



InCommon®



## 2019 InCommon Accomplishments

February 5, 2020

**Document Title:** 2019 InCommon Accomplishments

**Repository ID:** TI.141.1

**Persistent URL:** <http://doi.org/10.26869/TI.124.1>

**Authors:**

Dean Woodbeck

 <https://orcid.org/0000-0002-0996-1719>

Ann West

 <https://orcid.org/0000-0002-8215-4913>

Kevin Morooney

 <https://orcid.org/0000-0001-9058-3921>

**Publication Date:** February 5, 2020

**Sponsor:** Vice President, Trust and Identity Services and NET+

© 2020 Internet2. This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

---

## Table of Contents

---

# Table of Contents

About InCommon .....	3
Executive Summary .....	4
2019: Expanding the Tent .....	6
Articulating the Value Proposition .....	6
The InCommon Academy .....	6
Expanding and Supporting the Software .....	9
Scaling the Federation and improving trust .....	10
Making Collaboration Easier .....	13
Securing the Federation: SIRTFI (Security Incident Response Trust Framework for Federated Identity) .....	13
Research & Scholarship Category of Service Providers .....	14
Engaging with Research Communities.....	15
Future of Federation .....	15
eduroam .....	16
InCommon Certificate Service .....	17
Engaging the Community .....	18
IAM Online Webinar Series .....	18
2019 Internet2 Global Summit and 2019 Technology Exchange .....	18
Working Groups .....	18
Governance and Advisory Groups.....	20
Appendix A: 2019 Active Working Groups .....	23
Appendix B: IAM Online Topics .....	25
Appendix C - Glossary of Terms and Acronyms .....	26

## About InCommon

---

### About InCommon

---

InCommon provides the venue for the research and education community to work together and solve common problems. How do we do it?

- **Community-driven everything** – We work together with shared passion, directness, respect, and humor.
- **Act locally; think globally** - Our community-built solutions work for collaborations on campus, around the state, 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 identity and access management solutions solve problems related to:

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

Here are the services we provide:

- **The InCommon Federation** - Privacy-preserving single sign-on access to services - locally and around the globe.
- **The InCommon Trusted Access Platform** - Community-developed identity and access management software and services.
- **eduroam** - Operating (within the U.S.) the global WiFi network for research and education.
- **The InCommon Certificate Service** - Unlimited server and user certificates for one annual fee.
- **The InCommon Academy** - Expert-led component training, implementation support, and other resources.

---

## Executive Summary

---

*InCommon now has responsibility for the InCommon Trusted Access Platform, focusing on solutions such as managing access, scholarly collaborations, guest systems, and identity lifecycle management.*

---

## Executive Summary

---

This document outlines the major accomplishments for InCommon (the Internet2 Trust and Identity division) in 2019.

**Articulating the InCommon value proposition** - Changes in the InCommon family of services over the last two years provided an opportunity to revisit and revise the value proposition. As part of that effort, InCommon [rolled out a new website](#) mid-year, with an emphasis on clearly communicating the services and solutions provided by and for the community.

**Enhancing and supporting the InCommon Trusted Access Platform software** - The three-year TIER program (Trust and Identity in Education and Research) funded work to connect and simplify major community-developed identity and access management software ended in 2018. In 2019, InCommon assumed responsibility for what is now the [InCommon Trusted Access Platform](#), focusing on the solutions including managing access, scholarly collaboration, guest systems, and identity lifecycle management. An InCommon fee change, along with funding from Internet2 member dues, will fund the continued development and packaging of the software.

**InCommon Academy and expanding the tent** - The focus on solutions, and feedback that InCommon needs to do more to attract and educate those new to identity and access management, led to the InCommon Academy and BaseCAMP.

The [InCommon Academy](#) developed and delivered installation and training workshops for components of the InCommon Trusted Access Platform (Shibboleth, Grouper, COmanage, and midPoint).

The first [BaseCAMP](#) provided an introduction to identity and access management, and to federation and the InCommon Trusted Access Platform IAM suite of software. The intent is to expand the community and ensure younger professionals receive the background and training they need for success.

**Scaling the Federation and improving trust** - By mid-2019, 100 percent of InCommon participants met the [Baseline Expectations for Trust in Federation](#). Implemented in early 2018, this program most notably defined an InCommon Dispute Resolution process for participants and required certain elements be

## Executive Summary

---

included in the trust registry (metadata), such as certain contact information. InCommon also rolled out the [Metadata Query Service](#) (also known as per-entity metadata), which will eventually replace the metadata aggregate using a DNS-like pull approach.

**eduroam pilot in Utah** - InCommon and the Utah Education and Telehealth Network (UETN) [piloted a program](#) to deploy a wide scale implementation of eduroam to select K-12 institutions in the state.

## 2019: Expanding the Tent

---

*InCommon established the InCommon Academy to provide training and education opportunities related to the InCommon Trusted Access Platform components.*

### Articulating the Value Proposition

Much has changed since the last time InCommon redesigned its website in 2012. At that time, InCommon operated the federation and the InCommon Certificate Service. In the intervening seven years, InCommon has become a major focus of Internet2 and two significant services have joined the fold: eduroam and the InCommon Trusted Access Platform (identity and access management software suite and services).

Work in 2019 took advantage of the opportunity to clarify the InCommon value proposition as a platform for access to global collaboration communities, focusing on solutions provided by the software and services, and a resulting redevelopment of the website.

On Thursday, June 13, 2019, InCommon launched [the new incommon.org](https://www.incommon.org) with simplified navigation, clearer language describing the community and services, and a cleaner look. The use of WordPress as a platform provides the opportunity for multiple people to edit pages, allowing for more timely updates.

