduced three security-focused elements:

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 (Sirtfi).

Last year marked another major milestone in the Federation's journey to BE2. As of December 2022, the InCommon Steering Committee has endorsed the Community Trust Assurance Board's (CTAB) BE2 dispute resolution recommendations. While CTAB and InCommon Operations continue to work with the remaining organizations to meet BE2 requirements, more than 98% of services (identity providers and service providers) registered in InCommon now meet BE2 requirements.





One highlight of BE2's impact on improving trust and security: when BE2 rollout began in 2021, 56% of InCommon registered services scored "A" in the endpoint encryption test. As of fall 2022, 79% scored A, indicating remarkable improvement among the Federation participants' security awareness and readiness. Another significant marker is that 99% of InCommon-registered services have acknowledged their conformance with Sirtfi.

Security Incident Response Trust Framework for Federated Identity (Sirtfi)

On Nov. 14–18, 2022, 10 participating organizations from the InCommon Federation came together to practice cybersecurity incident response cooperation using the REFEDS Sirtfi framework. This event culminated 10 months of work by InCommon's Sirtfi Exercise Planning Working Group (SEPWG) to pull off a distributed, multi-organizational cybersecurity tabletop exercise as a proof of concept that our federation can practice cybersecurity cooperation together.

Research Engagement

National Institutes of Health (NIH)

InCommon continued work to help NIH implement multi-factor authentication and identity proofing requirements for selected NIH services.

- New data was analyzed to inform a forthcoming communication campaign.
- NIH has begun internal engagements with sensitive research services to migrate them to rely on the NIH Federation Gateway.

Ecosystem for Research Networking (ERN)
InCommon continues to monitor and support the ERN (formerly “Eastern Research Network”) project.

- ERN continued its pilot implementation of federating use of a CryoEM instrument.
- Planning continues for further outreach and all-hands meetings.

National Science Foundation (NSF)
InCommon continued work to help NSF implement and communicate about an upcoming multi-factor authentication requirement for research.gov.

- Associated NSF staff have continued meeting with their counterparts at NIH.
- Additional research.gov usage data are being gathered to help support an eventual communication campaign.

Federated Identity Management for Research (FIM4R)
An in-person workshop, the 16th meeting of FIM4R, held jointly with The Americas Grid Policy Management Authority, was convened alongside TechEx. More than 40 people from three continents attended. A remote review session for those who could not attend was held two weeks later, which recapped some of the main notables:

- A new pattern of research proxy usage emerging from the European Open Science Cloud initiative, in which community proxies are paired with resource proxies, and their common policy requirements are addressed by membership in a new type of federation.
- Identification of possible new work ahead for the FIM4R community to address policy and process requirements of proxy operators.
- Recognition of ways in which some small- and medium-sized research collaborations are poorly served by existing services and the difficulties that occur when those projects extend beyond their initial funding horizon

InCommon Trusted Access Platform

The InCommon Trusted Access Platform is a community-built IAM services and software platform for R&E. 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, midPoint, and more recently a user interface for managing Shibboleth metadata (Shibboleth IdP UI). 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-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

Access to Experts

Slack channels are a valuable primary means for community members to communicate with developers and get their support questions answered. During 2022 the software component channels were very active as highlighted in the table below:

Software Component Slack Channel	Membership	Messages Posted
COmanage	280+	500+
Grouper	~600	7,300+
midPoint	340	~500
Shibboleth	400+	~1,400
Shibboleth IdP UI	100+	650+

InCommon TRUSTED ACCESS PLATFORM

INSIGHT

The members of the Grouper community were key to our success, and we could not have deployed Grouper without them. The InCommon Grouper Slack channel provided us with a means to post implementation issues and get answers quickly.

Several members of the channel (inclusive of peer institutions and software developers) were even willing to jump on a Zoom call with us to help us figure out problems we encountered along the way. Without this support, our Grouper implementation would not have been as successful as it is.
—Jason Rappaport, DevOps Engineer, Princeton University

Key Accomplishments in 2022

Shibboleth Federating Software

- Substantial adoption of Identity Provider (IdP) V4.1 and later versions, allowing the new plugin model shipped in 2021 to start to bear fruit – Reviewing the data, more deployers are upgrading and moving away from V3.
- Several releases of our OIDC OP plugin, including shipping support for generic OAuth use cases, and an early access beta of an OIDC RP plugin – The code has matured quickly.
- The work to redesign the Service Provider (SP) software was started. Progress has mostly consisted of identifying and refactoring code intended to be shared between the SP and the IdP.
- A complete redesign of our build process with Maven was achieved. There is a secured supply chain down to the actual Maven plugins used to build the IdP with complete public key signature verification of every code artifact used or shipped. This level of protection is rare and perhaps unique among open source software efforts.

