Proposed Federation Partnership Models For InCommon and Regionals

DRAFT

DRAFT v1.0, 09-Jan-2014

Mark Johnson, MCNC
John Krienke, InCommon
Mark Scheible, MCNC
David Walker, InCommon
Ann West, InCommon

Table of Contents

Introduction

This document presents a proposal for federation partnership models between InCommon and Regional Network Providers (Regionals) to extend InCommon federation services to K-12 and community colleges. The models were originally discussed at an InCommon/Quilt Workshop which followed The Quilt Winter Meeting in February 2013 and further defined at a meeting specifically held to start the process. It took place on September 19, 2013 at the Chicago Airport Hilton; John Krienke, Ann West and David Walker of InCommon, and Mark Johnson and Mark Scheible of MCNC were in attendance.

K-12 and community college institutions are frequently challenged by the technical skillsets and the membership costs required to participate under the current InCommon operating and business model. The models proposed in this paper describe scenarios in which the Regionals can leverage their existing relationships and experience to fill the gaps between what's needed to participate in a federation and what these smaller institutions can do.

The *site administrators* of Identity Providers (IdPs) and Service Providers (SPs) do the vast majority of the work in a federation. It is the *Federation Operator's* role to provide technical services that scale federation for the members, and develop and enforce common standards and practices to ensure interoperability and multilateral trust among those IdP and SP administrators and their institutions. In particular, there are two key - but by no means sole - work functions performed by InCommon and other international R&E federation operators that provide the best opportunity for Regionals to add value and reduce cost for their constituents:

1. **The Registration Authority (RA) function**, which establishes the federation "trust" with the candidate organization. This involves:
    a. Vetting of the Organization and its Internet DNS domains
    b. Vetting of the Organization's People
        i. The Executive
        ii. One or two Site Administrators (SA)

2. **Metadata (MD) Management**, involving:
    a. Testing/Inspecting submitted MD according to community requirements
    b. Signing and publishing the Metadata Aggregate (MDA) of the federation
    c. Hosting the MDA for federation members to download

In looking at which organization would perform each of the above functions -- InCommon, the Regional or their constituent K-12 or Community College institutions (referred to as *Represented Organizations* (ROs) throughout this document) -- five models were identified, in addition to the current model.

These are based on shifting from InCommon to the Regional, the responsibilities for metadata management, onboarding of new members, process flows, legal agreements, and cost sharing, as well as value-added Regional support services not currently offered by InCommon. Background on existing and additional responsibilities may be found in Background Information for Regional / InCommon Collaboration.

The five models proposed are outlined in **The Models** section below. While there are many more potential models, we feel these five, focused on the RA and metadata management functions, represent the needs and strategies of most Regionals.

It is important to note that this document approaches these models from a high-level business perspective, and there are many more components and details to running and participating in a federation than are addressed here.

The Models

This section describes various models for service delivery, legal/contractual relationships, and cost sharing among InCommon (IC), a Regional network organization (RE), and a Represented Organization (RO) that uses the InCommon Federation. Note that the Represented Organization may or may not be a member (formal participant) of the InCommon Federation (*i.e.*, have a contract with InCommon in addition to the Regional); this will depend on the specific model.

Current Model

	Supports	**Contracts**	**Pays**
InCommon (IC)	RO	RO	
Regional (RE)			
Represented Organization (RO)		IC	IC

In the current model, the Represented Organizations each join InCommon and use its services. Since they are individual members of InCommon, the ROs appear as individual organizations to the rest of the federation. From InCommon's point of view, each RO is an independent legal entity and participant in the trust federation with its own authority over submitting and approving metadata updates. This model does not involve a legal contract between InCommon and the Regional.

Model 1: Facilitation and Support

	Supports	Contracts	Pays
InCommon (IC)	RO, RE	RO	
Regional (RE)	RO	RO	
Represented Organization (RO)		IC, RE	IC, RE

In the Facilitation and Support Model, the Regional coordinates *informally* with InCommon to help the Regional's ROs. The Regional provides services to assist its constituents in joining InCommon and enabling the Regional's users to access federated services (through an Identity Provider) and to offer services to other federated users (via Service Providers).

Since ROs are individual members of InCommon, they appear as autonomous participants to the rest of the InCommon federation and use the federation services directly. From InCommon's point of view, each RO is an independent legal entity and participant in the trust federation with its own authority over submitting and approving metadata updates - this is no different than the Current Model.

The Regional focuses on offering enhanced services for its constituent organizations, while InCommon provides its standard set of member services to the RO. Examples of Regional services include hosted IdPs, consulting services, SP integrations and training. This model does not involve a legal contract between InCommon and the Regional.