More features will come with version 2, including easier-to-access information about each InCommon organization, Identity Provider, and Service Provider.

### The InCommon Academy

The InCommon community, like many of the participating organizations, faces the challenge of educating and training professionals who are new to identity and access management in general and the U.S. research and education identity community in particular. During late 2018, [InCommon's Attributes for Collaboration and Federation Working Group](#) recommended that InCommon “expand the tent” by providing those new to the field with ways to learn about the community and its history, as well as educational and training opportunities.

### Expanding Training and Learning Opportunities

For the past decade, InCommon has offered several Shibboleth Installation Workshops each year. The InCommon Trusted Access Platform connected major community-developed software components and made them easier to

## 2019: Expanding the Tent

---

install. But this also created the need for training programs that would help participants deploy and configure the software.

In response, InCommon introduced the [InCommon Academy](#) during 2019, offering installation and configuration training as well as a hands-on practicum for InCommon Trusted Access Platform components, including Shibboleth, Grouper, COmanage, and midPoint. Offered in the context of business solutions such as guest management, access management, and research collaborations, the training program provides a context for the purpose of each component, as well as implementation guidelines.

### Training Curriculum

The Academy offered six courses during 2019; each using pre-configured training environments to enable hands-on labs, coupled with lecture and interactive discussion, including a virtual midPoint class.

Course	# Courses	# Participants	Unique Orgs Attending	Average Rating
COmanage Class	1	8	6	4.5 / 5.0
Grouper School	2	48	28	4.7 / 5.0
midPoint Basics	1	22	12	4.4 / 5.0
Shibboleth Installation	2	57	42	4.5 / 5.0
Totals (across the portfolio)	6	135	70	4.5 / 5.0

### Hands-on Practicum: Collaboration Success Program

The second iteration of the [Collaboration Success Program \(CSP\)](#) formed, involving six higher education institutions working together to adopt one or more of the InCommon Trusted Access Platform software components, and helping to accelerate adoption for the rest of the community.

## 2019: Expanding the Tent

---

*BaseCAMP fills a gap by providing a place for introductory information for those new to identity and access management and/or federation.*

The 2020 cohort formed during the fall of 2019, first coming together at a face-to-face meeting to learn more about common solutions provided by the

InCommon Trusted Access Platform and to [draft project abstracts](#). Each participating organization engaged in one or more software component training workshops (Shibboleth, Grouper, COmanage, and midPoint).

During 2020, the CSP participants will work through their project plans, resolving issues and sharing best practices.



### BaseCAMP 2019

Together with InCommon staff, a community planning group created [BaseCAMP](#) to provide an introduction to identity and access management, federation, and related software. Other meetings already provide a place to hear case studies and innovations (the Internet2 Technology Exchange) and forward-looking global discussions (AdvanceCAMP, which also takes place at TechEx). In addition, the Internet2 Global Summit provides a place for information geared toward managers and CIOs.

BaseCAMP 2019 took place in Milwaukee, Wisconsin, with an ambitious community-designed and delivered program that included a look at the identity and access management landscape, specifics of how the InCommon Federation works, and how the community-developed InCommon Trusted Access Platform can help solve common challenges for campuses, research organizations, and their partners. BaseCAMP attracted 70 attendees from 44 organizations. On a post-event evaluation, 96 percent of respondents would recommend BaseCAMP to others. Future BaseCAMPs are in the planning stages (including one scheduled for June 2020).

---

## Expanding and Supporting the Software

---

*Statistics show that general adoption of the InCommon Trusted Access Platform components is increasing.*

---

## Expanding and Supporting the Software

---

In 2019, InCommon assumed responsibility for what is now the [InCommon Trusted Access Platform](#), an identity and access management services and software suite designed by and for education, research, and their partners. It is built to integrate with existing systems and is packaged to simplify installation and configuration. This continues the work started during the three-year TIER program (Trust and Identity in Education and Research), which concluded at the end of 2018.

The suite helps solve common identity and access challenges, including

- single sign-on
- managing access
- managing scholarly collaborations
- enabling guest access
- supporting the identity lifecycle, provisioning and deprovisioning, guest systems, and others.

An InCommon fee change (effective January 1, 2020), along with funding from Internet2 member dues, will fund the continued development and packaging of the software.

Advances were made in the Trusted Access Platform software packages including:

- Inclusion of a midPoint container with [the software releases](#)
- Release of the [Shibboleth IdP Metadata Management Graphical User Interface](#) (Shibboleth UI) for community testing and feedback
- Development of a container for identity matching to prevent duplication (final development and testing still underway)
- Availability of a [demonstration/reference container package](#) with Grouper and midPoint integrated
- General improvements in the automated build/test pipeline enabling updated releases to be built in a few minutes as patches and minor features emerge from the component projects