Shibboleth Identity Provider (IdP) User Interface (UI) Software
Internet2 began a collaboration with Unicon in 2018 to gather community requirements around developing a graphical user interface to assist operators in integrating Service Provider (SP or Application) metadata with IdPs without the need to manually edit native XML files. During the last few years the development and community testing of this software has advanced to the point of adoption with the following accomplishments in 2022:

- 16 institutions have expressed interest, inclusive of contributing requirements and beginning testing.
- Five institutions have begun formal adoption with at least two of those moving to production.
- New features, such as Delegated Administration, operational on-the-fly updates of metadata, advances to stay current with the most recent Shibboleth releases, and support of OpenID Connect (OIDC), have been key to expanding adoption.

Grouper Access Management Software

- 14 software releases with more than 100 new or improved features
- New provisioners for Google, Azure, Box, Duo roles, midPoint, custom provisioners
- Improved provisioning UI
- Friendly attribute framework editor on group edit screen
- First pass at ABAC support with JEXL scripted groups
- Easy-to-use membership requirements
- New stem view privileges
- Improved failsafes
- Third-party library upgrades
- New Google and Duo admin role provisioners in framework
- Log4j upgrade

COmanage Registry Software

- Maintenance Registry v4.0.2 was released.
- Registry v4.0.2 was released.
- Match v1.0.0 was released.
- Registry v4.1.0 release candidate announced at the end of the year.
- CAKE framework migration is underway. So far, six milestone releases have been completed. Minimal viable release is expected at milestone release 12 or 13.
- The documentation for the project is updated to reflect deep-dive technical manuals and beginner-friendly user guides.

- First COmanage Match training workshop was conducted for 23 participants.

