Steward Program Proof of Concept
Six-Month Status Report

(7/25/2017)

Repository ID: TI.29.1
Authors: Mark Johnson
John Krienke
Kevin Morooney
Mark Scheible
David Walker <https://orcid.org/0000-0003-2540-0644>
Ann West
Mike Zawacki
Sponsors: Internet2 and MCNC
Superseded documents: (none)
Proposed future review date: (none)
Subject tags: steward, incommon, identity federation

Executive Summary

In December of 2016, MCNC and InCommon launched a proof of concept of the InCommon Steward Program, an effort to extend federation to K-14 schools (K-12 and community colleges). This report is an assessment after operating the proof of concept for its initial six months, intended to collect data and determine whether the program is meeting its goals and providing the expected benefits. In particular, we considered the following:

- Benefits to Stewards and Represented Constituents
- Impacts of outsourcing of InCommon's onboarding functions
- Impacts of increasing K-12 participation in InCommon
- Operational issues
- Resource requirements for InCommon and MCNC

.Some key observations are:

- Operational issues have been minimal and communication within the Registration Authority "virtual team," comprised of personnel from InCommon and MCNC, has worked well without over-taxing either organization's resources. There was considerable preparation put into training of MCNC personnel that contributed significantly to successful operation.
- There were no significant impacts on InCommon's trust model observed during the proof of concept, largely due to prior community outreach and consultation. In fact, the presence of a knowledgeable Steward has improved alignment with recommended operational practices. There was only one operational confusion related to trust that was quickly resolved; training for future Stewards will be improved in this area.
- The Children's Online Privacy Protection Act (COPPA) was discussed as part of the community consultation. While multiple potential issues were discussed that *could* be addressed by the Steward Program, it was decided to wait for real-world experience through the proof of concept before taking action. To date, the proof of concept has uncovered no COPPA-related issues.
- In general, impacts (positive or negative) of the Steward Program on K-12 have been difficult to observe, due to the timing of the proof of concept late in the school year. We hope to learn more when the new school year opens in the Fall.

Now that the Steward Program's federation onboarding and operational processes have been developed and tested, InCommon and MCNC will initiate a six-month business development phase to build on the program's value for Represented Constituents and Stewards as identified in Observations and Lessons Yet to Be Learned of this report, as well as to develop the greater program business and legal model. MCNC and InCommon will also develop a case study of the Steward Program, including recommendations for other Regionals interested in participating and related artifacts for community use.

Document Intent

This document provides a 6 month status report on the InCommon Steward Program Proof of Concept being conducted with MCNC, which runs the North Carolina Research and Education Network (NCREN).

Background

K-12 school districts and community colleges could reap the same benefits of federated Identity as do higher education institutions do with the InCommon Federation, but often lack the resources, skill sets, or experience to implement and manage the necessary infrastructure. The Quilt and more specifically MCNC have been working with InCommon on how to resolve this issue and developed the InCommon Steward Program to scale InCommon Federation Operations and ease the burden of federation for K-12 and community colleges.

From the beginning MCNC and InCommon adopted shared goals and have worked towards those goals resisting the temptation to expand the scope or add additional goals. The goals of the Proof of Concept are to understand

- Benefits to Stewards and Represented Constituents
- Impacts of outsourcing of InCommon's onboarding functions
- Impacts of increasing K-14 participation in InCommon
- Operational issues
- Resource requirements for InCommon and MCNC

Please see *Partnering for K-14: The InCommon Steward Program* (PDF) for more background and full description of the Steward Program and how it aligns with the InCommon Trust Model. Also, see the project's monthly blog for a recap of events during the proof of concept.

Findings

Roles of MCNC and InCommon

Scaling federation services to the large number of K-12 school districts and community colleges requires distributing some of InCommon's administrative and onboarding tasks, as well as providing direct support to K-14 institutions.

In this light, InCommon Stewards, currently limited to state and regional non-profit R&E network providers, wear two hats.

