InCommon – The Reality with Workday

Workday has been asked by multiple customers to consider joining the InCommon federation, a renowned Identity Management Federation serving customers in the Education and Government sector and their partners.

We have researched InCommon and its benefits for both Workday as a company and for our customers, and here we summarize our findings.

The Use Case for InCommon

I am a Security Administrator at Company X. Users at my company use SAML to access applications from multiple different companies. To set this up, Company X, technically Company X's Identity Provider (IdP), has to exchange its SAML metadata (setup data necessary to configure SAML) with each company.

This poses a problem as the number of businesses Company X works with grows. Manually exchanging and performing updates of SAML metadata becomes tedious. Often, individual companies have different:

- Requirements for the type of SAML metadata to exchange.
- Processes for exchanging SAML metadata.

This results in delays and possible mistakes when Company X deploys an update of its SAML metadata (because of security risks or updates).

This problem exists in reverse as well. If Workday has hundreds of customers allowing their users to sign in to Workday using SAML, Workday needs to provide and update its SAML Service Provider (SP) metadata hundreds of times.

How Can InCommon Help?

InCommon reduces to 1 the number of times you have to deploy your SAML metadata no matter how many business applications you use. InCommon also acts as an intermediary to host the data.

Example: Assuming your company and all your business applications are InCommon participants, Company X only has to submit its IdP SAML metadata to InCommon once. InCommon acts as the middleman from which the rest of Company X's business applications can pull Company X's IdP metadata on a recurring basis (recommended hourly). This also applies when Workday deploys updated SP metadata to all its customers that use SAML to sign in to Workday.

InCommon also requires:

- All participants to provide the same format of SAML metadata so the requesting applications know what to expect.

- Participants to submit their SAML metadata to the InCommon databases via an InCommon web application.
- Each company's SAML metadata to be signed with InCommon's private key, and verified with a given public key when the partner software system retrieves the data in XML format.

Workday's Unique Situation

Scenario 1: Updates to Workday's SP Metadata

Each Workday customer uses a copy of the Workday software that holds the customer's specific set of sensitive data. The customer owns and maintains this data.

In the use case for InCommon in which a company is using multiple services, or a service has multiple customers, Company X is the customer, and Workday is the service.

In reality, Company X remains our customer, but the service is Company X's owned instance of Workday. So the number of customers using Company X's Workday instance is one – Company X only.

In this case, InCommon would provide only Company X, not Workday, with access to InCommon to maintain its Workday instance's SAML SP Metadata. InCommon doesn't provide web services for a third party to update this data, so the Company X administrator would be responsible for making these changes manually in InCommon.

This means that an administrator from Company X is responsible for producing and exchanging the metadata for both Company X and Company X's Workday instance. Therefore, the administrator is responsible for manually updating Company X's:

- IdP metadata in InCommon.
- IdP metadata in the Workday application.
- Workday instance's SP metadata in InCommon.
- Workday instance's SP metadata in the Workday application.

Company X could maintain a seamless update process with other InCommon participants that it's partnered with, but would need to manually maintain the exchange of data for its Workday instance.

<u>Since the customer is responsible for making changes to their data in two places – in their instance of Workday and in their instance of InCommon – it isn't beneficial for Workday to join InCommon.</u>

Scenario 2: Updates to Company X's IdP Metadata

Workday's service currently requires customers to submit their SAML metadata in Workday via a task in the user interface. Workday also lets customers set up different IdP configurations for different environments, and use multiple IdPs in the same tenant for the same environment. When configuring IdPs in Workday, customers also consider:

- Which Workday instances an IdP configuration is active for.
- If an IdP is used in preview environments only.
- If an IdP is active.

This enables our customers to have more control over how users sign in to their different instances of Workday. Some of these instances are meant to preview upcoming Workday changes, and some are meant only for a certain set of users.

So if Company X makes changes to their IdP metadata in InCommon, Workday would need to make decisions on behalf of the customer on which IdP configuration to update in their Workday instance. Workday would need to decide if:

- Active IdPs should be changed.
- Inactive IdPs that match the Issuer ID should not be changed.

More specifically, the Workday service would only pull in a few fields from Company X's IdP metadata from InCommon:

- Identity Provider Name
- Issuer ID
- Public key
- Logout Request/Response URLs.

Then Workday needs to massage this data to apply and activate the changes in the correct environment.

In this case, if Company X's Workday instance receives Company X updates, and if Workday allows the data to be changed programmatically, then Workday's software would decide on a set of the Workday instance's tenants to update IdP metadata for. This means that Workday is manipulating customer data, which Workday can't do today. This would require:

- Explicit consent from Company X for every update, and changes to Company X's legal contract with Workday, clarifying that Company X is directing every action.
- Workday's Legal division to review and approve this process, and Workday to become partners with InCommon.

Additionally, Company X must be aware of the potential risks of using InCommon. InCommon currently publishes the metadata changes in a public facing XML file. This file is signed using InCommon's private key. Workday would catch a corruption caused in transit by verifying the signature on the metadata. However, a corrupted

file or bad metadata caused by an InCommon breach would not be caught by Workday and could immediately impact user sign in.

In this scenario, it would be possible for the Workday instance to accept the incoming changes, and wait on manual approval before deploying the updates. But it eliminates the main benefit of joining InCommon – the ability to automatically deploy updates to all partners at the same time, *without* additional manual work.

Conclusion

Our customers own their SP metadata for their Workday instance. Even though it's stored in a Workday instance, Workday doesn't own it and will not deploy it to InCommon on the customer's behalf.

After consulting with the advisory board of InCommon about our specific situation, together we have concluded that it isn't beneficial to any party for Workday to join InCommon. Doing so doesn't relieve the customer of manual work to enable SAML, because Workday inherently requires additional configuration from the customer intended to secure their data.

Workday does plan to develop a method for customers to export their SP metadata, from Workday in an XML format, making it easier for the customer's IdP to automatically consume it.