midPoint Registry and Provisioning Software

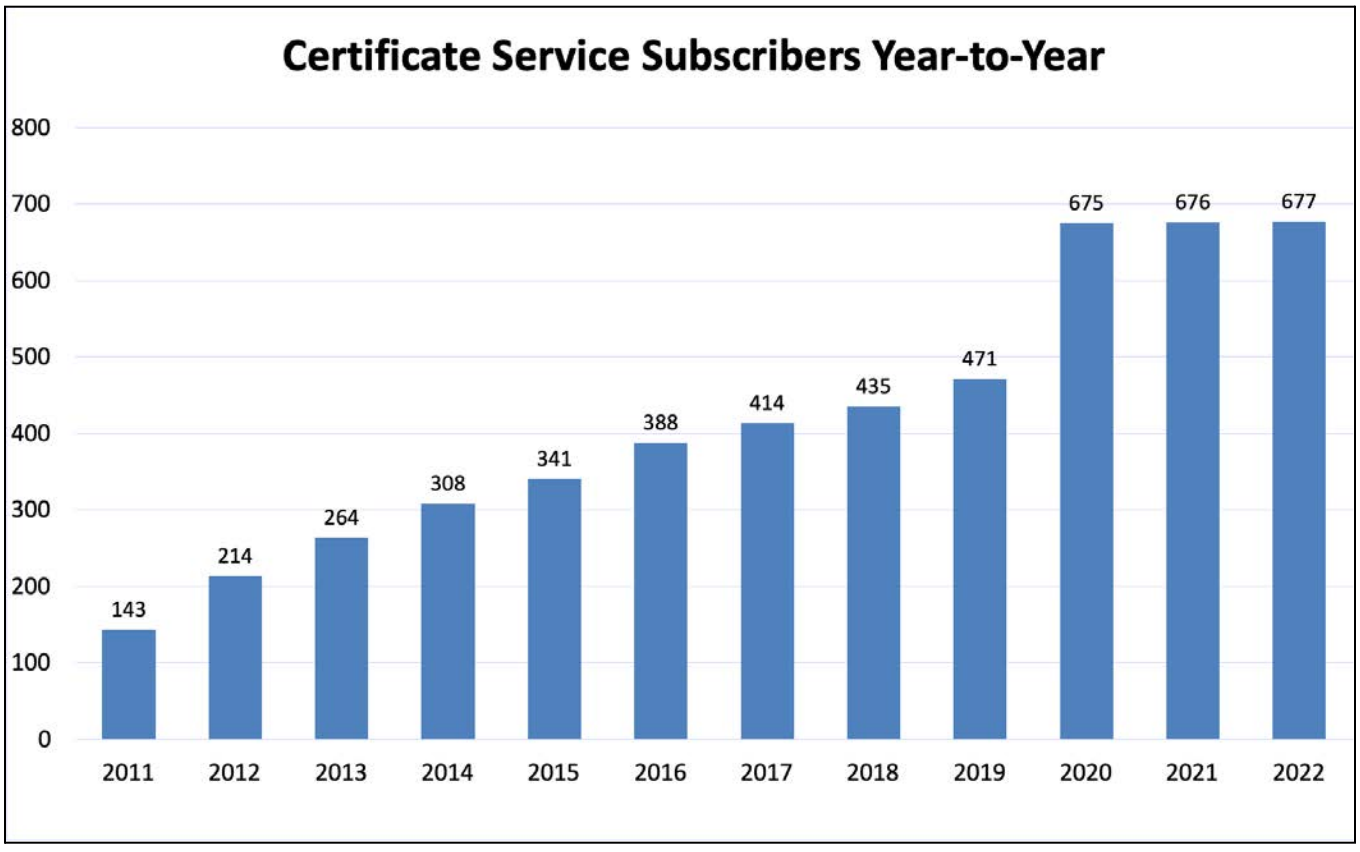
- midPoint 4.4.1 and 4.5 were released.
- midPoint in InCommon docker containers was upgraded to 4.4.1.
- The first version of ID Match API integration was developed. It will be released in midPoint 4.5.
- midPoint usage among HE institutions survey was published.
- Six public webinars were organized (midPoint 4.4, native PostgreSQL repository, upgrade to midPoint 4.4, tasks, customizing GUI, native reports).
- Work on guide about the first steps for implementing midPoint began, including first sharing and gathering feedback from the InCommon community through the midPoint working group. (https://docs.evolveum.com/midpoint/methodology/first-steps).
- A presentation was given at CSP about provisioning, synchronization, and connectors.
- A new website section was created to focus on getting started with midPoint (https://evolveum.com/get-started).
- Another Ivy league university started using the midPoint Academic Subscription.

InCommon Certificate Service

InCommon CERTIFICATES INSIGHT

The InCommon Certificate Service discussion list is among our most active with 1,600+ subscribers who offer each other ongoing support in managing certificates at their institutions.

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 Dec. 31, 2022, we had approximately 237,654 active certificates across 677 organizations.



Increased Engagement with Subscribers

Last year we focused in part on increasing our engagement with InCommon Certificate Service subscribers by launching a monthly communication and hosting events, both virtually and in-person.

- **Latest from the List:** In May we introduced a new monthly communication called *Latest from the List*, enabling us to leverage the active exchanges taking place between the 1,600+ subscribers to the InCommon Certificate Service discussion list. Each month we highlighted a frequently asked question from the list along with its corresponding response and added notes from our team as needed after vetting them. Participants on the list get the benefit of being a part of the InCommon community and drawing on its collective knowledge to get answers to their most pressing questions.
- **Webinar:** On March 22, 2002, the InCommon Certificate Service Team hosted a webinar to provide subscribers with updates on two important aspects of the service, OU field deprecation and ACME automation. Beginning April 1, 2022, Sectigo offered subscribers the option to temporarily turn off the OU field on a per-account basis, enabling them to conduct real-world tests to determine the impact of this change prior to the hard deadline of Sept. 1, 2022, for eliminating the field. Our team wanted to ensure that no InCommon Certificate Service subscribers are adversely impacted by this change. Plans are underway to host additional webinars in 2023.
- **Birds of a Feather (BOF):** During Internet2's Technology Exchange in Denver, we hosted a BOF gathering for the InCommon Certificate Service on Dec. 7, 2022. Subscribers were able to take advantage of this opportunity to get their questions addressed by Sectigo leadership. Nick France, CTO of SSL at Sectigo, who is responsible for the technology and practices necessary to operate Sectigo's global Certificate Authority (CA), traveled from Sectigo's UK office to attend TechEX.