- On behalf of InCommon, the Steward provides Registration Authority (RA) services related its member K-12 school districts and community colleges (also known as "Represented

Constituents" or RCs). The Steward is trained to follow the same vetting and onboarding processes as InCommon.

- On behalf of its Represented Constituents, the Steward manages Identity Providers and Service Providers and the associated metadata, and provides other technical services. Stewards are also responsible for direct support for their RCs.

InCommon is responsible for the one-time events of vetting the Steward's organizational identity and contact people, as well as providing training and support for the Steward.

While operational duties are performed by staff from multiple organizations, the overarching principle is that there is a single virtual organization comprised of staff from both InCommon and its Stewards that performs these duties according to common standards.

Onboarding Support

Onboarding Documentation: Considerable time was spent preparing documentation to support operation of the Steward Program, including policies, procedures, and how-tos for specific situations. A comprehensive slide deck created for the MCNC in-person workshop is reusable for future Stewards. All of this information is collected in the knowledge base.

Onsite Workshop: The orientation workshop was conducted over a three-day period at MCNC. Future workshops may take less time, given that this initial workshop included some service startup coordination. Because of the timing of the workshop, not all MCNC operational personnel were available. This may have resulted in the need for more time and attention from InCommon during MCNC's early registrations. For future workshops, it would be better to assure that all affected personnel are available.

Post Workshop Assistance: Once the training was completed, desktop video conferencing was used to monitor MCNC's first registration of RC IdPs. The approach worked well, particularly since not all MCNC personnel who eventually became involved were available for the in-person training. It also meant that InCommon personnel were available to assist when something went wrong.

Moving an Existing InCommon Participant to be an MCNC Represented Constituent: The first RC registration process uncovered an operational issue. The first RC was already an InCommon Participant and the written procedures did not address the process of migrating an existing Participant. Some just-in-time database updates were required, and MCNC and InCommon modified the procedures. The remaining registrations proceeded without problems.

Operational Support

Support for the Steward program is structured in two layers. The Steward provides support to its Represented Constituents, and InCommon provides support for the Steward. The team created multiple communication channels and a knowledge base for the people who perform operational duties from both InCommon and MCNC.

- InCommon holds regular meetings for staff members who perform Registration Authority tasks. These meetings were expanded to include MCNC staff members who also perform these duties, providing a forum for discussion of operational issues and potential changes to policies, procedures, and tools like the Federation Manager.
- An email list was created for asynchronous communication.
- A Slack channel was created for real-time communication on an as-needed basis.
- A wiki space was created as a knowledge base.

The multiple communication channels work well, allowing the right people at the right time to address the few issues that have arisen during the six-month period.

Trust Model Impacts

Separation of Duties: During the proof of concept, there was some confusion over Federation Manager user roles and the fact that the same person cannot approve their own organizational metadata submissions without violating the trust model. The issue was quickly resolved and will be covered in future Stewards' in-person workshops.

Aligning Practices: The second issue involved a K-12 district's vendor that was using a SAML1 assertion no longer supported by InCommon. The IdP migration process only registered the SAML2 endpoints, so the application broke for a half-day while the problem was resolved with the vendor. Here MCNC acting as a Steward ensured that basic Federation practices were met by their Represented Constituents and enhanced the interoperability of the Community as a whole.

K-12 Participation in InCommon

K-12 and Privacy: Prior to the proof of concept (PoC), there was considerable discussion about whether COPPA (Children's Online Privacy Protection Act) regulations might have an impact on access to some InCommon service providers.[1] In the end, however, it was decided that deploying mitigations for those impacts is not appropriate at this time. That decision will be revisited if significant issues surface with K-12 participation. It should also be noted that due to CIPA (the Children's Internet Protection Act) regulations, K-12 school districts are required to use content filtering to restrict access to many websites. This would naturally limit the number of websites that might be concerned about an increase in K-12 COPPA-protected students.

