



2023 INTERNET2
TECHNOLOGY
exchange

Scalable Trusted Federation

Updates from InCommon Advisory Committees

David Bantz, University of Alaska; Chair, Community & Trust Assurance Board
Jon Miner, University of Wisconsin; Co-chair, Community & Trust Assurance Board
Keith Wessel, University of Illinois; Chair, Technical Advisory Committee
Steven Premeau, University of Maine System
Albert Wu, Internet2

Today

InCommon Technical Advisory Committee (TAC) and Community Trust and Assurance Board (CTAB) have been working on several important initiatives to increase trusted interoperability among InCommon participants.

The first part of this session will describe the progress in these areas to date and how they will benefit scalable federation, including:

- Supporting better user identifiers and new entity categories
- Maturing practices through completion of Baseline Expectations v2 and operationalizing baseline expectations
- Contributing to and supporting standards updates with NIST and REFEDs

The second portion of this session will invite broad input on potential next directions to:

- increase assurance in identity and authentication
- facilitate interoperability and security
- streamline integration of relying parties
- better support protocol alternatives to SAML, e.g., OIDC

Community Trust and Assurance Board (CTAB)

- Represent the InCommon community in InCommon Federation trust and assurance related programs and initiatives.
- Develops projects and programs to improve trust, including participation in other national and international efforts.

CTAB Members

- David St Pierre Bantz (Chair, University of Alaska)
- Jon Miner (Vice Chair, University of Wisconsin - Madison)
- Warren Anderson (Laser Interferometer Gravitational-Wave Observatory)
- Pål Axelsson (SUNET)
- Matthew Eisenberg (National Institutes of Health)
- Erca Eibol (Florida Polytechnic University)
- Richard Frovarp (North Dakota State University)
- Michael Grady (Unicon)
- Scott Green (Eastern Washington University)
- Meshna Koren (Elsevier)
- Kyle Lewis (Research Data and Communication Technologies)
- Andy Morgan (Oregon State University)
- Rick Wagner (University of California San Diego)
- Eric Goodman (TAC Representative, University of California Office of the President)
- Albert Wu (Flywheel, Internet2)
- Tom Barton (Ex-officio, Internet2)
- Emily Eisbruch (Scribe, and holds us all together)

CTAB Updates

- **Baseline Expectations**
- **Best Practices**
- **Scalability**
- **New Challenges Opportunities**

Baseline Expectations (“BE”)

Community-developed technical requirements for InCommon participants that foster collaboration and trusted access to resources. CTAB advocates and monitors community compliance, and listens for possible evolution of BE.