Other Highlights from 2022 include:

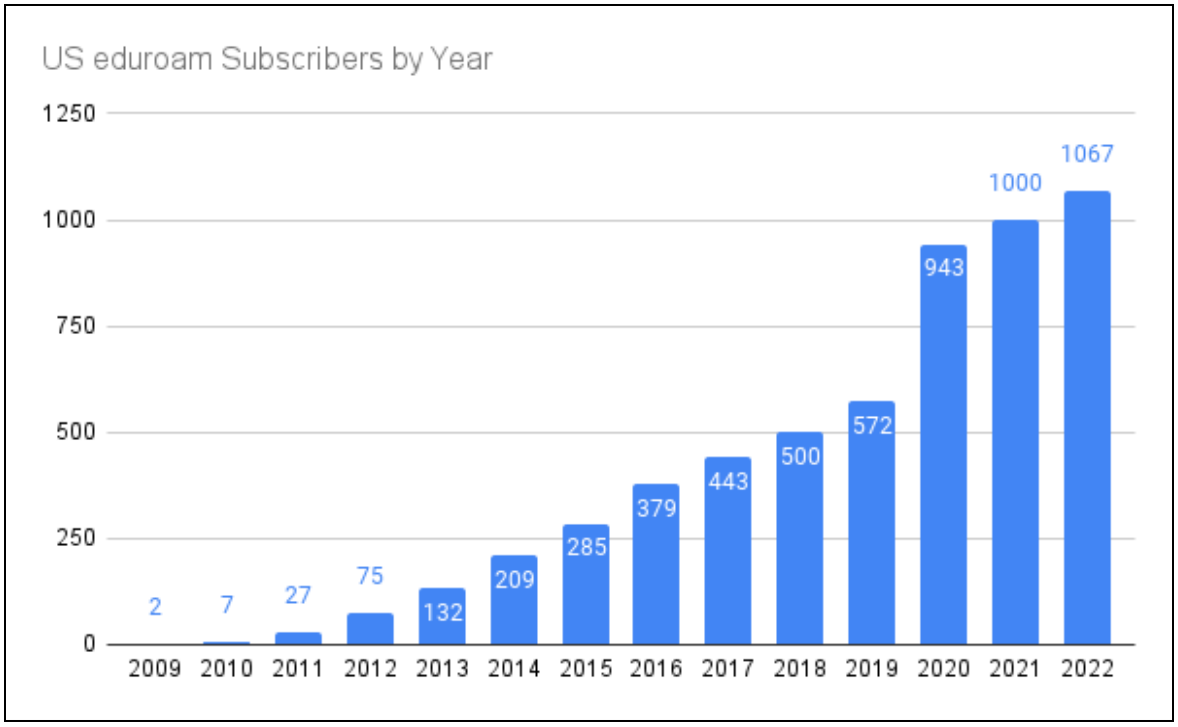
- Working with Sectigo to get an updated Higher Education Community Vendor Assessment Toolkit (HECVAT) in place
- Renewing our contract
- Holding the first in-person meeting between InCommon and Sectigo since the service was originally started
- Devising a new service strategy

eduroam

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

INSIGHT

Internet2 operates the U.S. node for the global eduroam roaming Wi-Fi network for R&E. 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. In 2022 the U.S. eduroam community grew the number of service locations in the U.S. to 2,958, the second largest number of service locations in any country in the world.



eduroam Support Organizations (eSOs)

ConnectEd Nebraska, Sun Corridor Network (serving Arizona), and Link Oregon joined the Utah Telehealth and Education Network (UETN) to form the latest cohort of eSOs and bring eduroam to the K-12 schools, libraries, museums, and hotspots within their states. Connecticut Education Network (CEN) continued its work with K-12, libraries, museums, and public hotspots in preparation for joining an upcoming eSO cohort. There are now more than 280 K-12 institutions using eduroam, with the program representing the fastest-growing segment of the eduroam community in the U.S. Here are some of the goals eSOs accomplished last year:

- Nebraska
  - Brought on 156 School Districts (covering 64% of all districts in Nebraska)
  - Deployed 9 SP-only sites at local Businesses
  - Partnered with local ISP to create SP-only sites at community centers and other public spaces
  - Ensured ongoing funding of the eSO program for the state of Nebraska through Network Nebraska fee structure
- Arizona
  - Deployed three initial pilot districts
  - Promoted eduroam within state library system
  - Started proof of concept for eduroam enabled LTE hotspots
- Utah
  - Nearly all school districts in Utah have now deployed eduroam
  - Brought up more than 50 new SP-only locations, including numerous state parks, DMV offices, and other state government facilities.
  - Launched “eduroam2go” – repurposing network gear to provide turnkey eduroam hotspots
- Oregon
  - Completed On-Ramp, joined as full eSO
  - Recruited nine school districts to lead eduroam deployment
- Connecticut
  - Deployed eduroam at four pilot school districts
  - Promoted eduroam within Connecticut’s K-12 community at annual member conference

INSIGHT

"Our entire team at Link Oregon is very excited to be recognized by Internet2 as the eduroam Support Organization for Oregon and to have this opportunity to extend the multiple benefits of seamless Wi-Fi roaming to our partners in the K-12, public library, and museum sectors."
—Steve Corbató, executive director, Link Oregon

eduroam Service Upgrades – Internet2 continues to enhance the eduroam service. This year, the team deployed a new self-service logging interface and testing for eduroam administrators. The service was also reviewed and optimized to run more cost effectively on its cloud infrastructure.

Better Security and Accessibility Documentation - The eduroam team completed both a HEVCAT and VPAT for the service this year. In addition to providing a community-accepted assessment, the completion of a VPAT encouraged several accessibility updates to the service, which is now accessible at a WCAG 2.0 AA level.

Community Working Group Report on eduroam User/Device Onboarding Requirements – The eduroam Advisory Committee (eAC) created a working group to develop requirement documents for user/device onboarding onto eduroam. This requirements document has been accepted from the working group by the eAC and is now out for community comment. The outcomes of the requirements working group will serve as a foundation for future service enhancement requests and review with community input and feedback.

Engaging the Community

Through its advisory committees and working groups, InCommon convenes the community to develop requirements, specifications, and program activities. Collectively, engaged participants contributed 2,800+ 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 2022 included:

- Overview and discussion of Trust and Identity goals for 2022
- InCommon Certificate Service review
- eduroam status report
  Included the following new members:
  - Klaas Wierenga from GÉANT, the global operators of eduroam and eduGAIN, the international federation peering service used by InCommon
  - Jen Leasure, the Executive Director of the Quilt
  - Brett Bieber, AVP IT Client Services University of Nebraska-Lincoln

PAG convened for a cumulative 24 community hours of work.

Community Architecture Committee for Trust and Identity
Chair: Robert Carter, Duke University
Vice Chair: Chris Phillips, CANARIE

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.

CACTI has been looking at the strategic landscape for IAM services at-scale within the R&E sector, and trying to understand gaps between the services that InCommon now provides, and what may be required in the future. CACTI also spun up the “Linking SSO Systems” working group, co-chaired by Brian Arkills from the University of Washington and Etan Weintraub from Johns Hopkins University.

CACTI also hosted and presented the November IAM Online webinar, “Extending IAM to the Cloud: It’s Still Your Program.” Thanks to Margaret Cullen, Kevin Hickey, and Rob Carter for leading that effort.

CACTI convened for a cumulative 91 community hours of work.

InCommon Steering Committee
Chair: Brad Christ, Eastern Washington University
Vice-Chair: Marc Wallman, North 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. The committee began discussions around kicking off a Futures Planning Process in 2023.

InCommon Steering convened for a cumulative 192 community hours of work.

“I’ve been able to work with great people from other institutions who usually have better ideas than I do – at least until I make them mine too. Working with others in InCommon is a welcome shift away from break-fix and other pressing and mundane day-to-day work and keeps my perspective appropriately focused on fundamentals and longer term goals.”
– David Bantz, 2022 CTAB Chair

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.

CTAB continues to spearhead InCommon's effort to improve trust and security among participants. Working in collaboration with InCommon Operations, CTAB completed InCommon's migration to Baseline Expectations 2. (Reference: InCommon Baseline Expectations 2 Dispute Resolution Closing Actions)

CTAB also sponsored InCommon's Security Incident Response Trust Framework for Federated Identity (Sirtfi) Exercise Planning Working Group. The group devised a distributed cybersecurity incident response exercise and subsequently carried out the exercise with community volunteers in November 2022.

