



Enabling Communities

Maarten Kremers, SURF

GN5-1 Workpackage Leader Trust & Identity

Atlanta, Georgia, USA

10th May 2023

Federated Identity Management

*Federated identity management (FIM) is the set of policies and technologies that enables one party to rely on the **authentication** performed by another trusted party, and the secure transfer of **identity information** for **authorization** purposes.*

Authentication (AuthN)

- Authentication is the **act of confirming the truth** of an attribute of a single piece of data or entity (the user of an application, for instance).
- Example (in the real world): authenticating the Mona Lisa.



- In the digital world we tend to simplify the confirmation by means of a login
 - **Username : Identification**
 - **Password : Authentication**



Authorization (AuthZ)

- Authorization is the function of **specifying access rights** to resources related to information security and computer security in general and to access control in particular.
- Example: going to a concert.



Managing AuthN and AuthZ

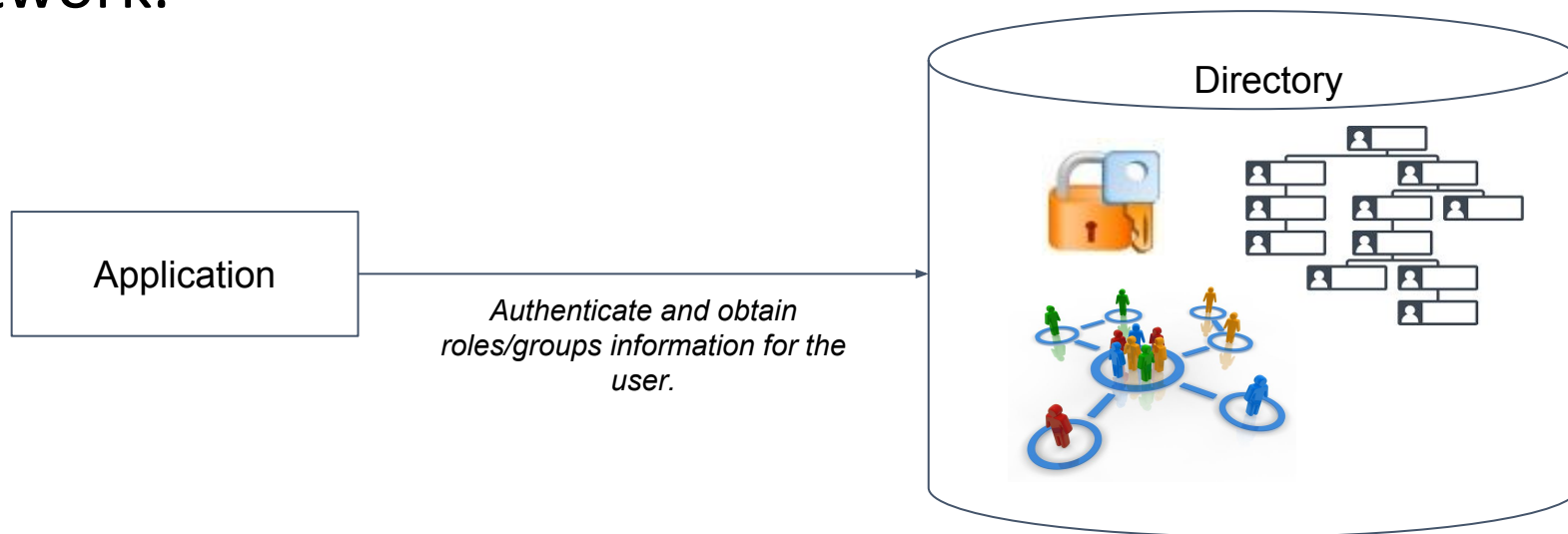
As we have seen, an application to deal with authentication and authorization has to manage the following information:

1. **usernames** and associated **passwords**, *to identify users and verify (authenticate) they are who they pretend to be;*
2. institutional **roles**, *to describe the roles within the group or organization (used for Role Based Access Control);*
3. user **groups**, *to pool together users that have the same role in the organization (groups are associated to roles);*
4. **access policies**, *rules in the form of (role name -> access right) to describe which operation each role is entitled to perform and which not inside the application.*

Externalizing authentication

For simplicity, and not to duplicate information, usually a **Directory** is used to collect username, password, roles and groups for the whole organization.

Directory services play an important role by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.



Federated authentication

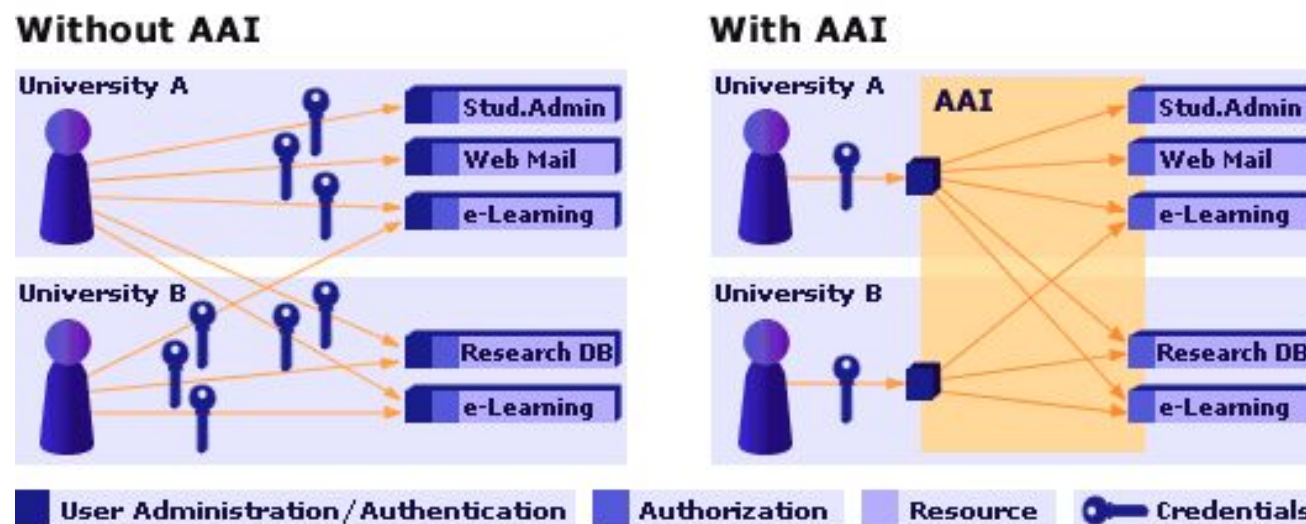
A directory is widespread and quite always used to maintain authentication information of an organization. Often to facilitate collaboration is useful to enable access to service to **users that belong to different organisations** compared to the one that operate the service. This can be possible by either asking people to create an account with that services or by enabling federated access.

To permit these users to access the application, we use a **federated identity**:

- users can authenticate on different **identity provider (IdP)** services on the network;
- the different IdPs use similar protocols and user definitions so that applications can deal with users belonging to different organization in a similar manner.

Federated authentication

The objective of the AAI is, in a nutshell, to **simplify inter-organizational access** to resources. With a single login, for instance, a researcher can access applications at multiple organizations (universities or research institutions).



Benefits of federated authentication

- **A user registers only once** - namely with the home organization to which the user is affiliated. This Home Organization is responsible for maintaining the user related information and provides the user with the credentials. Home Organizations can be institutions like universities, libraries, university hospitals etc.
- **Authentication** is always **carried out by the user's Home Organization**, which can also provide additional information about the user to the Resource upon Resource's request and user's consent.
- **All AAI-enabled Resources are available to a user** with a single set of credentials.
- **Security** - no need for Resource Providers to maintain their own set of credentials as authentication is outsourced (thus preventing password leakage)
- An **access control decision** (authorization) is made by the **Resource** based on the retrieved information about the user.
- **Privacy Preserving** – only the attributes required by a Resource are sent.