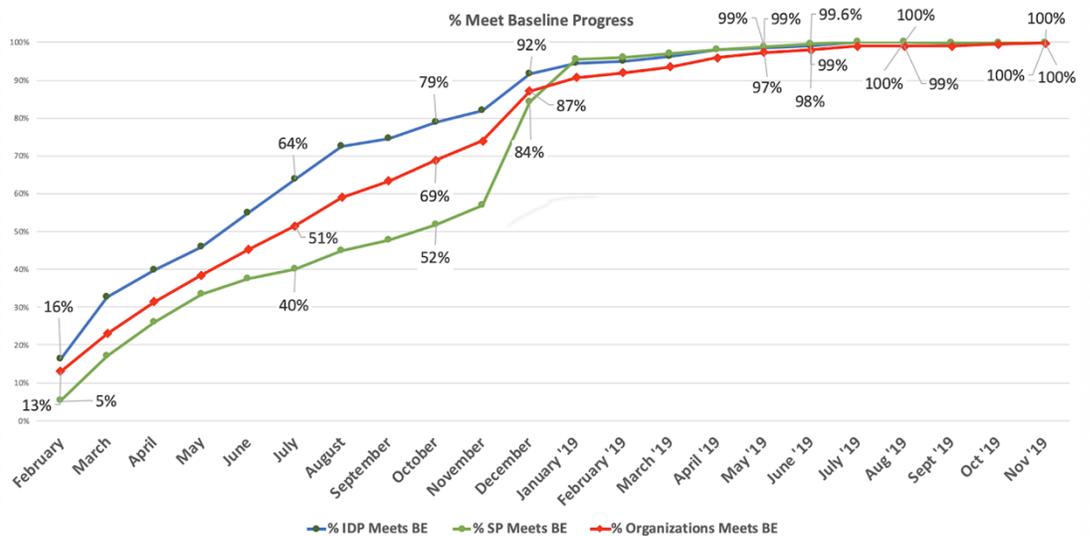
Statistics show that general adoption is increasing with thousands of downloads and hundreds of running containers in the field (note that these may not be in production but used for evaluation or training).

## Scaling the Federation and improving trust

# Scaling the Federation and improving trust

The growth of the InCommon Federation, now with more than 760 organizations, has led the InCommon [Technical Advisory Committee](#) (TAC) and [Community Trust and Assurance Board](#) (CTAB) to consider ways to maintain consistent trust among all participants in a federation of this size, and to look for efficiencies. Two 2019 milestones include significant steps to address these issues.

**Baseline Expectations for Trust in Federation** - By mid-2019, 100 percent of InCommon participants met the requirements of [Baseline Expectations for Trust in Federation](#). Implemented in early 2018, this program standardizes some processes among participants and requires certain elements be included in the trust registry (metadata), such as certain contact information.



*The community met Baseline Expectations over a relatively short period of time.*

Led by CTAB, the community developed this set of common expectations with the goals of:

- providing a baseline for trust

## Scaling the Federation and improving trust

---

*The Metadata Query Service provides faster start-up and far less memory requirements for those using the InCommon Federation.*

- making collaboration more predictable
- ensuring that the InCommon Federation's strategic value to research and education continues to grow

Also during 2019, CTAB [surveyed the community](#), asking about interest in several additions to Baseline Expectations. Based on that survey and further discussions, CTAB expects to propose another set of expectations sometime in 2020.

InCommon's success with the Baseline Expectations program has been noticed internationally. REFEDS and eduGAIN, the two leading organizations supporting international federation, have begun to determine how to translate this success across research and education federations worldwide.

**Metadata Query Service (per-entity metadata)** - Per the TAC's [Per-Entity Metadata Working Group final report](#), InCommon developed and rolled out a production candidate of the [Metadata Query Service](#) (also known as per-entity metadata) (MDQ), which will replace the metadata aggregate. Using MDQ, Identity Providers and Service Providers no longer have to download pre-load, and verify all of the thousands of entity descriptors in the InCommon aggregate. With MDQ, the SP or IdP only loads these on-demand. The service has an operational record of 100 percent uptime since it was launched in July 2019. More information on InCommon service status is available at <https://status.incommon.org/>

Reports from those switching to MDQ have been highly positive. One service provider reported: "We were able to switch to using MDQ. The service restarts in 5 seconds now versus 15 minutes." An identity provider sent an in-use memory graph showing the moment the university switched to using MDQ on its production Identity Provider servers.

## Scaling the Federation and improving trust



*One organization's graph of how MDQ significantly reduced memory needs.*

## Making Collaboration Easier

*The Research & Scholarship Category of Service Providers continues as an easy way to provide scholarly collaborators with unfettered access to services.*

## Making Collaboration Easier

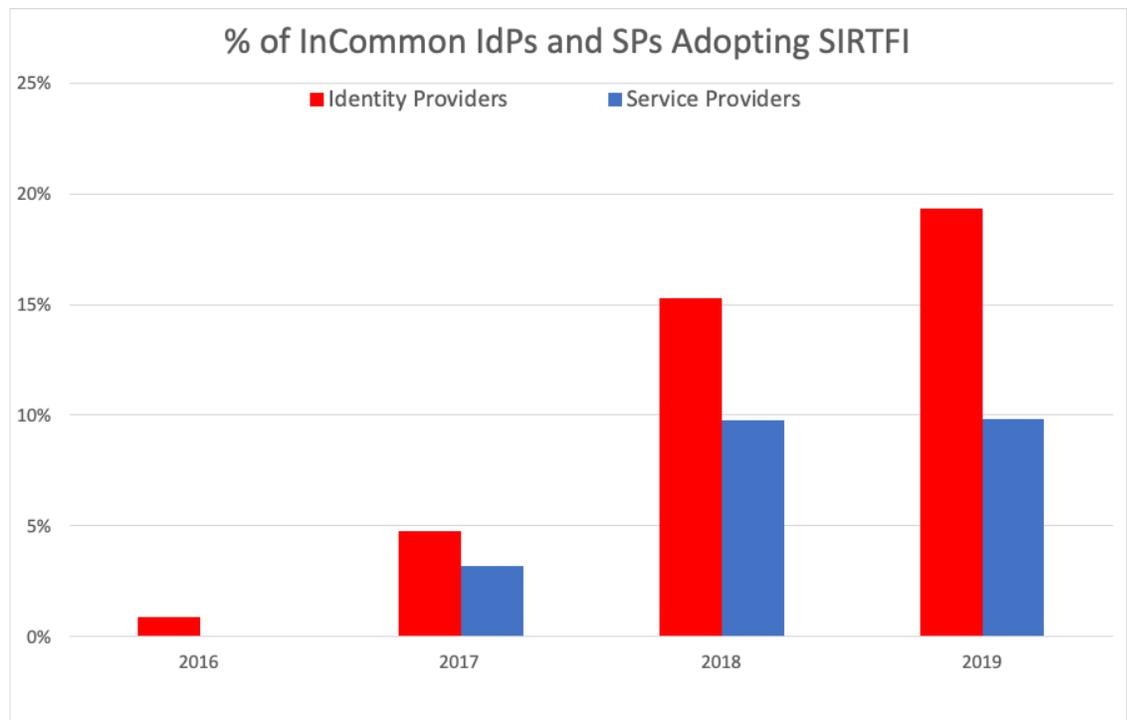
Support for research and academic collaborations is one of InCommon's key missions. InCommon continues to strengthen its connections with research communities and with other research and education federations worldwide.