Between attending committee meetings, hosting office hours, and participating in working groups, CTAB members collectively contributed an estimated 458 hours of effort in 2022.

InCommon COMMUNITY INSIGHT

"Volunteering with InCommon working and advisory groups has really helped me to grow, both personally and professionally. If you'd told me 12 years ago that I'd be chairing the TAC, I'd have said you were crazy. The challenge helps me to grow in leadership, learn lots of really useful technical bits, and feel the excitement of contributing to an organization that helps amazing people and amazing institutions do amazing things."
– Keith Wessel, 2022 TAC Chair

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.

TAC focused its 2022 efforts around two areas: making federation easier and looking ahead to the future of federation. "Making federation easier" has been a theme for the TAC for the past couple of

years. Items in this area focused on simplifying the process of deploying service providers and identity providers that can interoperate with the Federation with minimal effort or configuration. Notably, our work adopting the SAML 2.0 deployment profile and new SAML subject identifiers along with creating federating testing all work toward this goal. The TAC also continues to keep an eye on the HECVAT and how it can be used to simplify and improve federated services.

In the area of "the future of federation," the committee tracked several standing items this year such as upcoming browser technology changes which will very definitely impact federation in the near future, the challenge of integrating SP "middlethings" into the Federation properly, and policies around entity IDs. During the latter half of the year, we also spent a lot of time understanding the impact of digital wallets and verifiable credentials and how they fit into federation. The following sections detail our progress on each of the year's work plan items.

Reference: 2022 InCommon Technical Advisory Committee Accomplishments

TAC members collectively contributed an estimated 458 hours of effort in 2022.

eduroam-US Advisory Committee (eAC)
Chair: Jeff Egly, Utah Education and Telehealth Network (UETN)
Vice-Chair: Brett Bieber, University of Nebraska

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

Key topics discussed in 2022 included:

- Accepting User/Device Onboarding service requirements
- Providing community input on infrastructure changes and Support Organization program updates

eAC convened for a cumulative 120 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

This working group meets every week on alternating days and has attracted a large following of community IAM architects from those just beginning to highly experienced veterans in the field.

The group focuses on all aspects of implementing the Trusted Access Platform software including integrations between components and with commercial applications.

Highlights for 2022 include:

- Reviewed Identity Match API including complete implementations of the API in COmanage and independently in midPoint
- Recorded discussions of Grouper templating, provisioning, and proposed entity data system capabilities with Chris Hyzer
- Recorded discussion of COmanage and midPoint user invitation, self-registration, and onboarding and midPoint SSH connector
- Architecture and design for using COmanage as Identity Registry integrated with midPoint for provisioning
- Volunteers took on drafting a list of connector how-tos.
- Helped organize a panel on campus midPoint deployments for TechEx in December 2022
- Interview with experts to obtain better understanding of the growing adoption of Azure AD for a growing set of IAM tasks
- Organized a project for next iteration of Grouper/midPoint integration
- Developed a Process map illustrating the path from raw System of Record (SoR) data to access policy and enforcement
- Reviewed state of development of ProvisioningIAM's open source Base Connector Utility for creating ConnID connectors for midPoint
- Supported the Trusted Access Platform (TAP) Workbench used by participants in the Collaboration Success Program
- Conducted review of the draft Big Ten Academic Association (BTAA) Provisioning Cookbook

Working group members collectively contributed an estimated 500 hours of effort in 2022.

InCommon midPoint Working Group

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

This working group was convened to advance community understanding for implementing and integrating midPoint. Several demonstrations were conducted for and by the community:

1. Patterns for using midPoint in Higher Education
2. Integration of Identity Matching with midPoint
3. Updates to the User Interface for ease of use
4. Demonstrations of using midPoint for Identity Governance

The working group provided a great forum for discussion on integrations of midPoint with Grouper and applications as well as resolving some common issues institutions were having. Various issues around the use of midPoint containers and potential improvements based on community experiences were discussed with some resolution for implementation going forward. A base connector developed by Provision IAM was presented and discussed for use in the development of new connectors. Recordings of the more interesting demonstrations and presentations are linked to the wiki shown above. Thanks to the Evolveum Team for preparing and conducting demonstrations and leading this working group.

Working group members collectively contributed an estimated 297 hours of effort in 2022.