Attributes

Authentication

Authorization

The *R&S attribute bundle* consists (abstractly) of the following required data elements:

- *shared user identifier*
- *person name*
- *email address*

and one optional data element:

- *affiliation*

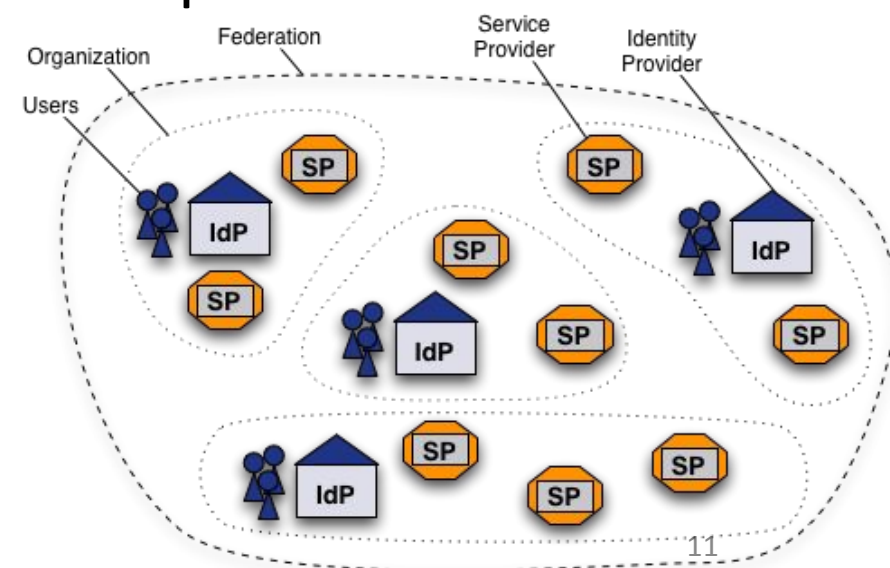
Example of (abstract) bundle of attributes – the R&S attribute bundle

What is a Federation

A federation is a **collection of organizations** that agree to interoperate under a certain rule set. Federations will usually define trusted roots, authorities and attributes, along with distribution of metadata representing this information.

In general each organization participating in a federation operates:

- one **Identity Provider (IdP)** for their users, and
- any number of **Service Providers (SP)** or applications.



Federations in the R&E world

A **federation operator** is an organisation that operates an identity federation.

Operation typically includes at minimum:

- Collecting, processing and republishing **metadata** (*metadata permits to create a trust between IdPs securely*)
- Common **policies** and **agreements** that federation participants adhere to
- Guidelines and **best practices** to operate services in the federation
- Helpdesk to assist users and debugging issues

Most academic federations are operated by the **national research and education network** (NREN). These organisations typically also operate the network connecting the universities and research organisations within a country.

Trust

The interfederation

NRENs usually operates federation within a country. To scale to a global level, R&E introduced the concept of **interfederation**.



Interfederation takes place if a **user from one federation accesses a service which is registered in another federation**.

eduGAIN is the most known and largest academic Interfederation service to exchange trusted identity information across boundaries of (national) identity federations.



Trustmarks

To ensure interoperability and to signal policies, optional trustmarks are in place

- **Code of Conduct (CoCo)**

- Signals compliance of an SP with the GEANT Code of Conduct

- **Research & Scholarship (R&S)**

- SP requests to get a defined set of information (id, name, mail, affiliation)



- **REFEDS Assurance Framework (RAF)**

- Signals 4 components on the identity of user

- **Single factor AuthN (SFA) and Multi factor Auth (MFA)**

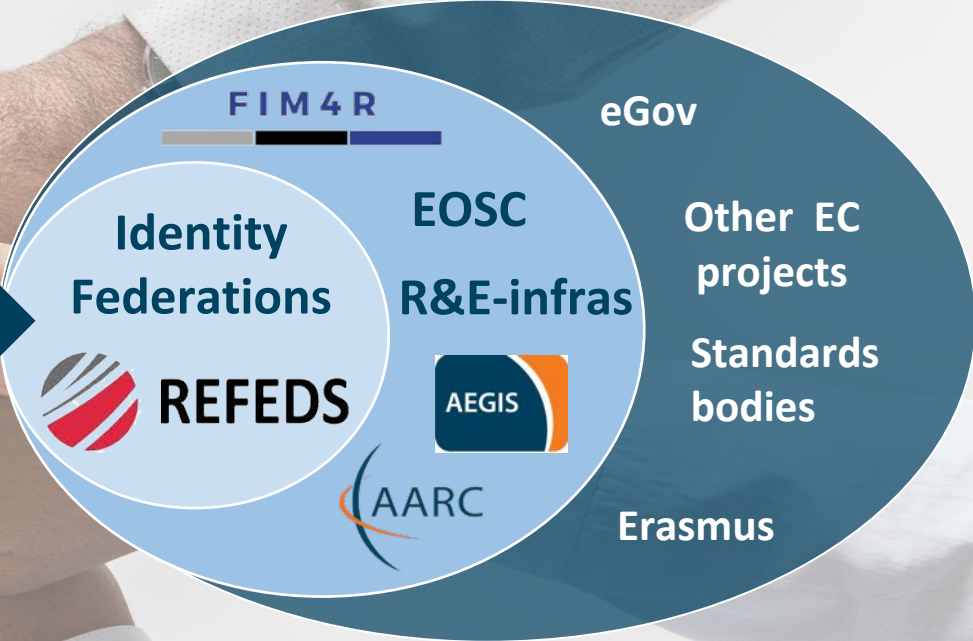
GN5-1 T&I Team and Key Collaborations

WP 5

Marina Adomeit SUNET
Maarten Kremers SURF



T1		Paul Dekkers SURF	
T2		Davide Vagheti GARR	
T3	Core AAI Platform	Christos Kanellopoulos GÉANT	
T4		Michelle Williams GÉANT	
T5		Niels van Dijk SURF Michael Schmidt LRZ	
T6	Enabling Communities	Maarten Kremers SURF	
T7	Distributed Identities	Christoph Graph, SWITCH	



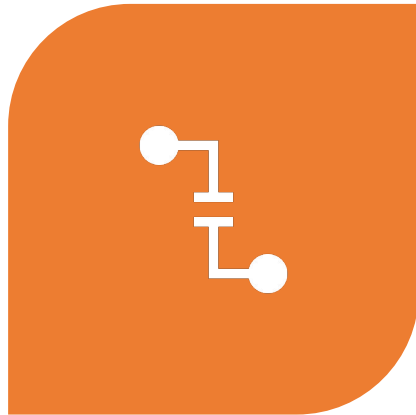
Enabling Communities

T&I eScience Global Engagement

The '**eScience Global Engagement**' of EnCo in the GEANT project is there to support those developments in **the policy and best practice areas** that would benefit **the community at large**, and do that by means of **supporting** the work in the **existing forums** such as WISE, FIM4R, IGTF, REFEDS, AARC-community, and the research and e-Infra communities directly