Model 2: Business Partnership (Business Steward Role)

	Supports*	Contracts*	Pays*
InCommon (IC)	RE, (RO)	RE, (RO)	
Regional (RE)	IC, RO	IC, RO	IC
Represented Organization (RO)		RE, (RO)	RE or IC

** This model may have different options for agreements among the organizations*

The Business Partnership Model would be appropriate for a Regional that has strong business connections with its constituents, is interested in cutting the cost for their RO's to join InCommon, but has limited technical resources required for technical support.

In this Model, the Regional partners with InCommon to be a Registration Authority (RA) for its ROs. In this role, the Regional would perform functions like management of legal relationships, billing, and validating participating organizations and their officers, etc. These are required to set up and maintain trust with the RO. This model would require a legal contract between InCommon and the Regional for the performance of these functions on InCommon's behalf. Agreements between InCommon and the ROs may depend on how this model is implemented (see TBD below).

This model relies on shifting the responsibilities for operational onboarding, billing and likely the metadata submission processes from InCommon to the Regional, leveraging the strengths of both organizations to reduce overall cost and achieve a more cost effective federation solution for ROs. The Regional may or may not provide training and support services for the ROs.

Depending on the agreement established with InCommon (see TBD below), if there is no direct relationship between InCommon and the ROs, then this model requires the Regional to keep its member organizations apprised of national federation issues, as well as to represent its member organizations in InCommon as a single Regional entity.

TBD:

This model needs input from the Regionals (and InCommon) on what would be a likely scenario (or scenarios), for sharing the RA and business administration functions.

Option A - The Regional joins InCommon and acts on its behalf as a Registration Authority for all ROs performing the functions listed above, including the management of individual agreements with InCommon for each of its ROs (in which case the ROs would be recognized members of InCommon).

Option B - The Regional joins InCommon and acts on its behalf as a Registration Authority for all ROs performing the functions listed above. In addition, as part of the contract with InCommon the Regional also acts as the legal entity responsible for all ROs (and additionally would likely be responsible for the conduct of their IdPs and SPs in InCommon). In this scenario, the ROs would not be recognized members of InCommon and are represented in InCommon through the single Regional entity.

Another scenario might have the Regional start with Option A and migrate to Option B as the number of ROs reaches some "critical mass".

The expectation is that there would be a reduction in the fees owed to InCommon as a result of this partnership. However, it's not clear whether Option A would result in a total fee equal to n organizations times a discounted amount or not. Option B might involve the Regional paying under a similar formula, or paying an annual "flat rate".

Also, the Business Partnership Model only describes the administrative and RA role filled by the Regional, it does not address the Metadata Management or technical service needs of the ROs.

These can be handled by the RO if it has the resources and skillsets in place, or these services might be contracted out to one of the InCommon Affiliates.

Model 3: Technical Steward (Role)

	Supports	Contracts	Pays
InCommon (IC)	RE	RE, RO	
Regional (RE)	RO	IC, RO	IC
Represented Organization (RO)		RE, IC	IC, (RE)

The Technical Support Model would be appropriate for a Regional that has strong technical resources, but doesn't have close business relationships with its constituents or may not want the responsibilities of the Business Steward role.

In the Technical Support Model, the ROs delegate the support of their *federation infrastructure* to the Regional. The ROs may or may not be direct members of InCommon, but the Regional likely is, and InCommon supports the Regional staff.

In this model, the Regional provides technical support functions where they *may* be done more cost effectively than by the RO. The Regional is responsible for the operation and support of the ROs' IdPs, and the metadata management functions such as submission, testing, inspection and validation, some of which are currently provided by InCommon. Additionally, the Regional may provide facilitation and training services for the ROs. This model would likely involve a legal contract between InCommon and the Regional.

TBD:

While the Technical Steward Model describes the Metadata Management and Technical Support role filled by the Regional (for its ROs), it does not address the administrative and RA responsibilities required by InCommon to join the federation. These would likely still need to be performed by InCommon directly with the RO. Therefore, it's not clear this would be a viable model on its own, unless taking over the Metadata Management functions for their ROs (including some functions currently performed by InCommon) would result in a lower membership fee for their constituents.

It has not been determined yet what legal role the Regional would have in InCommon with respect to its Represented Organizations. Whether this model would require the Regional to be the legal entity responsible for the conduct of its ROs' IdPs and SPs in InCommon or whether *each RO would still need to join InCommon as a legal entity?*

This Technical Steward Role might instead be considered an “Outsourced Support” role which could apply to either a Regional or an InCommon Affiliate. Under that scenario, however, the Represented Organization would need to sign a legal agreement with InCommon and be legally responsible for the conduct of its IdPs and SPs like any other member in the federation.

