Social-to-SAML Gateway FAQ

InCommon has launched a Social-to-SAML Gateway as a pilot project.

Frequently Asked Questions:

The Social-to-SAML Gateway Project

What are the goals of the Project?

This project is an experiment to test the need for Social-to-SAML gateway, which allows identities from outside the InCommon Federation to access Federation-based services. It also will help us:

- expand the value of the Federated Identity user experience
- explore the issues created by using a variety of social identity providers in a federated context
- enhance our understanding about policy differences between an assertion from a campus IdP and from a social IdP

There has been considerable discussion about how to operate a trust fabric containing different types of identity providers; this project is a first step to learn about the issues that will arise in that kind of environment. There is interest in exploring ways that the functionality of the current lightweight implementation could be extended to provide "identity augmentation" functionality.

What is this Gateway? Why might I be interested in it?

Using a gateway broadens the set of people who can access a SAML-protected resource. Normally, only community members from campuses running a SAML IdP would be able to access these resources; using the gateway opens access to include anyone who can authenticate at one of the social identity providers. Applications that are already SAML-enabled can accept SAML assertions from the Social-to-SAML gateway. These assertions would represent people who authenticated at one of the social identity providers.

Social identity providers typically support non-SAML protocols. The gateway accepts assertions via a non-SAML protocol and then constructs a SAML assertion containing identifiers and attributes that a SAML-enabled service can understand. SAML-enabled applications can accept SAML assertions from a gateway in the same way that they accept assertions from SAML IdPs. Indeed, the gateway **is** a SAML IdP.

Accepting users who authenticate through a social identity provider relieves campuses of the burden of maintaining a potentially large set of user accounts for 'loosely associated' affiliates at the institution.

Why is this called a pilot?

This is an experiment. It is not a production service offered by InCommon. It is a pilot being offered by the University of Texas System, in partnership with InCommon. It starts October 1, 2012; during Q1 2013 we will assess the usage and determine next steps. The gateway may be shut down (during summer 2013) or it may evolve to become a real service. It may be made available as a download package that campuses can install locally.

Currently, the SLA terms for the gateway are strictly "normal business hours, central time zone". Normally issues and problems will be addressed within one business day.

Will the pilot end? If so, when?

Yes, it will definitely end; it will not be a perpetual, open-ended pilot. An assessment during Q1 2013 will determine next steps.

What are the terms of use for the Gateway?

There are no guarantees of any sort. Period.

How do I provide feedback?

To report issues or bugs, suggest additional features, or to outline your use case, fill out the Social-to-SAML Feedback Form. Use case descriptions will be used as input to the pilot assessment.

Using the Gateway

What would using this Gateway look like to browser users ?

There is a set of demo sites available here. The entry for each of the supported social providers includes a clickable link to demonstrate the user experience.

How can I use the Gateway with my application?

To use the gateway, the application owner must decide which social providers s/he is willing to accept as authentication sources. In addition, the site hosting the application (or the application itself) will need an extensible Discovery Service so that browser users can identify their Home Organization (presumably a member of InCommon) and/or one or more social providers.

There are many different ways that a site could configure an SP to use the Social-to-SAML Gateway. To keep things straightforward and simple, here is a description of one way to do this:

1. Install the Shibboleth SP or use an existing deployment.
2. Install the Discovery Service component bundled with the SP.
3. Make sure the SP is a member of the InCommon Federation, adding it to InCommon metadata if necessary. (This is because the Gateway consumes InCommon metadata.)
4. Choose which social providers you want to use. (A list of supported social providers is given on the Social-to-SAML Gateway Demo page.)
5. Configure the SP to load metadata for the chosen social providers. (Metadata files are linked on the Social-to-SAML Gateway Demo page.)
6. Configure the SP (and possibly the application) to consume the attributes provided by the chosen social providers. (In particular, some social providers assert long, opaque identifiers.)

If you have questions or problems, please post them on the mailing list.

Which social identity providers does the Gateway support?

A list of social identity providers supported by the gateway is available.

Is Gateway metadata included in the InCommon metadata aggregate?