T&I Enabling Communities



INTEROPERABILITY



TRUST

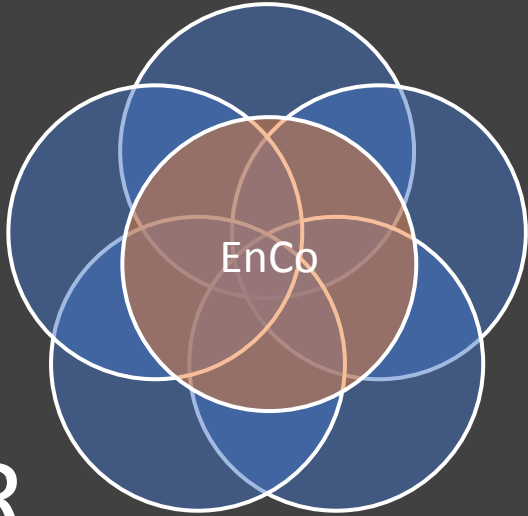


SECURITY

REFEDS



IGTF



AARC



FIM4R

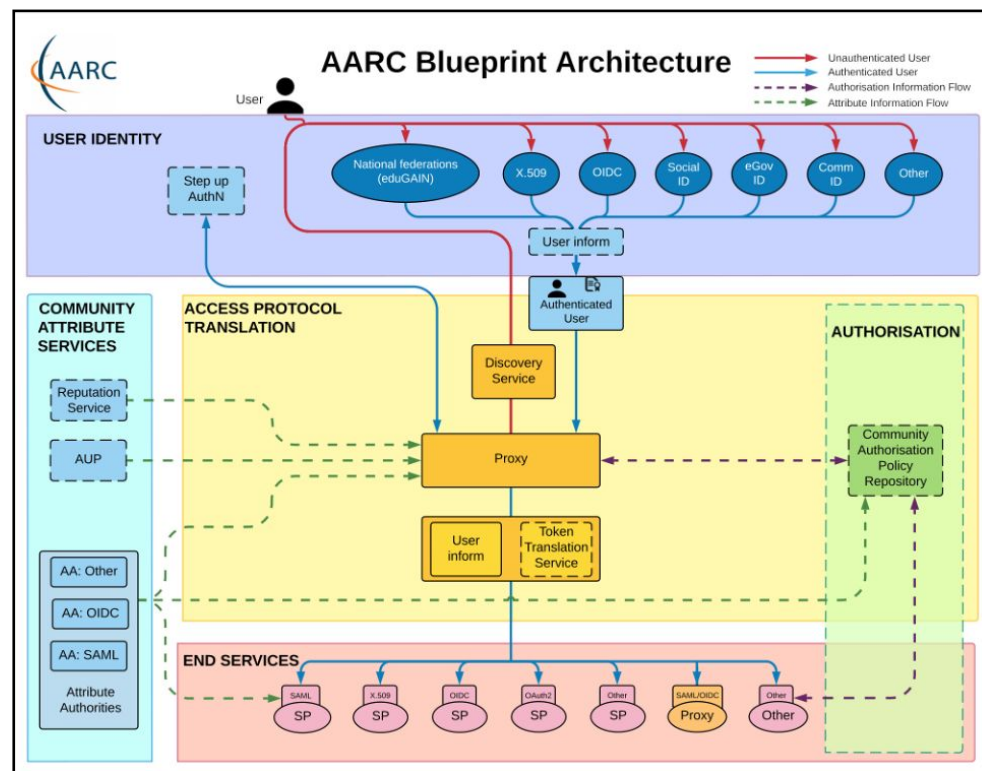
WISE





Interoperability, sustainability, integration and compatibility: **Authentication and Authorisation for Research and Collaboration (AARC)** – a set of turn-key AAI solutions bringing research collaborations closer together.

T&I Enabling Communities



The AARC Blueprint Architecture (BPA)

is a set of software building blocks that can be used to implement federated access management solutions for international research collaborations.

T&I Enabling Communities



Harmonising rules for a common infrastructure: The **Policy Development Kit (PDK)**
Harmonising the rules that organisations apply to identity management is essential for achieving an integrated AAI framework.

T&I Enabling Communities

Not sure how to begin with the AARC Blueprint Architecture? There are plenty of [guidelines](#) available but it can be a minefield at first. Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

Getting Started:

- How should I design my infrastructure? What is the AARC Blueprint Architecture? [AARC-G045](#)
- How should I approach performing a Data Protection Impact Assessment? [AARC-G042](#)
- How should my infrastructure support Federated Security Incident Response? [AARC-I051](#)

Access Protocol Translation:

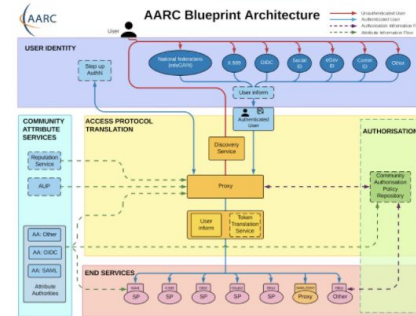
- Which best practices should I follow for my Token Translation Services? [AARC-G004](#)
- How should I translate from Identity Federation information to X.509 certificates? [AARC-G010](#)

Proxies:

- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? [AARC-G015](#)
- How should I express assurance information for users when interacting with another proxy? [AARC-G021](#)

Community Attribute Services:

- How should attributes from multiple sources be aggregated? [AARC-G003](#)
- How should I express the home institute of a user? [AARC-G025](#)
- What are the best practices for running my Attribute Authorities securely? [AARC-G048](#)
- Which Acceptable Use Policy should I use to facilitate interoperability? [AARC-I044](#)



End Services:

- My service needs to act on behalf of the user - how should I handle credential delegation and impersonation? [AARC-G005](#)
- My services are not web based, how can I use identities from the proxy? [AARC-G007](#)
- How should Services hint which IdP they would like users to use? [AARC-G049](#)
- Which Security practices should I follow? [AARC-G014](#)

User Identity:

- How should I integrate Social Media Identity Providers? [AARC-G008](#)
- How should users link accounts, and how does that affect Assurance? [AARC-G009](#)
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? [AARC-G029](#)

Assurance:

- How should assurance information of external identities be calculated? [AARC-G031](#)
- What can I say about assurance of identities from social media accounts? [AARC-G041](#)
- How is assurance impacted by account linking? [AARC-G009](#)
- How should assurance information be shared with other infrastructures? [AARC-G021](#)
- Which Assurance Profiles should I use, there are so many! [AARC-I050](#)

Authorisation:

- How should I manage authorisation information from multiple sources? [AARC-G006](#)
- How should group and role information be expressed to facilitate interoperability? [AARC-G002](#)
- How should resource capabilities be expressed? [AARC-G027](#)

What next? Are you looking for a kick start with your policies? Take a look at the [Policy Development Toolkit](#) which provides a set of templates.

Certain guidelines are being adopted by the AEGIS community to support interoperability between infrastructures - consider prioritising [these best practices](#).