Model 4: Full Service Steward

	Supports	Contracts	Pays
InCommon (IC)	RE	RE	
Regional (RE)	RO	IC, RO	IC
Represented Organization (RO)		RE	RE

This Full Service Steward Model combines the responsibilities of the Business Partnership and Technical Steward roles (Models 2 and 3) and is appropriate for a Regional that has close business relationships with its constituents, a strong technical staff, and is likely a current InCommon member (Sponsored Partner).

The Regional partners with InCommon to be the Registration Authority (RA) for this defined subset of InCommon users, providing RA processing and Administrative Functions (participant agreements, billing, performing validation and administrative functions for Organizations, Officers, etc.) on behalf of their ROs. This model relies on sharing the responsibilities for operational onboarding and metadata management processes between InCommon and the Regional, leveraging the strengths of both organizations to reduce overall cost and achieve a more cost effective federation solution for ROs.

The Regional and/or the ROs establish multiple IdPs, potentially one per Represented Organization. The IdPs may be configured so they appear as individual IdPs (one for each RO), to the rest of the InCommon federation, even though they are represented by a single organization, the Regional. From InCommon’s point of view, the Regional acts as the legal entity responsible for all IdPs, although the Regional may have independent legal relationships with the ROs. While ROs may have operational responsibility for their own IdPs, metadata updates must be approved or submitted by the Regional. In this model, the Regional would also provide support and training to its ROs.

Because there is no direct relationship between InCommon and the ROs, this model requires the Regional to keep its Represented Organizations apprised of national federation issues, as well as to represent them in InCommon as a single Regional entity. Legally, the Regional is the contracting entity responsible for the conduct of the participating ROs' IdPs and SPs in InCommon.

InCommon becomes the central operator of federation services such as trusted lookup and error handling services, which the RO use through the Regional. This model would require a legal contract between InCommon and the Regional.

Model 5: Full Federation Operator

	Supports	Contracts	Pays
InCommon (IC)	RE	RE?	
Regional (RE)	RO	IC?, RO	IC?
Represented Organization (RO)		RE	RE

In the Full Federation Operator model, the Regional is operating a separate federation from InCommon and establishes its own processes for "onboarding" the Represented Organizations and maintaining a Regional lookup services, error handling etc. The Regional and InCommon have a signed agreement that allows the Regional to exchange information (metadata aggregates) about participating IdPs and SPs to aid interoperability. Federation policies and Metadata registration rules may or may not be aligned, affecting the cost and utility of the partnership.

In this model, the Represented Organizations are not members of InCommon and can't access services in the InCommon federation unless information about the IdPs and SPs (metadata) is exchanged. Support by InCommon is limited to this metadata exchange process; the Regional provides all training and support for the Represented Organizations.

This is probably the least cost effective model, as many trust processes must be duplicated between InCommon and the Regional.

High-Level Comparison of the Models (Chart)

Roles/Models	Services Provided	Legal	Cost
Current	● No Regional Services Provided to ROs ● InCommon supports the RO directly	**ROs join InC** Contract between InC and RE is NOT required	Normal Member Fees for RO
Facilitation and Support	● Regional may assist RO with submitting InC Participant Agreement ● Regional may provide Support & Training services ● Optional hosting of RO's IdPs/SPs by Regional	**ROs join InC** Legal contract between Regional and InCommon may not be required	Normal Member Fees for RO
Business Partnership	● Regional provides delegated Registration Authority (RA) and Contact Relationship Services to ROs ○ Vetting of ROs and contacts (Exec and SA/DSA) ○ Managing contacts with RO is ongoing ○ Process InCommon Agreements, Billing for ROs ● SA submission or approval of RO Metadata by RE will likely be required ● Additional Support Services provided by Regional to ROs are Optional	**Legal Contract Required (between RE and InCommon)** **ROs may or may not be members of InC** depending on how the model is implemented (the contract between the RE and IC)	**Cost Sharing** Between InCommon and the Regional
Technical Steward	● Regional provides Support to RO ● Delegated Metadata management and submission to InCommon... ○ May submit MD as SA for ROs ○ (Auto-validate MD is scripted) ○ Manually-validate MD ○ Regional Submits Validated Metadata to InC ● Facilitation & Hosting is Optional	**Legal Contract Required (between RE and InCommon)** **ROs may or may not be members of InC** depending on how the onboarding functions (RA) are handled	**Cost Sharing** Between InCommon and the Regional
Full Service Steward	● RE provides all of the following to RO:	**Legal Contract Required (between RE**	**Cost Sharing** Between