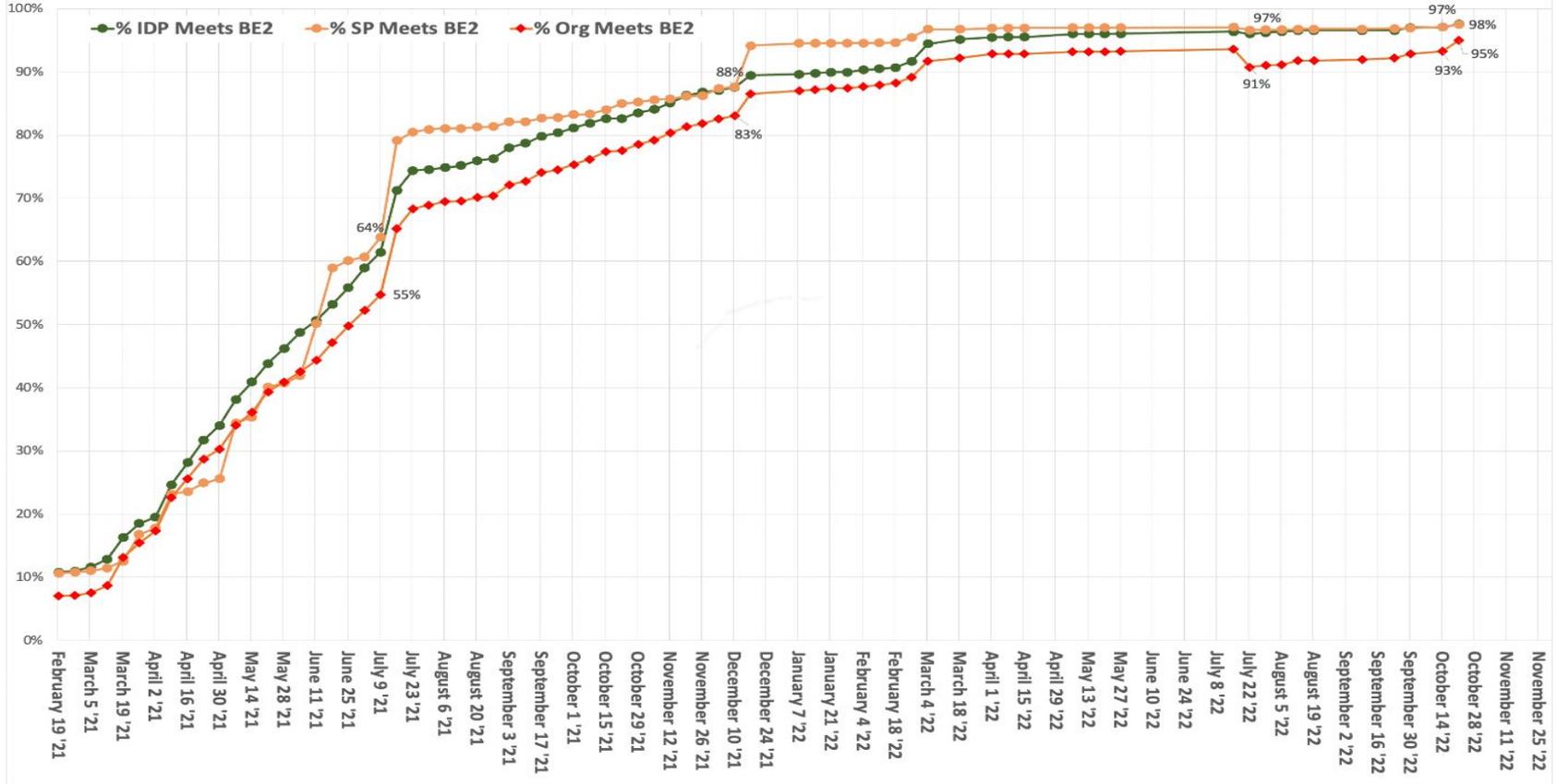
V1 (2020): ***maintain information about IdPs and SPs:***

- contact information for IdPs and SPs;
- URLs for privacy policy & logo

V2 (2022): ***information security readiness:***

- TLS 2.0 for all end points in IdPs and SPs;
- Explicit adherence to Security Incident Response Framework (SIRTFI)

Baseline Expectations Progress - % Meet BE2



“Operationalizing” Baseline Expectations

- Working group report:
<https://spaces.at.internet2.edu/display/ctab/2023-operationalizing-be-wg-summary-report>
- Automate Baseline Expectation adherence assessments
- Alert participants for updates needed to maintain accuracy
 - Contact information validation (technical and otherwise)
 - Validation of assertions
- InCommon Federation operations needs (tools)
to support ongoing BE compliance
 - Support greater delegation of functions to improve accuracy and latency
 - Simplify Federation Manager and other tools to improve ease-of-use.

SIRTFI Exercise

Continuing work on improving operational use of SIRTFI Framework.

- Training on SIRTFI in development.
- Resources on how to implement locally
- IAM Online in July: <https://incommon.org/academy/iamonline/>
- Table-top Exercise (TTX) in November
 - Volunteer now! -
<https://spaces.at.internet2.edu/display/sepwg/SIRTFI+Exercise+Working+Group>
- Come see Kyle go in to detail at 2:40!

Improving Trust with Clearer “Assurance” Guidance

REFEDS Assurance Framework v2

- Public consultation completed and working group reviewing feedback.
- Hopefully you didn't miss the session before this!

REFEDS MFA Profile v1.2

- Public consultation concluded and working group reviewing feedback.