Linking Guidelines, BPA and PDK

<https://aarc-project.eu/architecture/>

<https://edu.nl/h3dm4>



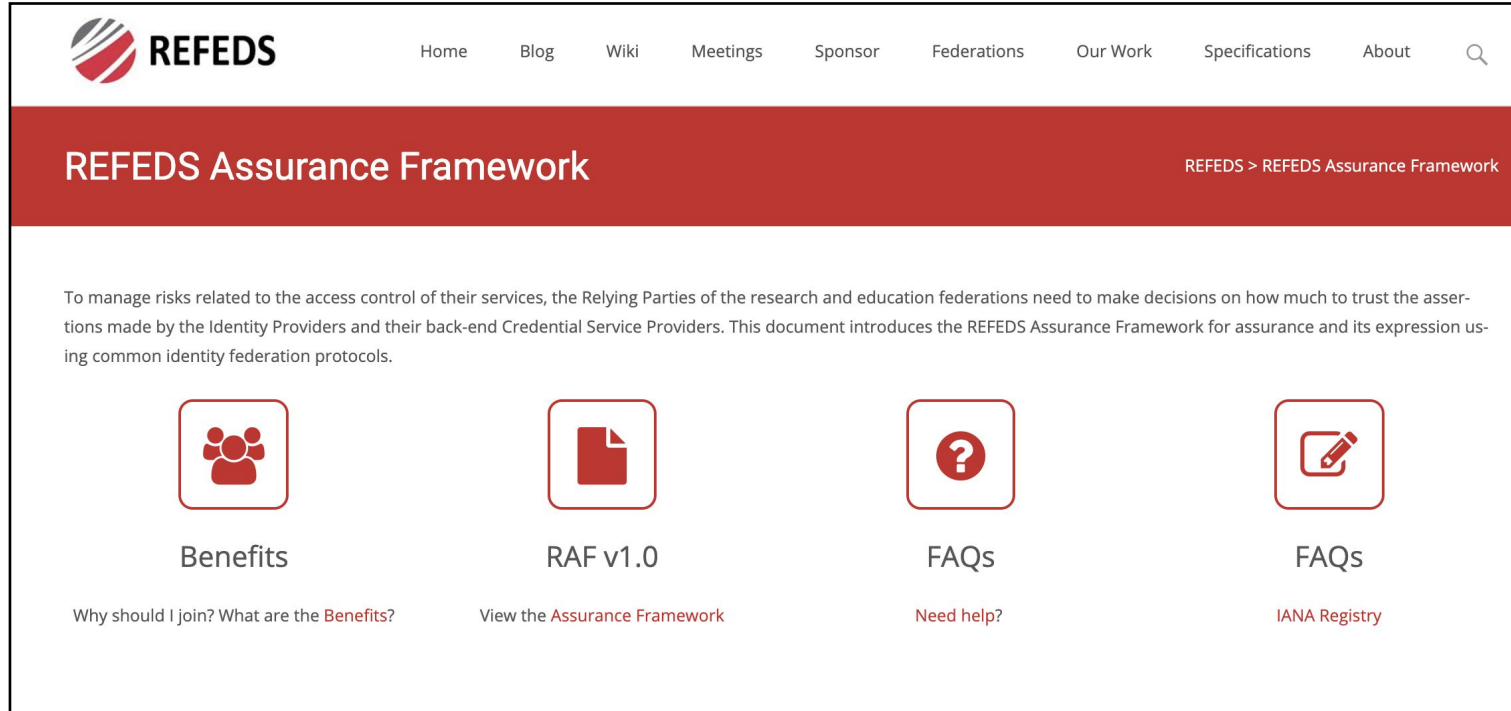
The **AARC Engagement Group for Infrastructures (AEGIS)** brings together global representatives from AAI operators in **research infrastructures and e-infrastructures**, which are **implementing authentication and authorisation** services that support **federated access**, to discuss **adoption of policy and technical best practices** that facilitate interoperability across e-infrastructures and research infrastructures.





REFEDS (the Research and Education FEDerations group) is to be the voice that articulates the mutual needs of research and education identity federations worldwide.

T&I Enabling Communities



The screenshot shows the REFEDS Assurance Framework page. At the top, there is a navigation menu with links for Home, Blog, Wiki, Meetings, Sponsor, Federations, Our Work, Specifications, and About. The main heading is "REFEDS Assurance Framework" with a breadcrumb trail "REFEDS > REFEDS Assurance Framework". Below the heading, there is a paragraph explaining the framework's purpose: "To manage risks related to the access control of their services, the Relying Parties of the research and education federations need to make decisions on how much to trust the assertions made by the Identity Providers and their back-end Credential Service Providers. This document introduces the REFEDS Assurance Framework for assurance and its expression using common identity federation protocols." Below this text are four icons in red boxes, each with a corresponding title and link: "Benefits" (Why should I join? What are the Benefits?), "RAF v1.0" (View the Assurance Framework), "FAQs" (Need help?), and "FAQs" (IANA Registry).

REFEDS Assurance Profile (v1.0)

- Consisting of **three individual specifications**:
 - [REFEDS Assurance Framework](#) (RAF), ver 1.0, published 2018
 - [REFEDS Single Factor Authentication Profile](#) (SFA), ver 1.0, 2018
 - [REFEDS Multi Factor Authentication Profile](#) (MFA), ver 1.0, 2017
- Component-based approach
- Two identity assurance profiles: Espresso (high assurance) and Cappuccino (moderate assurance)

v2.0 in progress





PROCEEDINGS
OF SCIENCE

Making Identity Assurance and Authentication Strength Work for Federated Infrastructures

Jule Anna Ziegler,^{a,*} Uros Stevanovic,^b David Groep,^c Ian Neilson,^d David P. Kelsey^d
and Maarten Kremers^e

^aLeibniz Supercomputing Centre, Garching near Munich, Germany

^bKarlsruhe Institute of Technology (KIT), Karlsruhe, Germany

^cNikhef, Amsterdam, the Netherlands

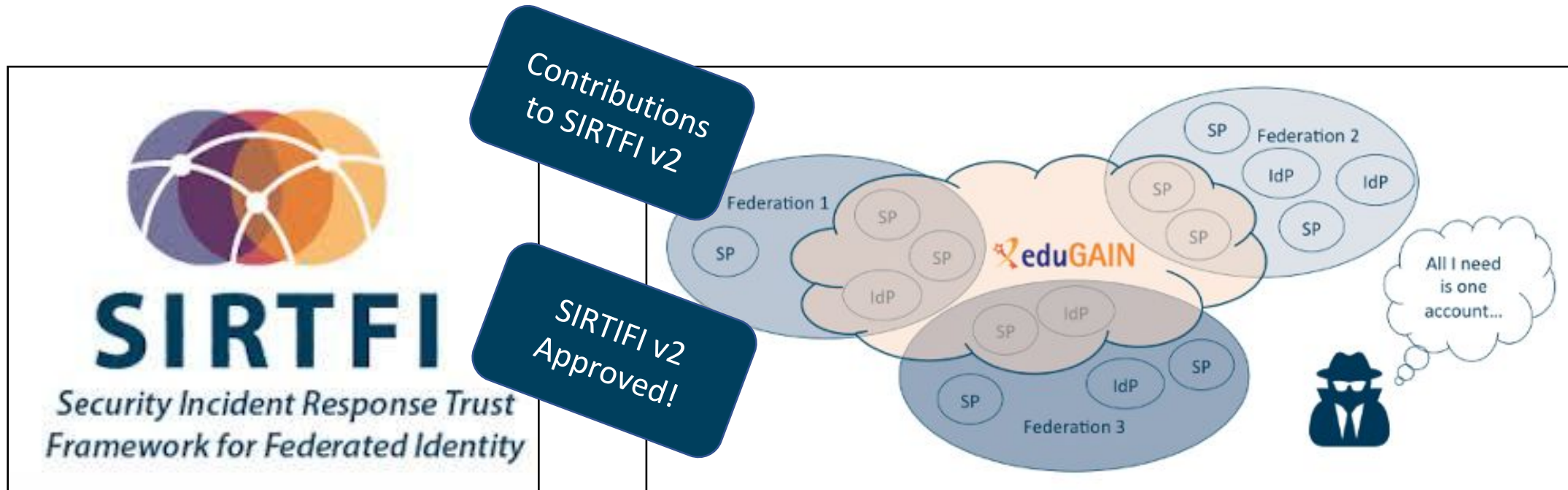
^dUKRI STFC Rutherford Appleton Laboratory, Didcot, United Kingdom

^eSURF, Utrecht, the Netherlands

Full paper
published

[https://doi.org/10.22323/
1.378.0029](https://doi.org/10.22323/1.378.0029)

T&I Enabling Communities



Source and more information:
https://refeds.org/wp-content/uploads/2016/02/Why_Sirtfi.pdf

eduGAIN Security Incident Response Handbook

Preface	1
Chapter 1. Understanding Your Role and Responsibilities	2
Introduction	2
Roles	2
Scope	3
Responsibilities	3
Federation Participants	4
Federation Operators	4
eduGAIN Security Team	4
Chapter 2. Security Incident Response Procedures	5
Federation Participants	5
Federation Operators	6
eduGAIN Security Team	7

Contributions to the
eduGAIN security
incident Handbook



Preface



As with products of any REFEDS Working Group, in this instance the SIRTFI Working Group, this document is a community-developed Best Practice Recommendation. However, as with the SIRTFI Trust Framework itself, these Best Practice Recommendations are most effective when all parties it addresses agree to follow it. Organisations such as Federation Operators or eduGAIN may decide to incorporate adoption of these Best Practice Recommendations into their own policies, as many have done with the SIRTFI Trust Framework.