During the first six months of the proof of concept, no significant issues with K-12 participation in InCommon were observed. This was due to several issues that are listed below in the section on "Limitations". However, due to delays in bringing a number of services online for K-12 users to access, there was no real increase in the number of K-12 users.

It is expected there will be more opportunity to evaluate the impact of increased K-12 participation in the federation after the next school year begins in the fall of 2017.

---

[1]The primary focus of COPPA is to protect children under the age of 13 from the online collection of their personal data. The website operators must post a Privacy Policy with specific information about data use and include contact information and the ability to "opt-out" for parents.

Communications

There was significant communication and consultation with the community, both within InCommon and internationally, before the proof of concept was launched (see InCommon Steward Program: Federation for K-14).

The proof of concept included monthly community updates provided via a blog. There were also more formal press releases highlighting specific achievements:

- MCNC and Internet2 celebrate federated ID milestone with Davie County Schools
- FIM: Three letters with infinite possibilities for NC education (+ video)

Observations and Lessons Yet to Be Learned

A key objective for the Steward Program was for InCommon to transfer the Registration Authority (RA) process from InCommon Operations to the Steward, and not impact the InCommon trust model. An objective of MCNC (the Steward) was to be able to more economically provide federation services to K-14 institutions, particularly those that didn't have the resources to operate IdPs on their own. And a joint objective of the Steward Program was to more easily scale federation using the resources of the stewards.

Impact to the Regional: The impact on MCNC of the operational aspects of federation (essentially, the RA functions and metadata registration) has been manageable. For the reasons described in "Value Proposition" below, however, the timely development of service providers for our RCs and timing of the proof of concept with respect to the school year, has prevented us from observing the overall benefits of the Steward Program's value proposition.

Value Proposition: The following items were limitations that prevented establishment of the K-14 value proposition in time to be observed during the first six months of the proof of concept:

1. **Steward as Service Catalyst** - In the Steward Program section above, the steward is described as wearing two hats, 1) On behalf of InCommon, maintaining the trust model by vetting RCs and registering their metadata, and 2) Representing the RCs by installing and operating their IdPs in the InCommon federation. However, the Steward needs to wear a third hat, in that they need to 3) Work with service providers to ensure federated services exist for their RCs to benefit from federation. Not many organizations in InCommon provide services to K-12 institutions. Since the Steward POC was primarily focused on K-12 institutions, new services needed to be cultivated, and the Steward needs to work with these service providers to federate their application/resource. However, this takes time to both communicate the value proposition to the service provider, and if they're receptive to that, to develop the federated solution. The time required for establishing these services (if they don't already exist) must be factored into any startup timeline.

2. **Service Organization Adoption of Federation** - New services had been identified for the POC, however, while there was interest in pursuing federation, other work was already scheduled within the six-month window and a federation solution was competing with existing projects for the service providers.

3. **TIming of the PoC** - Unfortunately, due to delays in getting the Steward POC started, it didn't begin until the middle of the school year (mid-December), so while there was interest in participating in the program, schools traditionally do not implement new services or changes until the start of the following school year (implementing over the summer).

4. **Existing Statewide Identity Infrastructure -** Although possibly unique to North Carolina, there exists a statewide IAM infrastructure for K-12 which provides accounts and access to many of the common cloud-based applications used in the schools. Therefore, candidate service providers to introduce in the proof of concept were limited to those applications not already being provided through the existing infrastructure.

Scaling the Federation: In developing the Steward Program, the expectation was that stewards would be adding large numbers of K-14 institutions. We deliberately limited participation in the proof of concept, so effects of scaling were not observed.

The Next Phase

Now that the Steward Program's federation onboarding and operational processes have been developed and tested, InCommon and MCNC will initiate a six-month business development phase to build on the program's value for Represented Constituents and Stewards as identified above in Observations and Lessons Yet to Be Learned, as well as to develop the greater program business and legal model. MCNC and InCommon will also develop a case study of the Steward Program, including recommendations for other Regionals interested in participating and related artifacts for community use.