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



InCommon supports the [international SIRTFI framework](#), which provides a way to coordinate incident response across all federations, and encourages adoption by all Identity Providers and Service Providers. covers four areas: operational security, incident response, traceability, and participant responsibilities.

The framework can also serve as a best practice roadmap for federation participants. The CTAB will propose addition of SIRTFI and other security-related elements to InCommon's Baseline Expectations in 2020.

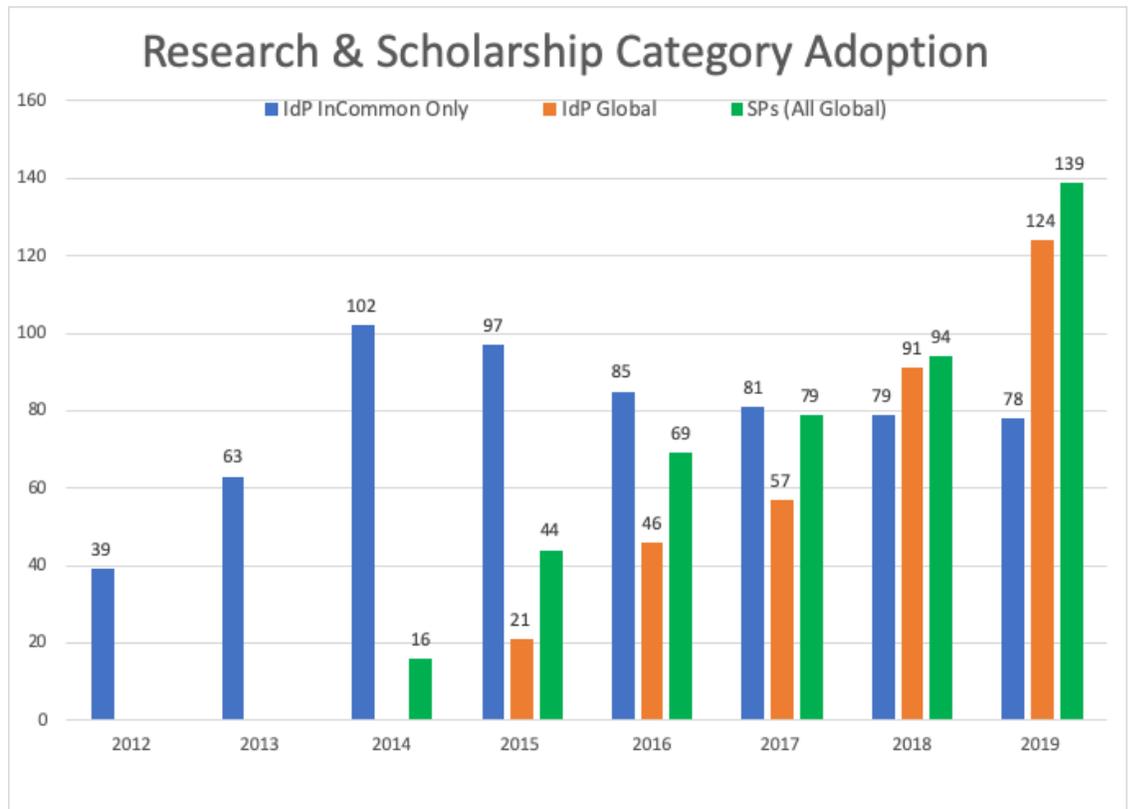


*This chart shows the percentage of InCommon Identity Providers (red) and InCommon Service Providers (blue) that indicate they support SIRTFI. This represents 107 IdPs and 478 SPs.*

### Research & Scholarship Category of Service Providers



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



*This chart demonstrates the growth in R&S, as well as a shift in how Identity Providers support the category. Initially, there was an “InCommon only” option (the blue bars), with IdPs supporting only R&S Service Providers that are InCommon participants (as opposed to supporting any global SP in the category). InCommon has worked to move IdPs to supporting all global R&S SPs (the orange bar). IdPs can no longer assert “InCommon SPs only.”*

## Making Collaboration Easier

---

### Engaging with Research Communities

InCommon continued its support of the [Federated Identity Management for Research](#) (FIM4R) effort by using the recommendations published in the FIM4R v2 paper to profoundly influence some of its activities and services, and by continuing its staff support for FIM4R's on-going efforts. FIM4R, which represents more than 20 research communities and research cyber infrastructures around the world, held its 14th meeting in conjunction with the Internet2 Technology Exchange in New Orleans with funding and staffing support provided by InCommon.