This document is based on previous work conducted in the AARC2 project¹.





The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and e-Research, identity providers, and other qualified relying parties.



Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

Publication Date: 2022-02-24

Authors: Members of the IGTF and the AARC Community; David Groep; Ian Collier, Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Sallé; Uros Stevanovic

With feedback from: Marina Adomeit; Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes Reetz

AARC Document Code: **AARC-G071**

AA Operations Security
Guideline 2022 (AARC-G071)

<https://www.eugridpma.org/guidelines/aaops/>





The Wise Information Security for Collaborating e-Infrastructures (WISE) community enhances best practice in information security for IT infrastructures for research.

SCI (Security for Collaboration among Infrastructures) Workgroup focusses on best practices, trust and policy standards for collaboration with the aim of managing cross-infrastructure security risks

SCI Trust Framework

- Enable interoperation of collaborating Infrastructures in managing cross-infrastructure operational security risks.
- Builds trust between Infrastructures by adopting policy standards for collaboration especially in cases where identical security policy documents cannot be shared.



T&I Enabling Communities

SCI

Security for Collaborating Infrastructures Trust Framework

Introduction

Research and e-Infrastructures recognise that controlling information security is crucial for providing continuous and trustworthy services for the communities. The Security for Collaborating Infrastructures (SCI) working group is a collaborative activity within the Wise Information Security for e-Infrastructures (WISE) trust community. The aim of the SCI trust framework is to enable interoperation of collaborating Infrastructures in managing cross-infrastructure operational security risks. It also builds trust between Infrastructures by adopting policy standards for collaboration especially in cases where identical security policy documents cannot be shared. Governing principles of the SCI framework are incident containment, ascertaining the causes of incidents, identifying affected parties, addressing data protection and risk management and understanding measures required to prevent an incident from reoccurring. The original **SCI version 1** Framework was produced in 2013.

The SCI Working Group has produced a second version of the framework, to reflect changes in technology, culture and to improve its relevance to a broad range of infrastructures.

[Access the SCI version 2 Framework here](#)

	A	B	C	D	E	F	G
1	Infrastructure Name:	<insert name>					
2	Prepared By:	<insert name>					
3	Reviewed By:	<insert name>					
4							
5	Operational Security [OS]	Maturity			Evidence		
6		Value	Σ				(Document Name and/or URL)
7							
8	OS1 - Security Person/Team						
9	OS2 - Risk Management Process						
10	OS3 - Security Plan (architecture, policies, controls)			2.0			
11	OS3.1 - Authentication		3				
12	OS3.2 - Dynamic Response		1				
13	OS3.3 - Access Control						
14	OS3.4 - Physical and Network Security						
15	OS3.5 - Risk Mitigation						
16	OS3.6 - Confidentiality						
17	OS3.7 - Integrity and Availability	Q	1	1.0			
18	OS3.8 - Disaster Recovery						
19	OS3.9 - Compliance Mechanisms						
20	OS4 - Security Patching		1	1.0			
21	OS4.1 - Patching Process						
22	OS4.2 - Patching Records and Communication						
23	OS5 - Vulnerability Mgmt		1	0.7			
24	OS5.1 - Vulnerability Process						

Self Assessment Tool

Guidance Doc





Top Level Infrastructure Policy Template

Questions to ask yourself when defining the policy:

- Who are the actors in your Infrastructure environment?
- How will you tie additional policies together for the infrastructure?
- Which bodies should approve policy wording?

This policy is effective from <insert date>.

INTRODUCTION AND DEFINITIONS

To fulfil its mission, it is necessary for the Infrastructure to protect its assets. This document presents the *policy* regulating those activities of *participants* related to the security of the Infrastructure.

Definitions

Infrastructure All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support *services*.

Service An *infrastructure* component fulfilling a need of the *users*, such as computing, storage, networking or software systems.

Revision PDK
in progress
based on
feedback and
experience



T&I Enabling Communities

WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructure for the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have implicit or explicit expectations on their remit, responsiveness, and level of confidentiality. It is a well recognised fact that data that is not

Contributions
by EnCo



Dashboard / ... / SCCC-JWG

Communications Challenge planning

Created by David Groep, last modified by Maarten Kremers on Jan 22, 2020

Body	Last challenge	Campaign name	Next challenge	Campaign name	Status
IGTF	October 2019			IGTF-RATCC4-2019	Completed
EGI	March 2019	SSC 19.03 (8)			(Completed
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction Test	Repeats three times a year

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a human. It need not be a detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also be done by email. A contact address does not bounce, to testing if the organisation contacted can do system memory forensic analysis and engage effectively.

- ability to receive – mail does not bounce or phone rings
- automated answering – ticket system receipt or answering machine
- human responding – a human (helpdesk operative) answers trivially (e.g. name)
- human familiar with subject-matter responding – responsible person responds
- service analysis capability - a responsible person or team can investigate and resolve common incidents reported to the contact address

See also <https://www.eugridpma.org/agenda/47/contribution/6/material/slides/0.pptx> for some background.

Please **do not post sensitive data** to this Wiki - it is publicly viewable for now.

FIM4R

FIM4R (Federated Identity Management for Research) is a collection of research communities and infrastructures with a shared interest in enabling Federated Identity Management for their research cyber infrastructures. In order to achieve this, FIM4R develops requirements bearing on technical architecture, federated identity management, and operational policies needed to achieve a harmonious integration between research cyber infrastructures and R&E Federations.

T&I Enabling Communities

FIM4R



Support by EnCo



T&I Enabling Communities



Workshop #16 @ Denver,
Dec 2022

Workshop #17 @ CERN,
Feb 2023



FIM4R



Engage!

- <https://fim4r.org>
- <https://refeds.org>
- <https://wise-community.org>
- <https://www.igtfn.net>
- <https://aarc-community.org>

- Contact us: policy@aarc-community.org



FIM 4 R





Thank You

INTERNET2
2023
COMMUNITY
exchange

May 8-11, 2023 Atlanta, GA



INTERNET
2

Enabling Trust for Communities

Part II – an InCommon Update

Albert Wu, InCommon Federation Manager, Internet2

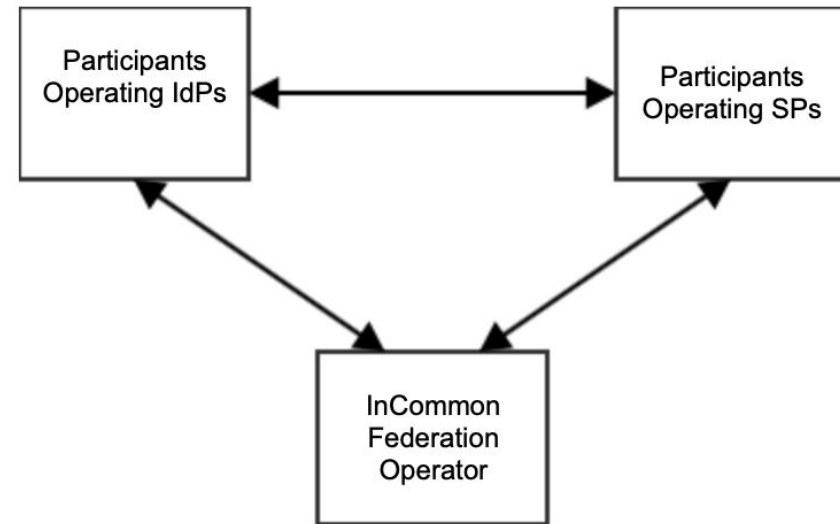
The InCommon Federation creates trust

The InCommon Federation creates multilateral trust among all federation Participants to exchange identity information in a secure manner.

Adherence to interoperability profiles scale that trust to thousands of participating organizations with millions of users.