No. Since this is a pilot, it was decided not to include gateway metadata in the aggregate, at least not at this time. To use the gateway, a service manually configures gateway metadata into its SAML software (usually Shibboleth, but not necessarily).

Does the Gateway provide a unique identifier for each person?

Yes, the gateway asserts an `eduPersonPrincipalName` (`ePPN`) and a SAML2 Persistent NameID for each user. (The content of the Persistent NameID is identical to the content of the `eduPersonTargetedID` attribute.) Relying parties trust these identifiers at their own risk.

The `ePPN` asserted by the gateway for a particular user is the same for all downstream SPs. (We say that the `ePPN` is "scoped to the Federation.") This is because a social IdP sees the gateway as a single app and knows nothing about the downstream apps.

The SAML2 Persistent NameID asserted by the gateway for a particular user is unique per SP. The NameID is computed from the `ePPN` and the SP entity ID (which is why the NameID is unique per SP). Note that this NameID is not stored (since the gateway is stateless) and therefore the identifier is not revocable.

For a sample of the attributes asserted by the gateway for each social IdP, run the corresponding test SP for that IdP.

Does the Gateway provide other attributes and values?

The provided attribute values will vary from one social identity provider to another. This page (link?) summarizes what each social identity provider asserts. Minimally, though, an application will always get an `eduPersonPrincipalName` value.

How do I know if the person name asserted by a social IdP (if any) is correct?

To our knowledge, there is no social IdP that makes claims about the veracity of person names. Even a certified LoA-1 IdP (social or otherwise) makes no such claims.

That said, some social IdPs (such as PayPal) and many InCommon IdPs have identity-proofed *some fraction* of their users at *some level of assurance* (LoA). We do not, however, have any mechanism in widespread use today that permits IdPs to make such claims. Therefore a relying party must make its own determination regarding this aspect of LoA, on either a per-IdP or per-user or per-transaction basis, in whatever manner best satisfies its assurance requirements.

Could I run a version of the Gateway locally, at my campus?

Yes. Here's how to obtain instructions (link?). Some campuses have already expressed an interest in enhancements including:

- invitations
- storing state about browser users in an LDAP directory local to the gateway
- augmenting identity by storing and managing additional attributes on those user objects (e.g., permissions)

Further Considerations

Is the Gateway approach suitable for every application?

Probably not. Many campus-based applications rely on campuses to do some checking to ensure that the digital identity of "Jane Doe" is, in fact, issued to the real Jane Doe. With social identities, usually there is no such checking. Applications that rely on such identity vetting (e.g., applications supporting courses that issue grades) probably should not use this Gateway. However, there are lots of campus-based applications that do not require this level of identity vetting (e.g., applications supporting collaborative work). It is STRONGLY RECOMMENDED that each service evaluate whether using the gateway creates an unacceptable risk for that service. As noted, however, many services will conclude that they are not facing any additional risk.

Are there any legal issues for a service provider if it uses the Gateway?

The operator of the gateway assumes no responsibility for anything. Both the browser user and an SP site using the gateway are on notice that they have no expectation of privacy, and no legal rights. Each SP using the Gateway must determine its own responsibilities.

What is the level of assurance associated with the Gateway?

The gateway does not assert any LoA value (unspecified); it just passes through the attributes that the social identity provider has provided. Nothing can be said about the trustworthiness of the attributes, which are not covered by any federation policy.

A handful of social identity providers are certified by OIX to be US ICAM LOA 1 Certified Identity Providers. (Like InCommon, OIX is an ICAM-approved Trust Framework Provider.) For example, Google and PayPal are certified LoA-1 identity providers supported by the gateway.

In particular, Google is known to assert the ICAM LOA 1 policy URI **by default**, in response to **all** authentication requests. However, the gateway is not currently configured to capture this URI and echo it in the SAML response asserted downstream (since that would require just-in-time validation of the claimed LoA). Thus service providers make determinations regarding LoA on a per-transaction basis at their own risk.

Does the Gateway store any information about who is using it?

The Phase 1 implementation is intentionally lightweight. The gateway maintains NO state information about the browser users who use it. It does maintain log files so we can get some sense of which applications are relying on the gateway.