### Future of Federation

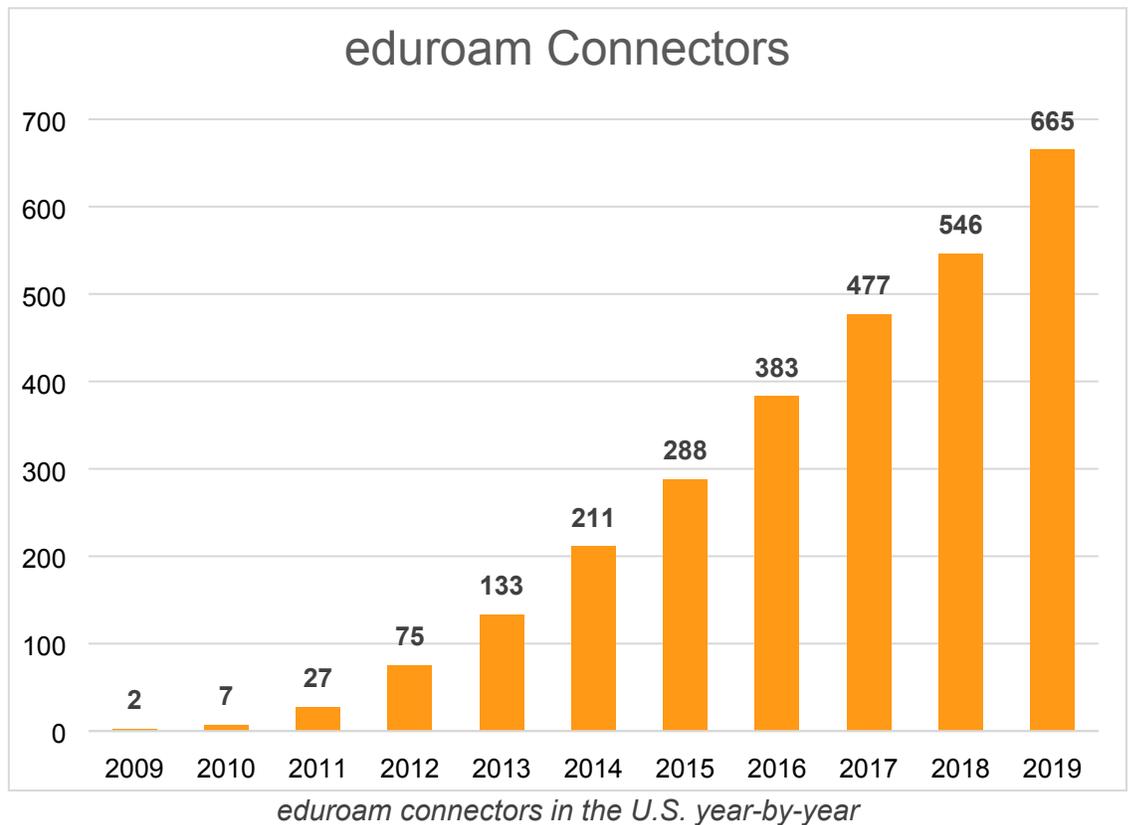
InCommon has taken a leadership role in the REFEDS [Federation 2.0 working group](#), which is doing a form of strategic planning to arrive at strategies InCommon and other R&E federations should undertake to remain valuable and viable over the next 10-15 years, and recommendations for next steps towards implementation of those strategies. Publication of the working group's report is expected sometime in the first half of 2020.

## eduroam

**UETN/InCommon K-12 partnership** - InCommon and the Utah Education and Telehealth Network (UETN) [developed a program](#) to deploy a wide-scale implementation of eduroam to select K-12 institutions in the state. Goals included developing a business model in which InCommon and regional networks develop partnerships to expand the service.

During the program, UETN successfully deployed eduroam to several K-12 school districts, as well as on bus and train lines in the state of Utah. Participants also created processes, technical documentation, and training needed for InCommon to engage additional regional networks during 2020.

**eduroam-US Advisory Committee forms** - At the end of 2019, the Internet2 Community Architecture Committee for Trust and Identity chartered an [eduroam-US Advisory Committee](#) (eAC). The eAC will help formulate strategies and practices for U.S. and global research and education roaming networks.