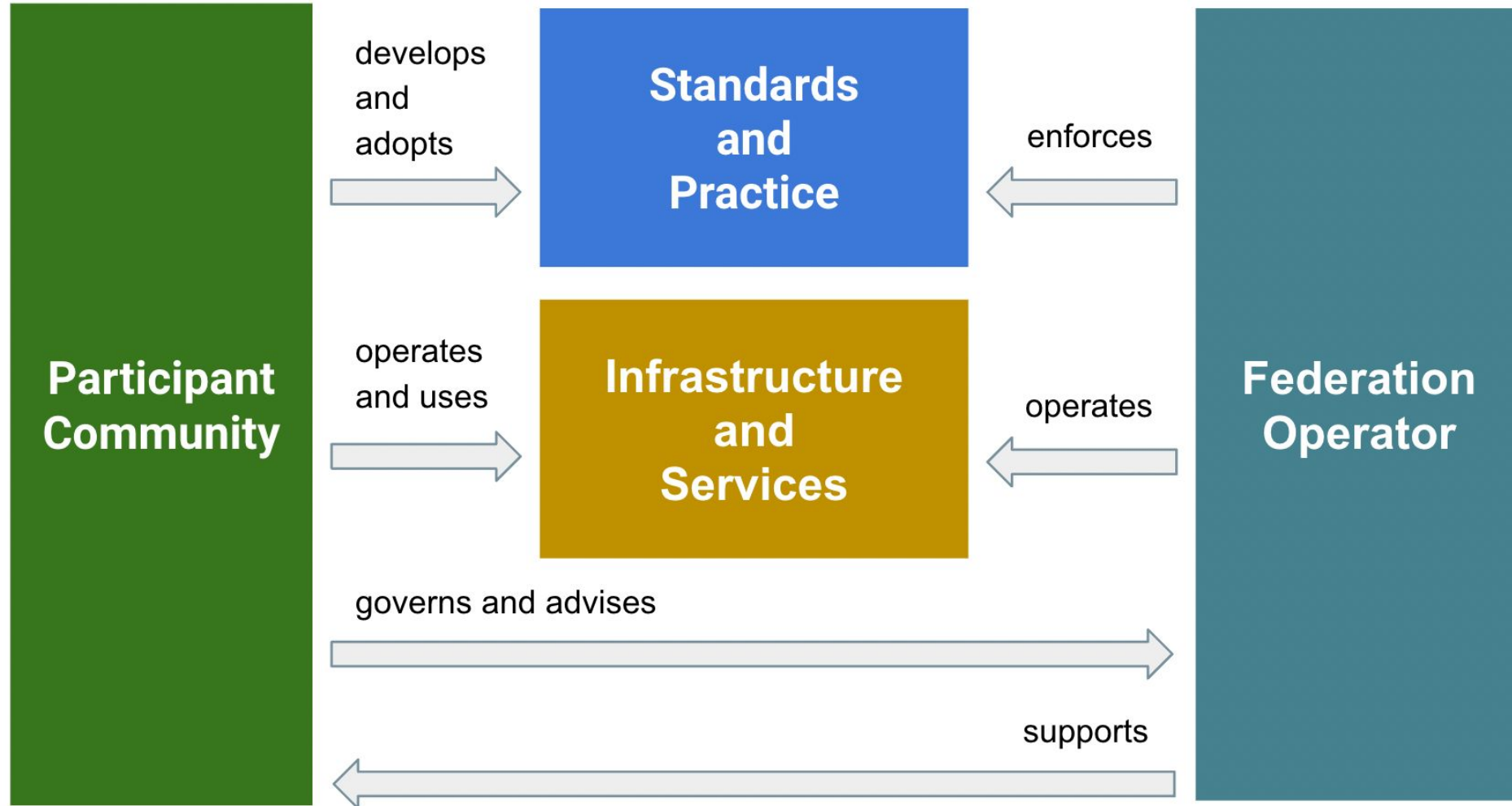
Identity Providers trust Service Providers to respect user privacy and to not misuse the information they receive.

Service Providers trust Identity Providers to securely authenticate users and provide accurate user information.



The Federation Operator provides services to broker and facilitate this multilateral trust.

InCommon Federation illustrated



Recap: what is the InCommon Federation?

Community

InCommon Federation is a community of organizations made up of higher education, research, commercial and government organizations who agree to adopt common identity management practices and technical standards to enable seamless academic collaboration at a global scale.

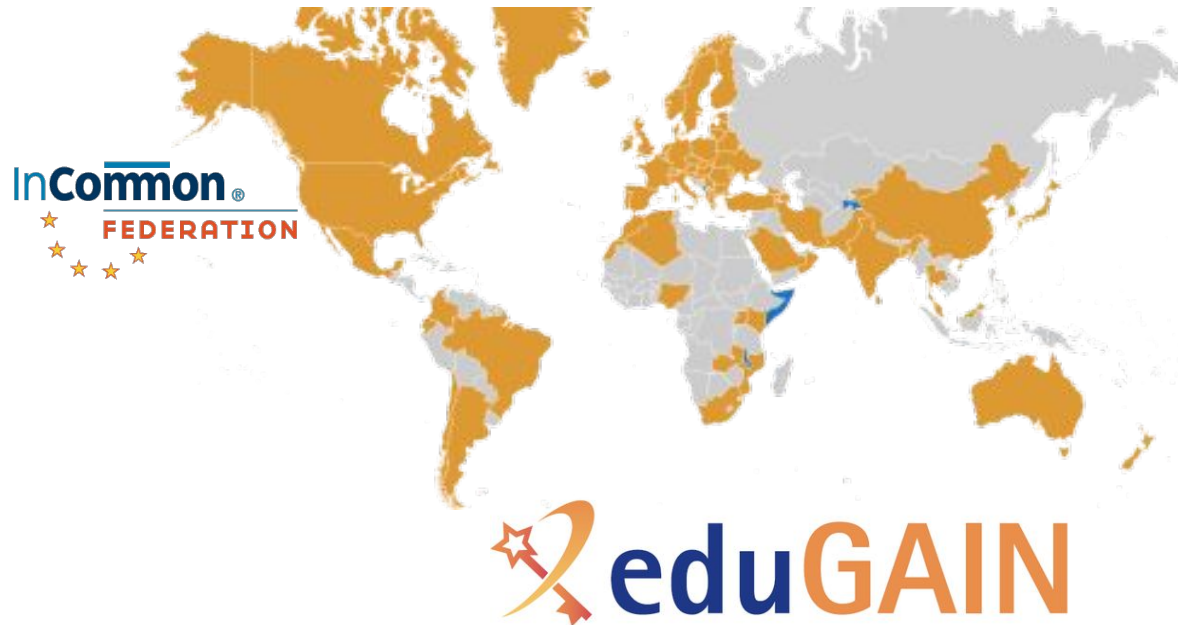
Standards & Practice

By adhering to these **community-curated standards and practices**, InCommon participants enable secure single sign-on access to local and global collaboration tools, connecting 10 million+ users and thousands of scholarly collaboration and research resources.

Infrastructure & Services

Internet2, with guidance from community governance, operates the necessary **infrastructure** to sustain this globally connected trusted access ecosystem. It also carries out adopted policies and practices. Internet2 is the InCommon Federation's **Federation Operator**.

