InCommon Assurance Program: Transition and Close

October 28, 2019: Updated May 2021
v.3

This document provides an overview of and recommendations for the InCommon Assurance Program, given the success of InCommon Baseline Expectations as the next step in the community's evolution of trust. It also provides an overview of the closing of the program

Background

The InCommon Assurance Program began in February of 2012 as a result of discussion with CIOs and the US Government Services Agency (GSA) Federal Identity Credential and Access Management (FICAM) program looking to provide secure and identity proofed access to federal services. The InCommon community was motivated to pursue this because:

- The Federal Government Services Agency announced they were going to require Federal Agencies like NSF and NIH conform to a federated approach, requiring credentials approved at the NIST identity Assurance standard (800-63) levels
- Research service providers had real risks to manage that federation needed to address --- Identity assurance was the only concept anyone understood at the time that seemed to fit that need
- Our standard of "declarative" trust (the POP statement, a set of questions and self-reported disclosures) at the time was only a stepping stone to a higher level of trust. At some point we knew we had to raise the bar more broadly and more scalably

Over 5 years and thousands of hours of community-driven analysis and documentation, the program launched with an Identity Assurance Assessment Framework (IAAF) that included two Identity Assurance Profiles (IAP), Bronze and Silver, which were comparable to FICAM's levels 1 and 2 respectively. Six campuses applied for Bronze and one campus for Silver.

While testing was conducted that yielded practical solutions (See Outcomes section), real operational transactions between a certified campus identity provider and federal agency service provider never came to fruition. Primarily, this was due to two issues: the lack of federal service applications requiring certified credentials, and the internal audit and documentation barrier to adopt the profiles on the campus side. Over time, the

program value moved from an operational access technology to campuses adopting the Bronze profile as a means of demonstrating best practices in identity management.

With the revision of the core NIST Standard (800-63 v3), FICAM made significant changes to its program and created a draft for comment. The approach was determined to be untenable for the InCommon community especially given the lack of value.

In September 2019, GSA terminated their agreement with InCommon, underscoring their move away from their FICAM role and as a coordinating body for Agencies looking to federate with InCommon Participants. However, federal agencies' interest in InCommon doesn't seem to be affected by GSA's change as evidenced by discussions with NIH's increased support for seamless access to their research-oriented services registered in InCommon.

A New, Tested Approach: Baseline Expectations

At the same time, FICAM was revising its program, the InCommon Assurance Advisory Committee (AAC) , the body that oversees the InCommon Assurance Program, saw a larger need to address trust across the Federation. Among the InCommon participant community, there was a growing dissatisfaction with the scalability of the Participant Operating Practices (POP)---this self-declared and self-published set of answers to questions about trusted operations. To determine whether or not a partner was trustworthy, an organization reviewed their POP. This approach, while useful in the early days to provide transparency, didn't scale.

To that end, the AAC reviewed the POP and the difficulties inherent in the high-bar of the Assurance audit process. After about a year of discussions, the group developed a set of high-level statements that all InCommon Participants must adopt with the goal of increasing trust over time. Given the new approach, the AAC rechartered their role and changed its name to address these larger issues, becoming the CTAB, the Community Trust and Assurance Board.

From Optional Assurance to Baseline Expectations

The requirements that CTAB developed are broad and meant to be understandable by individuals outside of IT. Called Baseline Expectations, they more directly addressed the identity and service provider needs for basic security, authority to operate, InCommon metadata accuracy, and so on to ensure that the federation had a foundation on which to build. Addressing more than trust, the requirements are also meant to reduce friction to support Federation and ease the user experience

Built into this new idea was constant evolution of the expectations, dispute resolution to enable the community to monitor itself, and the idea that the key players in the

federation---identity providers, service providers, and federation operators---all contributed to the health of the federation.

Fast forward today and after 18 months of work on the part of CTAB and the community, InCommon has 100% adherence to Baseline Expectations v1.

Important Outcomes of the Assurance Program

Significant community work done under the auspices of the Assurance program led to the following conclusions:

- **Adoption:** Designing a new program requires understanding and participation of parties concerned. The disconnect between Federal Agencies and campuses created a significant “chicken-and-egg” problem in which each side expected the other to be significantly subscribed before adopting themselves. Now we include key players, iterate on smaller chunks of a big idea to ensure adoption and grow it over time to demonstrate the value (and adoption) is apparent.
- **Requesting MFA during the Transaction:** A mechanism for signaling the need for and completion of multi-factor authentication to support the Silver specification during a transaction was developed and tested. The InCommon Multi-factor Authentication Profile was subsequently transitioned to the international community of R&E federations, called REFEDS, to become a global standard.
- **Shibboleth Support for MFA:** Through early testing with NIH, requirements were developed for Shibboleth software to support the MFA Profile and the related escalation of a user’s authentication method by the identity provider.
- **New Partners:** Working with sister Trust Frameworks such as the Kantara Initiative has opened up doors for the InCommon community to influence global multi-sector federation standards.
- **Baseline Expectations**: Baseline Expectations and related approach for community engagement, vetting and adoption was a key outcome of the Assurance Program

Next Steps

There are three key actions that we have taken as result of the findings:

Transition the InCommon Assurance Program - GSA closed the FICAM program and now looks to Kantara to certify citizen-facing credential providers for the VA and other large-scale services. The federal government has also implemented login.gov, it’s own large scale identity provider instead of relying solely on others to do so.

Recommendation: InCommon leadership recommends we engage the affected campuses and close the program.

Status as of May 2021: Complete. All campuses have withdrawn from the program.

- Virginia Tech - Bronze/Silver
- Harvard University - Bronze
- University of Chicago - Bronze
- George Washington University - Bronze
- Quinnipiac University - Bronze
- University of Nebraska Medical Center - Bronze
- University of Maryland - Baltimore County - Bronze

Develop a contingency approach to address the need for high-assurance credentials - Federal Agencies and other security-minded cohorts may require the use of high-assurance credentials in the future.

Recommendation: InCommon will work with identity providers and partner organizations to offer high-assurance credentials if/when the need arises. One option would be to partner with Kantara: Identity providers could be certified through Kantara, and InCommon could include these trust marks in our metadata.

Status as of May 2021: Recent discussions with NIH is yielding a new approach to providing higher assurance credentials by leveraging the global federation standards through REFEDS. These standards specify how a provider of services can request the user to authenticate with a second factor and signal the need for information about identity proofing from the identity provider. These two standards coupled with the Baseline Expectation requirements go a long way towards pragmatically addressing security requirements for NIH. Once this approach is rolled out, we expect to broker a discussion between NIH and other Federal Agencies like NASA and NSF about doing something similar.

Evolve and Extend Baseline Expectations - CTAB is starting work on the Baseline Expectations v2, evolving the program as designed. REFEDS, the global research and education federation operators group, has developed approaches to assurance in the research space that was designed not to be onerous. As needs arise, CTAB may extend Baseline Expectations by adding optional profiles to address specific community needs.

Recommendation: InCommon Operations will continue our collaboration with the community and support the evolution of Baseline Expectations in addition to REFEDS research assurance profiles.

Status as of May 2021: NIH has adopted the REFEDS Assurance Framework and requires the use of it for access to research-related services. This is driving the international community to provide more guidance on implementation which is very positive. In addition, InCommon-wide adoption of Baseline Expectations version 2 is

underway. These new requirements raise the security by requiring encrypted exchanges between IdPs and SPs and mandates federation incident response cooperation.