	○ Facilitation and Support Services ○ Business Partnership Services (RA, Administrative, Billing) ○ Technical Steward Services (Metadata management and submission)	**and InCommon)** ROs are not Members of InC	InCommon and the Regional
Full Federation Operator (Regional)	● Independent Federation Operator - manages all services for Regional Federation. ● May exchange Metadata Aggregates with InCommon (Publish & Subscribe)	Domestic Interfederation Agreement or MOA between Regional and InCommon?	Undetermined (may be a fee for Publish & Subscribe service)

Other Issues Raised During the Chicago Meeting

- Some models require the Regional to represent its membership to the rest of the federation. This may introduce contractual and liability issues within the Regional, and could impact the name used by the Regional for this purpose within the rest of the federation.
- There is currently no Regional participating formally in InCommon governance. Perhaps Regional representation should be added to the InCommon Steering Committee.
- Need to define the “membership status” (or new member categories) of institutions represented by the Regionals – as well as a “Regional” membership class. This would also include default or optional membership benefits available to Regionals and their member institutions (ROs).
- InCommon’s certificate service is available to Regionals for internal use. A new agreement with Comodo allows Regionals to sell certificates to K-12 schools.
- Cost recovery models require more thought. Some Regionals may bundle federation services into their existing pricing models, and some may not. The revenue sharing between the Regional and InCommon (particularly for the three *Stewardship Models*) will require closer examination of the costs and savings associated with shared operational responsibility.
- The concept of Regional-based entity tags was discussed. It’s not clear there is a need for Regional-based entity tags, but there could be for K-12. The problem would be in knowing who is authoritative and how schools would be vetted.
- We need to address both “How do we scale?” and “How do we mature?” The latter argues for leaving responsibility for developing activities like assurance with InCommon as they mature, rather than distributing them to Regionals.
- K-12 and Community Colleges need fairly direct support. The Regionals are probably better positioned than InCommon to provide that direct support.

Next Steps

1. After organizing and developing the five models in the current revision of this paper it is clear that to move forward, InCommon needs to propose an acceptable pricing structure for Models 2-4 based on the shared responsibilities between InCommon and the Regional.

2. Term sheets listing these responsibilities need to be created (these will likely be the foundation for legal agreements).

3. MCNC plans to pilot the Full Service Steward model (Model 4) with InCommon after working through items 1 and 2 above, and will report to other Regionals via The Quilt.

Glossary

Terms

- Regional (RE) - a Research and Education (R&E) Network Provider
- InCommon (InC or IC) - the National R&E Federation Operator for the USA
- Represented Organization (RO) - Constituent organizations of the Regionals
- Identity Provider (IdP) - A server(s) running federation software which authenticates users (identities), or the organization which "owns" the identities.
- Service Provider (SP) - A server(s) running federation software which protects a resource or application, or the organization which offers the resource. Also referred to as a Relying Party (RP).
- Metadata (MD) - Data that describes attributes used in the federation process such as those used to identify – and either locate or determine the relationship to – a particular Identity Provider or Service Provider.
- Metadata Aggregate (MDA) - a file which contains an aggregate of metadata from multiple IdPs and SPs.
- Registration Authority (RA) - an organization that establishes the "trust" among federation members by vetting candidate organizations and their representatives.
- Site Administrator (SA) - an individual who is responsible for submitting an organization's MD to the Federation Operator.
- Delegated Site Administrator (DSA) - an individual who can submit MD to a Site Administrator for submission to the Federation Operator.
- Federation Operator (FO) - the organization responsible for managing the services offered by the Federation, operating a service infrastructure supporting real-time transactions among participants, overseeing compliance audits of Federation participants, and maintaining records, documents and other resources of the Federation.

Processes

- Submit agreement - Initiate a legal agreement between InCommon and the RO or the Regional.
- Process agreement - Process a submitted agreement
- Process billing - Set up initial and ongoing billing
- Vet exec & SA - Verify the identities of a Represented Organization's executive and *Site Administrator (SA)* contacts
- Vet organization - Verify the legal standing and domain ownership of a Represented Organization
- SA submits MD - Submission of metadata (MD) by a *Site Administrator (SA)*. This submission may create a new entity in the federation, modify an existing entity, or remove

an entity. It may be a direct submission by the SA or approval of an earlier submission by a DSA.

- DSA submits MD Submission of *Metadata (MD)* by a *Delegated Site Administrator (DSA)*. This submission may create a new entity in the federation, modify an existing entity, or remove an entity. Submissions by DSAs must be approved by SAs.
- Auto-validate MD - Automated validation of a metadata submission by the web service used by SAs and DSAs.
- Manually-validate MD - Manual inspection of metadata submissions for checks that cannot be automated.