Federation by the Numbers



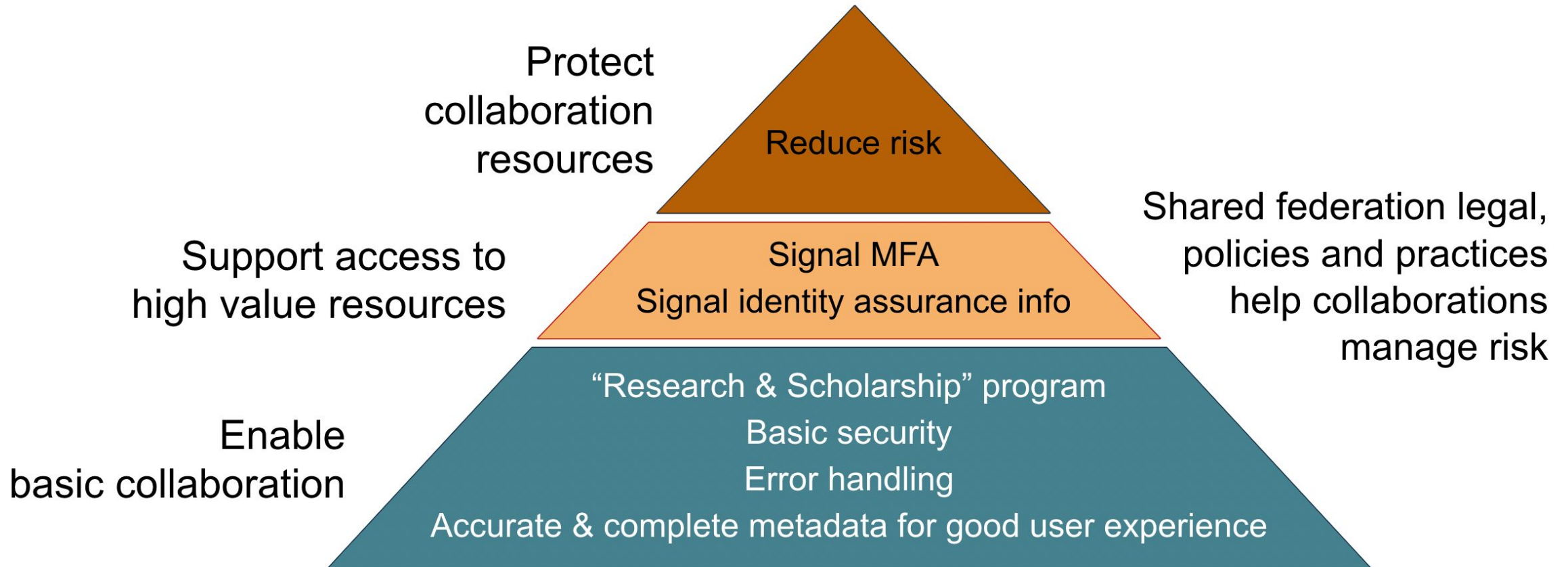
InCommon Federation (United States)

- 771 participant organizations
- 581 identity providers
- 5,676 service providers

eduGAIN: global inter-federation

- 78 countries
- 8,907 registered systems
 - 5,332 identity providers
 - 3,592 service providers

Building the pyramid of trust and interoperability



Building the pyramid: Baseline Expectations

The **Baseline Expectations for Trust in Federation** (Baseline Expectations, BE) is how the InCommon Federation establishes that trust among Federation participants.

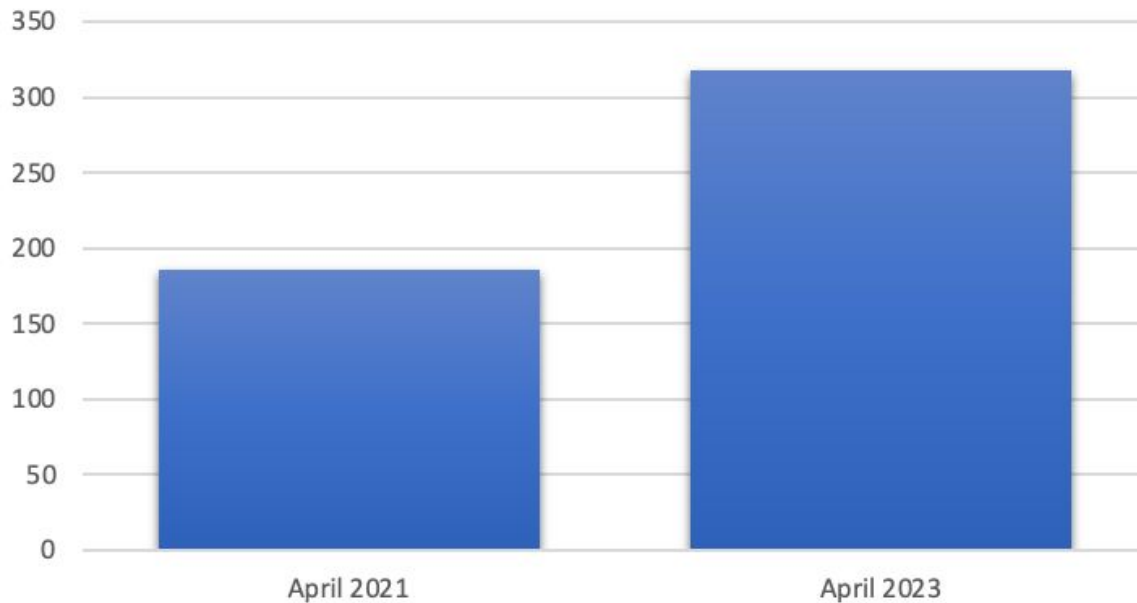
- provide a baseline for trust
- make collaboration more predictable
- include three brief sets of statements, each for **Identity Provider Operators (IdP)**, **Service Provider Operators (SP)**, and the **Federation Operator** respectively.
- evolves as the community's needs evolve to ensure that the InCommon Federation's strategic value to research and education continues to grow

<https://incommon.org/federation/baseline-expectations-for-trust-in-federation/>

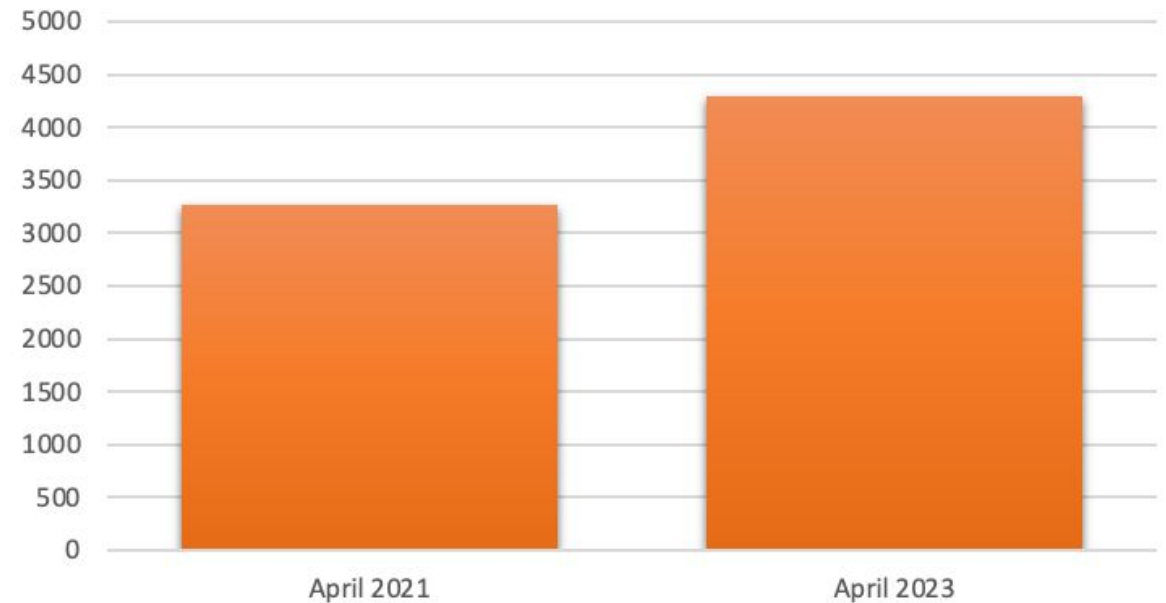
Raising Trust through Baseline Expectations – an example

“...endpoints are secured with current and trustworthy transport layer encryption.”