## InCommon Certificate Service

---

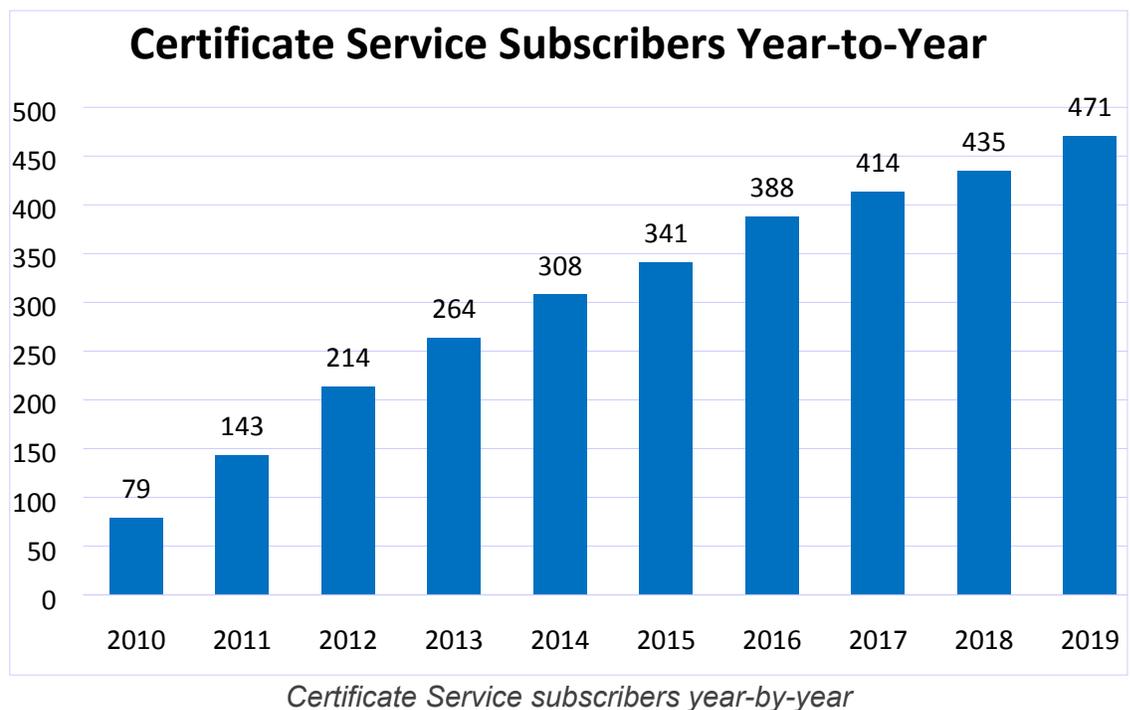
### InCommon Certificate Service

---

The [InCommon Certificate Service](#) provides unlimited certificates (SSL, EV, client, and others) for one annual fee. Key accomplishments in 2019 for the Certificate Service are listed below. The work is driven, in part, by a bi-annual survey of Certificate Service subscribers.

#### 2019 Accomplishments for the InCommon Certificate Service

- Worked with Sectigo to develop a new test page for subscribers who are integrating their SSO System with the Sectigo Certificate Manager (SCM)
- Began testing Sectigo's new ACME Service (for rollout in 2020)
- Saw continued growth of SSO integration with SCM
- Worked with Sectigo to ensure that our community has access to new training videos for using SCM
- Worked with Sectigo to add additional content to the status page
- As of December 31, 2019, we had approximately 270,000 active certificates across 471 organizations



---

## Engaging the Community

---

### Engaging the Community

---

InCommon convenes the community to develop requirements, specifications, and program activities in the form of working groups and advisory groups. During 2019, **150 individuals from 105 different organizations participated** in an InCommon working group or advisory group.

#### IAM Online Webinar Series

The monthly [IAM Online webinar series](#) marked its 10th year of operation in 2019. [Appendix B](#) includes a list of topics and speakers. IAM Online is a partnership with the EDUCAUSE Higher Education Information Security Council. Archived sessions are available on an [IAM Online YouTube channel](#), which is operated in conjunction with [GÉANT](#).

#### 2019 Internet2 Global Summit and 2019 Technology Exchange

The [2019 Internet2 Global Summit](#) (held in April) and the [2019 Internet2 Technology Exchange](#) (TechEx) (this year held in December) provide opportunities for the InCommon community to gather and to interact with other Internet2 communities. TechEx in particular is an important technical meeting for InCommon, with a significant global component and attendance.

The InCommon community combined three focused meetings into the 2019 TechEx: REFEDS, the conference for research and education identity federations worldwide; [Advance CAMP](#), the unconference meeting that explores just-in-time issues and challenges of community-wide interest or concern; and [two tracks of InCommon sessions](#) (CAMP), with campus-focused sessions comprised of community proposals. Approximately 180 identity and access management professionals attended the meeting.

#### Working Groups

Much of the work (and innovations) of InCommon takes place in working groups, chaired and populated by community members. [Appendix A](#) includes a list of the working groups and their charters, links to wiki pages, and any reports or other results. Groups active during 2019 are listed here.

## Engaging the Community

---

InCommon Working Groups	Chair	Working Group Materials
OIDC/OAuth Deployment Working Group - work completed in 2019	Nathan Dors, University of Washington	<a href="https://spaces.internet2.edu/x/jJiTBg">https://spaces.internet2.edu/x/jJiTBg</a>
Deployment Profile Working Group - work completed in 2019	Keith Wessel, University of Illinois Urbana-Champaign	<a href="https://spaces.internet2.edu/x/WolQBg">https://spaces.internet2.edu/x/WolQBg</a>
Identity Provider as a Service Working Group	Mary McKee, Duke University; EJ Monti, Duquesne University	<a href="https://spaces.at.internet2.edu/x/XoGIC">https://spaces.at.internet2.edu/x/XoGIC</a>
Banner Integration Working Group	Matthew Brookover, Colorado School of Mines	<a href="https://spaces.at.internet2.edu/x/gYY5CQ">https://spaces.at.internet2.edu/x/gYY5CQ</a>
InCommon Trusted Access Platform Software Integration Working Group	Keith Hazelton, University of Wisconsin-Madison	<a href="https://spaces.at.internet2.edu/x/SgFwBQ">https://spaces.at.internet2.edu/x/SgFwBQ</a>
Component Architects Working Group	Steve Zoppi, Internet2	<a href="https://spaces.internet2.edu/x/RAFwBQ">https://spaces.internet2.edu/x/RAFwBQ</a>