NIST 800-63-4

- Participated in public consultation and provided feedback, especially on Federation Assurance Level

What's Next for CTAB in 2023 and Starting 2024 Work Plan

- Integrating RAF 2.0 in to BE and InCommon
 - (When it's published)
- Framing the next chapter in Federation Maturity
 - How do we even have the discussion about what's next?
 - BE has been highly successful, but does what we've done in the past and how we've done it still apply?



**InCommon Technical
Advisory Committee
(TAC)**

What is the TAC?

- InCommon Technical Advisory Committee
- Advise InCommon staff and Steering Committee
- Follow strategies and practices in R&E federations
 - Address current issues
 - Help plan for future trends

Current members

- Keith Wessel, University of Illinois Urbana-Champaign
- Heather Flanagan, Spherical Cow Consulting
- Joanne Boomer, University of Missouri
- Judith Bush, OCLC
- Matthew Economou, Independent Contractor
- Derek Eiler, University of Nevada System
- Eric Goodman, University of California Office of the President
- Matthew Porter, Benelogic
- Steven Premeau, University of Maine System
- Mark Rank, Cirrus Identity
- SME: Marina Krenz, REN-ISAC
- SME: David Walker, Independent
- Flywheel: Albert Wu, Internet2

2023 TAC Work Plan

Theme: Future-proofing InCommon

Work plan items:

- SAML 2.0 deployment profile adoption
- Entity category adoption
- Address federation proxies
- Federation testing - continued

2023 TAC Work Plan

TAC also helps with or monitors the following community developments:

- Digital wallets
- NIST 800-63-4 Consultation
- Browser changes
- HECVAT

SAML 2.0 Deployment Profile Adoption

- SAML2int (the profile) defines standards for interoperability
- Ratified by Kantara and accepted by InCommon in 2019
- Many profile items planned for adoption by InCommon
 - A significant one is the roll-out of new subject identifiers
 - public and pairwise
 - Supersede things like eppn, eptid, non-transient name IDs
- Working on a phased adoption of profile items

Entity Category Adoption

- REFEDS created new entity categories
- Signal the "level" of information needed by an SP
- Anonymous, pseudonymous, personalized
- Greatly improved signaling over current practices
- Working on the smoothest way to work this into federation practices

The working group invites your feedback

Working draft of the Deployment Guidance for * Access Entity Categories:

https://docs.google.com/document/d/1B45F1GKHjUY0j3QNIQ_XojFziKN9W02xCuL49vdAQRk/

Federation Proxies

- Formerly called "SP middle things"
- Building off of discussions from 2022 TechEx
- How to integrate proxies into federation framework
- What happens on other side of proxy might not follow rules
- Outcome: report recommending adjustments to operational practices
- Community WG spinning up to help make these changes

Federation Testing

- Two meanings
 - a sandbox for federation members
 - A framework for InCommon automatically testing compliance
- Needed for a while with a couple of false starts
- TAC is trying to bite off a smaller piece to start

Join Us

- Come to lunch: our face-to-face follows this session
- Join a community working group
- Nominate yourself (or someone else) for the TAC

What's Next

**What's do we do next? We
want your feedback!**



What's do we do next? We want your feedback!

What is important to you? What can we address to make the federation better and improve trust and interoperability? Are we looking at the right things? Are we including you? Can we?

Ideas

- Federation Capability Maturity Model?
- What does eduPersonEntitlement mean anyway?
- Can we scale? Does it scale? Should it scale?

Drive the Bus!

Leadership and Advisory Groups

Leadership opportunities for
community members who contribute
their insights, expertise, and talents
within Identity & Access Management

Taking nominations now through
October 1!

InCommon Steering Committee

InCommon Technical Advisory Committee (TAC)

InCommon Community Trust and Assurance Board (CTAB)

Community Architecture Committee for Trust and Identity (CACTI)

eduroam-US Advisory Committee

Please visit the Advisory Committee poster in TechEX foyer for more
information and submit a nomination.
Otherwise, you may click this [link](#) to submit a nomination.