**Number of IdPs scoring "A"
in TLS encryption test**



**Number of SPs scoring "A"
in TLS encryption test**



Community's call to action raising trust and interoperability

In 2020, NIH called on its fellow InCommon community to support federated MFA and identity assurance to meet requirements for easy and secure access to NIH resources.

In 2021, the electronic Research Administration (eRA) system became the first NIH system to require MFA and basic user information through federated access.

The community responded.



April 2023 Webinar: NIH Community Update on MFA and Identity Requirements
https://drive.google.com/file/d/1b7ygO3la2nTL_v2d6oNEhctopSKaNW1Q/view

Major commercial solution providers are pitching in...

The screenshot shows the Microsoft Learn website interface. At the top, there is a navigation bar with the Microsoft logo, 'Learn' tab, and various menu items like 'Documentation', 'Training', 'Certifications', 'Q&A', 'Code Samples', and 'More'. Below this is a secondary navigation bar for 'Azure' with sub-menus for 'Product documentation', 'Architecture', 'Learn Azure', 'Develop', and 'Resources'. A search bar and 'Sign in' link are on the right. The main content area features a breadcrumb trail: 'Learn / Azure / Active Directory / Fundamentals /'. The article title is 'Introduction to multilateral federation solutions', dated '04/04/2023' by '1 contributor'. A 'Feedback' link is visible. Below the title, there is a section 'In this article' with links for 'Challenges with multilateral federation solutions' and 'Next steps'. The first paragraph of the article reads: 'Research universities need to collaborate with one another. To accomplish collaboration, they require multilateral federation to enable authentication and access between universities globally.' Below this is another section header 'Challenges with multilateral federation solutions' with a sub-header 'Universities face many challenges. For example, one university might use one identity'. On the left side, there is a sidebar with a search filter 'Filter by title' and a list of navigation links under 'Fundamentals documentation', including 'Overview', 'What is Azure Active Directory?', 'First steps', 'Create a Directory', 'Add a custom domain name', 'Associate an Azure subscription', 'Add your privacy info', 'Add company branding (preview)', 'Users, groups, and licenses', 'Quick security wins', 'Support and help', 'Reference', 'Identity architecture and deployment', 'Architecture', 'Azure AD architecture', 'Road to the cloud', and 'Parallel identity solutions'.

The community's persistent efforts to champion trusted and scalable federated access do pay off.

In April 2023, Microsoft published official documentation recognizing R&E's need for multilateral federation solutions and recommended a series of options to integrate Azure AD with InCommon.

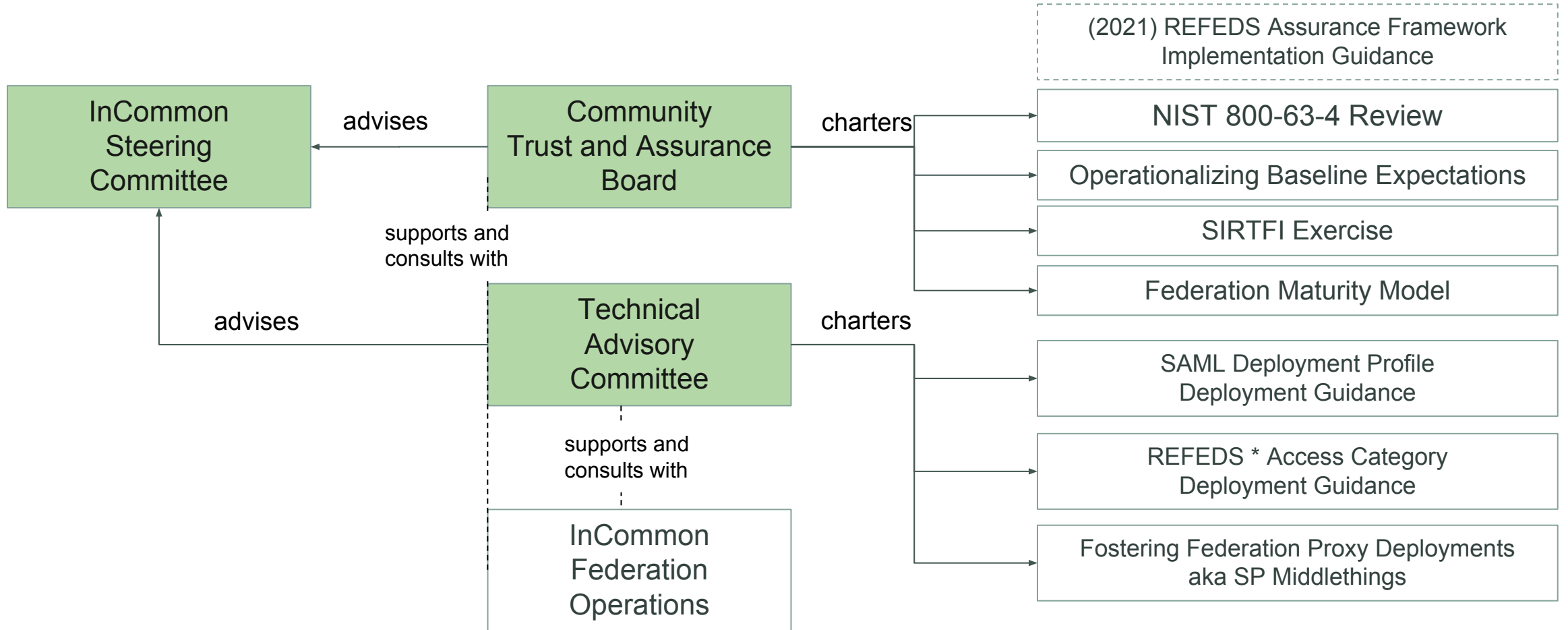
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/multilateral-federation-introduction>

Community Committees govern InCommon

A trio of sustaining committees consisting of elected community members governs the affairs of the InCommon LLC, promotes InCommon mission, establishes policies, and advises InCommon Operations.

- **InCommon Steering Committee (Steering)** - governs the affairs of the InCommon LLC: promotes InCommon mission, establishes policies, delegates authorities where appropriate, and advises InCommon Operations.
- **Community Trust and Assurance Board (CTAB)** - shepherds community consensus on trust and assurance related issues. CTAB is the steward of the InCommon Baseline Expectations for Trust in Federation policy framework.
- **Technical Advisory Committee (TAC)** provides community advisory to InCommon's operational processes practices, strategies, capabilities, and roadmap.

Community governance fostering trust and interoperability



How do I participate / get help?

Ask Questions

The InCommon Participants Mailing List (participants@incommon.org) is the main online gathering place for the community. Introduce yourself, and ask questions. Chances are someone on the list has been where you are and are eager to help.

Contact help@incommon.org for any official federation operations related matter.

Join Working Groups

InCommon moves forward via progress made in working groups. Joining a working group is a great way to network, learn, and make a difference at the same time.

Working groups are usually open to everyone. Whether you have expertise or just want to share your use cases, jump in!

Drive the bus

Do you know someone, perhaps yourself, who would be a great fit to help lead this community forward? Nominate them to serve on one of the leadership committees.

Call for nomination takes place each Fall. To learn more, visit <https://www.incommon.org/community/leadership/>

Resources

- InCommon Baseline Expectations for Trust in Federation:
<https://incommon.org/federation/baseline-expectations-for-trust-in-federation/>
- InCommon: Get NIH Ready
<https://spaces.at.internet2.edu/display/federation/get-nih-ready>
- REFEDS Assurance Framework Implementation Guidance for InCommon Participants
<http://doi.org/10.26869/ti.157.1>
- (Microsoft) University Multilateral Federation Solutions
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/multilateral-federation-introduction>
- CTAB 2023 Work Plan
<https://spaces.at.internet2.edu/display/ctab/ctab-2023-work-plan>
- TAC 2023 Work Plan:
<https://spaces.at.internet2.edu/display/inctac/InCommon+TAC+2023+Work+Plan>