### Governance and Advisory Groups

#### Trust and Identity Division

##### Trust and Identity Program Advisory Group

*Chair: Klara Jelinkova, Rice University*

The [Trust and Identity Program Advisory Group \(PAG\)](#) provides community executive input and guidance to the Vice President for Trust and Identity and NET+ for the creation and direction of division programs and services including, but not limited to, InCommon Federation and Certificate Services, the Trusted Access Platform, training programs, and eduroam. Key topics discussed in 2019 include:

- Messaging to CIOs regarding the InCommon Trusted Access Platform vis a vis commercial offerings (where the platform fits)
- eduroam - a security review, a regional pilot in Utah, and formation of a community advisory group
- FIM4R (Federated Identity Management for Research), a report from an international research cyberinfrastructure community with recommendations for federations and InCommon's response
- InCommon fee change and its role in ensuring the continued development and sustainability of the InCommon Trusted Access Platform software and services
- BaseCAMP, developed for those new to identity management and/or federation, as part of a broader effort to "expand the InCommon tent."

##### Community Architecture Committee for Trust and Identity (CACTI)

*Chair: Chris Phillips, CANARIE*

CACTI ([Community Architecture Committee for Trust and Identity](#)) 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.

During 2019, CACTI completed the hand-off of the directory schemas that had been conceived of and governed by the Middleware Architecture Committee for Education (MACE) Directories working group nearly 20 years ago, to the

## Engaging the Community

---

international REFEDS organization. This change was critical for the ongoing maintenance of these core standards in a globally connected identity ecosystem.

CACTI also devoted significant effort to reading, understanding, and interpreting the requirements of the [Federated Identity Management for Research \(FIM4R\) version 2 paper](#) produced by the international research cyberinfrastructure community. CACTI mapped the recommendations of this group into areas of focus within the InCommon community. From there, it recommended changes in programs and governance, which has increased research involvement in governance groups, and additional attention paid to the needs of research within the InCommon Trusted Access Platform and InCommon Academy.

Additionally, CACTI reflected on the challenges of making InCommon services and software easier to use by smaller institutions, and this also resulted in input to the Trusted Access Platform and Academy programs.

### **InCommon Steering Committee**

*Chair: Ted Hanss, Yale 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. Policies and practices approved by the Steering Committee are available on the [policies](#) page of the InCommon website. **Key topics discussed** in 2019 include:

- InCommon fee change to ensure sustainability of the federation and of the InCommon Trusted Access Platform software and services
- Making the business case for InCommon to those in various roles on campus and in organizations
- Continued support for research collaboration
- Expanding training and engagement opportunities
- Support for ensuring all federation participants meet Baseline Expectations

## Engaging the Community

---

### **InCommon Community Trust and Assurance Board**

*Chair: Mary Catherine Martinez, Innosoft*

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 topics discussed in 2019

- Led the continued effort to bring all InCommon Participants to adherence with InCommon Baseline Expectations (in collaboration with InCommon staff)
- Developed theme and requirements for Baseline Expectations 2.0 to continue to further trust and interoperability in federation
- Added international members to better coordinate and widen the deployment of Baseline Expectations to the global research and education identity federation community

### **InCommon Technical Advisory Committee**

*Chair: Janemarie Duh, Lafayette College*

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

Key topics discussed in 2019

- Chartered the IdP-as-a-Service Working Group to develop requirements and implementation strategies for those looking for federation-ready cloud-based solutions
- Increased collaboration with other committees (CTAB, CACTI) and convened a "badging" subgroup to develop ways to incentivize best behaviors among participants
- Evaluated the potential impact on the InCommon Federation of emerging technology (e.g., WebAuthn, RA21/Seamless Access)

## Appendix A: 2019 Active Working Groups

---

### Appendix A: 2019 Active Working Groups

---

#### **InCommon OIDC/OAuth Deployment Working Group**

*Chartered by: InCommon Technical Advisory Committee*

*Chair: Nathan Dors, University of Washington*

*Wiki: <https://spaces.internet2.edu/x/jJiTBg>*

This working group formed to build on the work of a previous OIDC/OAuth deployment working group, which focused on determine campus use of the protocol. This phase two was intended to develop use cases and best practices. The working group discovered that there was insufficient subject matter expertise in the community. Further, it found that there are actually few campuses actively using the protocol. It completed its work by recommending revisiting the topic in a year or two.

#### **InCommon Deployment Profile Working Group**

*Chartered by: InCommon Technical Advisory Committee*

*Chair: Keith Wessel, University of Illinois, Urbana-Champaign*

*Wiki: <https://spaces.internet2.edu/x/WoIQBg>*

The work of the Deployment Profile working group, chartered in 2018, was tasked with updating the legacy SAML v2 Interoperability Profile (SAML2int), the first major rewrite of this material. This deployment profile specifies how software should be configured given a specific set of deployment goals and defines the requirements for SAML software capable of operating in multilateral federations like InCommon. The working group finished its work, [created a final report](#), and sent the results to Kantara for ratification and curation.

#### **Identity Provider as a Service Working Group**

*Chairs: Mary McKee, Duke University; EJ Monte, Duquesne University*

*Wiki: <https://spaces.at.internet2.edu/x/fIC-C>*

This working group formed to address the problem of campuses that may not have the staff or skills to operate a federation-capable identity provider. One solution is a cloud IdP-as-a-Service offering. The working group is identifying the characteristics an IdPaaS offering would need to ensure good federation participation. The working group conducted a survey to determine interest in (and identify desired features for) an IdPaaS option and has started developing a list of features and characteristics that a federation-friendly solution would possess.