InCommon PeopleSoft Integration Working Group

Chair: Tommy Doan, Southern Methodist University
Wiki: https://spaces.at.internet2.edu/display/DSAWG/InCommon+PeopleSoft+Integration+Working+Group

This was a new working group sanctioned by CACTI for 2022. A primary accomplishment was the convening of many institutions already using PeopleSoft and presenting their use cases as to how the application was currently used at their institution as well as goals for integrations with the Trusted Access Platform software. Several institutions that have already successfully accomplished some

level of integration with the Trusted Access Platform presented their patterns and ways they dealt with challenges along the way. Recordings of the more interesting demonstrations and presentations are linked to the wiki shown above. Thanks to Tommy Doan of SMU for volunteering to chair this group. He will be assisted by Keith Hazelton (consultant to Internet2) and Ethan Kromhout (UNC Chapel Hill).

Working group members collectively contributed 217 hours of effort in 2022.

Component Architects Working Group

Chair: Steven 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.

Highlights for 2022 include:

- Regular quarterly review of software component progress and issues reflected upon the things of note emerging from CACTI and where there are intersections
- Opened the year to re-focus on priorities around community adoption and education, roles of partners, software projects, and Internet2
- Improving on documentation and communication with the community on location of resources (i.e., wiki vs complimentary resources on the web, etc.) and how to help provide better navigation to key topics
- Review of telemetry and heuristics primarily for the Trusted Access Platform component containers – how to take steps to get statistical information from each of the deployed solutions to help reflect adoption back to the community as well as provide information back to institutional users
- Working with the community to drive more of their contributions in the form of how-tos and even software modules to reduce replication and accelerate development for smaller institutions with similar use cases
- Addressing emerging needs driven by NIH and healthcare (in general)

- Succession planning for our teams to ensure continuity in community support for the software and subject matter experts in IAM in general

Of particular note was the development of a formal charter for this working group, which will be finalized and published in early 2023.

Working group members collectively contributed an estimated 460 hours of effort in 2022.

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.

During 2022 the program matured into a fully collaborative team who contribute to the R&E IAM community and work together to solve technology challenges and develop solutions that enable the academic mission. The program consists of nine organizations: CILogon, Cirrus Identity, Evolveum, Moran Technology, Provision IAM, RDCT, Spherical Cow Group, Unicon, and West Arete.

InCommon Catalysts are always looking at ways to provide support to the community by actively participating in community committees and working groups. In this way, they stay in tune with community needs and also contribute expertise from areas they specialize in. See InCommon Catalysts Bring Energy and Expertise to Community Conversations for highlights of the many activities to which the organizations contributed.

Last year, the InCommon Catalysts gave lightning talks at BaseCAMP and TechEX. Three catalysts also sponsored BaseCAMP: Cirrus Identity, Unicorn, and West Arete. During TechEX, they presented at a number of sessions.

As part of our ongoing commitment to providing the community with additional opportunities to benefit from the insights and expertise of InCommon Catalysts, we introduced a quarterly Q&A advice column, *Catalyst to Catalyst*, in April that we feature in our e-newsletter InCommon News. *Catalyst to Catalyst* provides perspectives on key IAM topics for the InCommon community.

The InCommon Catalysts convened for a cumulative 51 community hours, which does not include the many hours they spent assisting members of the community through the InCommon Collaboration Success Program and other initiatives.

Supporting the Community

InCommon INSIGHT

Last year InCommon Operations supported close to 8,000 help desk tickets.

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

Major Initiatives

- We checked the TLS security level of more than 500 identity providers and nearly 6,000 service providers 32 times during the course of 2022 and reported it to Federation Site Administrators via the InCommon Federation Manager.
- We continue to evolve and refine our implementation of service features that support the InCommon Federation Baseline Expectations for Trust in Federation v2.0.
- We moved InCommon Federation delegated administrators to unified federated login in the Federation Manager via Internet2's IAM platform (based on the InCommon Trusted Access Platform) and now have only one legacy group of users left to migrate to federated/IAM platform-based access.
- We developed processes for supporting eduroam testing and deployed them in the eduroam Federation Manager.
- We engaged with agency partners Painless Security, Unicon, Cirrus Identity, Alfa Jango, and Provision IAM to help develop our infrastructure and services in a scalable, reliable way
- We continue to work to build our information security program. We helped the community with a number of security events throughout the course of 2022.

InCommon Operations supported almost 8,000 new requests for help in 2022 through our help@incommon.org help desk.