## Appendix A: 2019 Active Working Groups

---

### **InCommon Trusted Access Platform Software Integration Working Group**

*Chair: Keith Hazelton, Independent Consultant*

*Wiki: <https://spaces.at.internet2.edu/x/SgFwBQ>*

- Developed the [InCommon Trusted Access Platform Library](#)
- Worked with Evolveum to develop integration patterns between Grouper and midPoint using messaging
- Worked with the InCommon Academy to identify and develop the most common Identity and Access Management use cases for which solutions are needed by the Community
- Developed packaging for training and demonstration IAM reference implementations using the Trusted Access Platform
- Spun off a Banner Integration Working Group to continue work began in the TIER Collaboration Success Program to develop integration patterns between Banner and midPoint *Wiki: <https://spaces.at.internet2.edu/x/gYY5CQ>*
- Continued collaboration with the Big Ten Academic Alliance on provisioning and de-provisioning *Wiki: <https://spaces.at.internet2.edu/x/DANhBq>*

### **Component Architects Working Group**

*Chair: Steve Zoppi, Internet2*

*Wiki: <https://spaces.internet2.edu/x/RAFwBQ>*

- Worked to support advancement and better consolidation of documentation, training, and common support channels for the InCommon Trusted Access Platform
- Commissioned and monitored work on developing the Grouper Deployment Guide V2 as a living wiki space for continued evolution based on community input
- Advised and progressed Shibboleth Identity Provider User Interface development work with Unicon.
- Supported the launch of the Collaboration Success Program with volunteer SMEs
- Supported the transition of TIER to the InCommon Trusted Access Platform and the TIER Working Groups to the InCommon Software Integration Working Group
- Continue collaboration and guidance for the project leads and software partners on providing value to community needs in the IAM space.

## Appendix B: IAM Online Topics

---

### Appendix B: IAM Online Topics

---

[IAM Online](#) is a monthly webinar series on Identity and Access Management (IAM) topics, sponsored by InCommon, Internet2, and the EDUCAUSE Higher Education Information Security Council. Links to slides and recordings are on the [IAM Online web page](#). An archive of IAM Online presentations is also available on the [IAM Online YouTube](#) channel.

**New InCommon Metadata Service, Per-Entity Metadata Deployment** (January 2019) *Presenters: Nick Roy, David Shafer, Albert Wu, Shannon Roddy (all Internet2)*

**CILogon and eduTEAMS: Collaboration and virtual organizations made easy** (March 2019) *Moderator: Tom Barton, University of Chicago and Internet2. Presenters: Jim Basney, National Center for Supercomputing Applications (University of Illinois), Christos Kanellopoulos, GÉANT*

**Shibboleth development roadmap and consortium update** (April 2019) *Presenters: Scott Cantor (Shibboleth Project and The Ohio State University); Justin Knight (JISC)*

**We're moving your metadata, not your cheese – a webinar on the release of the production candidate service** (July 2019) *Presenters: Nick Roy (Internet2); Albert Wu (Internet2)*

**Real-world experience moving IdM to the cloud at Illinois** (September 2019) *Presenters: Erik Coleman (University of Illinois at Urbana-Champaign); Keith Wessel (University of Illinois at Urbana-Champaign)*

**Containerization: Streamlining operations and reducing downtime** (October 2019) *Moderator: Paul Caskey (Internet2). Presenters: Paul Riddle and Chris Sutherin (both University of Maryland Baltimore County)*

**Going passwordless at Stanford** (November 2019) *Moderator: Tom Barton (University of Chicago and Internet2). Presenter: Michael Duff (Stanford University)*

**Baseline Expectations v2: Continuing to raise the bar** (December 2019) *Presenters: David Bantz (University of Alaska); Albert Wu (Internet2)*

## Appendix C - Glossary of Terms and Acronyms

---

### Appendix C - Glossary of Terms and Acronyms

---

**Baseline Expectations - Baseline Expectations for Trust in Federation** - A set of common expectations that all Participants meet, intended to make collaboration more predictable and improve the user experience. See [www.incommon.org/federation/baseline/](http://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 Partners** - A diverse group of higher education institutions committed to adopting and deploying the TIER software components and helping to accelerate adoption for the rest of the trust and identity community. See <https://spaces.internet2.edu/x/oQrABg>. Transitioning to Collaboration Success Partners in 2019.

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

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

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

**eduGAIN** - An interconnection of identity federations around the world, simplifying access to content, services and resources for the global research and education community. [eduGAIN](#) enables the trustworthy exchange of information related to identity, authentication and authorization.

**eduroam** - A global wireless network access service developed for the international research and education community. eduroam allows students,

## Appendix C - Glossary of Terms and Acronyms

---

researchers, faculty, and staff secure seamless wireless access at all participating institutions. See [www.incommon.org/eduroam](http://www.incommon.org/eduroam).

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

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

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

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

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

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

**R&S - Research & Scholarship Category of Service Providers** - The Research and Scholarship Entity Category (R&S) is an international specification that provides a simple and scalable way for Identity Providers to release a small set of attributes, or information, to an entire group of Service Providers serving the Research and Scholarship Community. Service Providers are vetted prior to being added to the category. See [refeds.org/research-and-scholarship](http://refeds.org/research-and-scholarship).

## Appendix C - Glossary of Terms and Acronyms

---

**REFEDS - Research and Education FEDerations** - REFEDS is a voice that articulates the mutual needs of research and education identity federations worldwide. See [refeds.org](http://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](http://refeds.org/sirtfi).

**SP - Sponsored Partner** - A business partner that provides resources to a higher education institution and is sponsored for participation in InCommon by a participating higher education institution.

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

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

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

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