InCommon Service Provider Onboarding - Primer Document (Draft)

DRAFT v1, August 2018

Document Title: InCommon Service Provider Onboarding - Primer Document
Document Repository ID: TI.96.1
DOI: 10.26869/TI.96.1
Persistent URL: http://doi.org/10.26869/TI.96.1
Authors: InCommon Streamlining SP Onboarding Working Group
Publication Date: August 2018
Sponsor: InCommon TAC

Table of Contents

1. Introduction

Single Sign-On (SSO) authentication uses technologies such as Security Assertion Markup Language (SAML) to ease user management and user experience for a wide range of services. In order to work correctly however, SAML depends upon the secure and effective exchange of keys and other information contained in metadata. Such exchanges can pose a burden for administrators. Failure to update metadata results in downtime and support calls. In addition, metadata exchanged in an insecure manner may result in security breaches and theft of sensitive information.

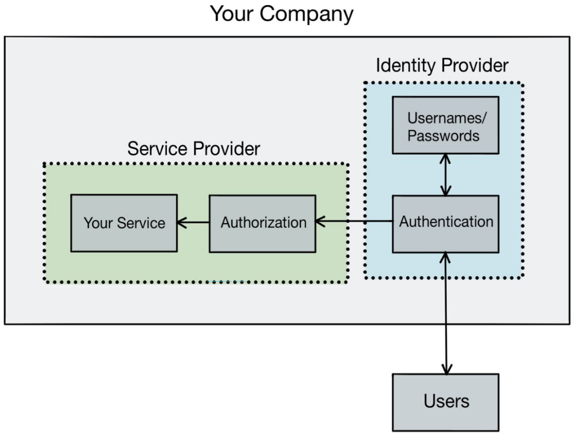
Fortunately, joining a federation such as InCommon can greatly relieve the support burden associated with exchanging this metadata by addressing the security as well as the manual processes of changing and updating metadata. This Primer explains both SAML basics, as well as how InCommon can ease the use of SAML support for your organization.

2. SAML Basics

How does SSO (using SAML) ease user management? Simply put, SSO enables companies to be free from the work of managing customer user accounts and passwords. Your customers will run an Identity Provider (IDP), while you will run a Service Provider (SP) that can accept SAML assertions for authentication. You can then delegate all user password and account issues to the Identity Provider.

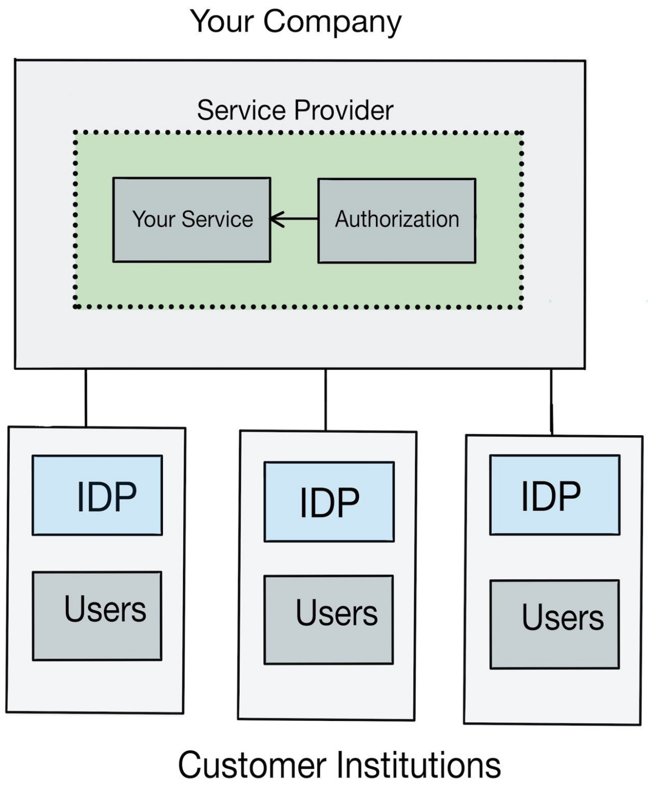
A Traditional Non-Federated Environment

Here's a diagram of a traditional environment. Your service consists of authorizing users, plus providing a service (labeled as Service Provider below). In addition, you must also provide authentication, keeping up, maintaining and securing User IDs and passwords for every user:



A Federated Environment

In a federation SAML environment, the user management burden is shifted to the individual schools or institutions, moving the identity provider aspect out of your organization:

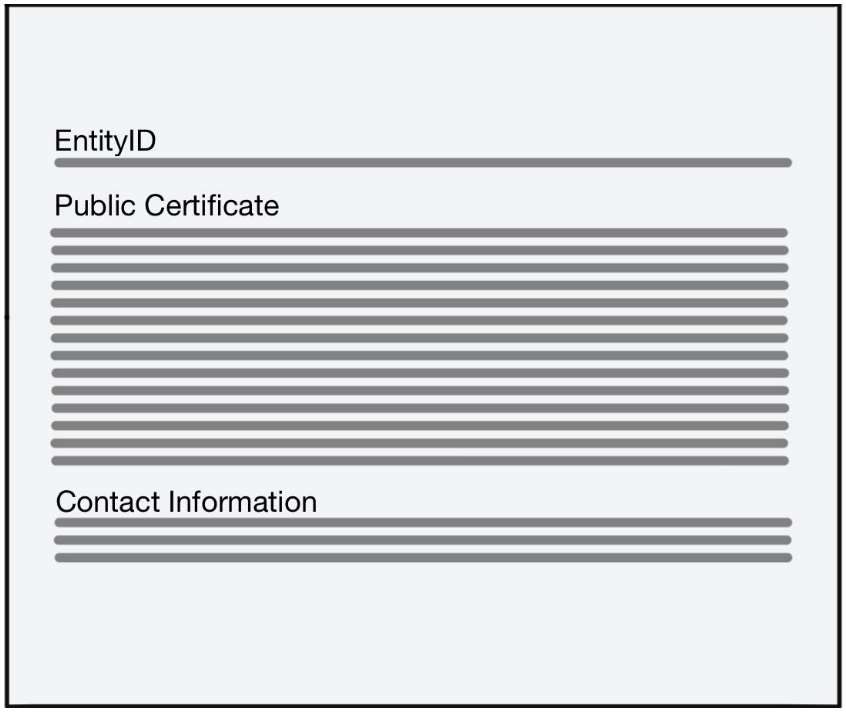


This takes your company out of the password management business, shifting that burden to the user's institutions. You no longer need to store or secure user passwords. When users do have password issues, they call their institution, not you. Provisioning and deprovisioning users is now up to your customers, freeing you from that responsibility.

However, in order for SAML to work properly, you must exchange server information, or metadata with every institution you plan to work with to use SAML.

3. Federated Metadata Basics

Why exchange metadata? SAML does not function properly without servers knowing about one another's key pairs. The metadata includes minimal information about your Service Provider, such as its public key, its endpoints and other information:

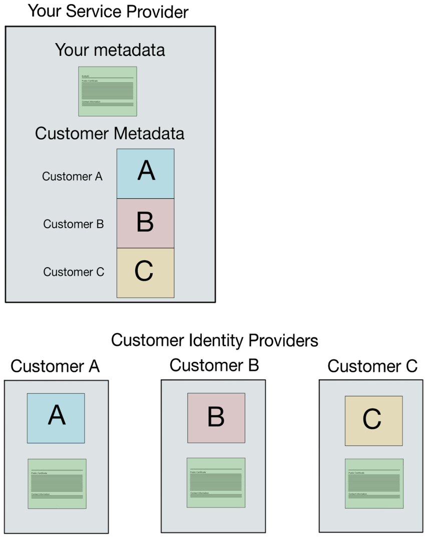


For community metadata examples, please see:
https://incommon.org/federation/info/all-entities.html

How are the key pairs* used in the metadata?

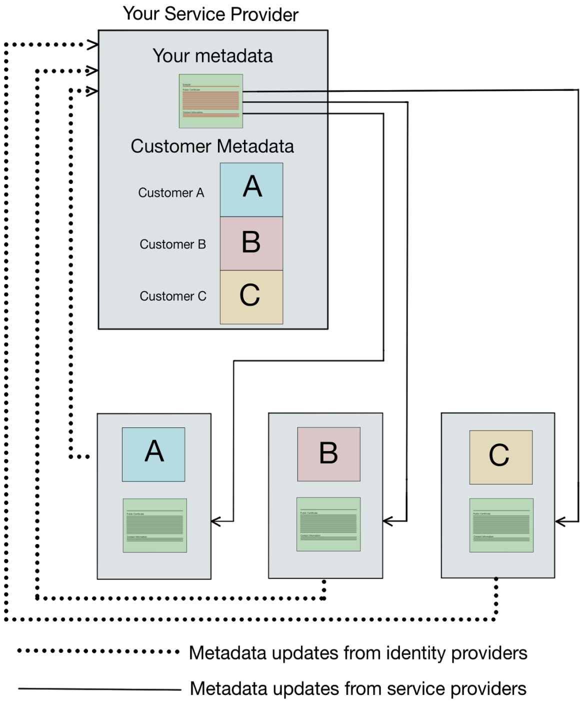
1. Service Provider - Authentication Request
    a. The Service Provider digitally signs their Authentication Request using their private key. When the Identity Provider receives this Authentication Request, they are able to verify the signature by using the **Service Provider's public key*** from the metadata file; the Identity Provider can then verify the Service Provider is who they say they are.
    b. Optionally, the Service Provider can use the **Identity Provider's public key*** in the metadata file, to optionally encrypt the Authentication Request.
2. Identity Provider - Authentication Response
    a. The Identity Provider digitally signs their Authentication Response using their private key. When the Service Provider receives this Authentication Response, they are able to verify the signature by using the **Identity Provider's public key*** from the metadata file; the Service Provider can then verify the response came from the trusted Identity Provider.
    b. Optionally, the Identity Provider can use the **Service Provider's public key** in the metadata file, to encrypt the Authentication Response. The Service Provider is then able to decrypt this response by using their private key.

Isn't it a pain to distribute metadata to and from all my customers? Yes, and it makes change control more difficult. You will also need to manage and update metadata for each and every customer you have. They will each have a copy of your metadata, and you will have a copy of their metadata:



When you change your (SP) metadata, or your keys for any reason, you will need to send that updated metadata to each customer (IDP), and ask them to load it into their Identity Provider. This is what we call a bilateral trust, and is a manual process. If any customer fails to update the appropriate metadata, their service will cease to work properly, causing an outage for those users.

Likewise, if the customer (IDP) has any changes to their metadata, they in turn must notify the Service Providers (SP) and send them the appropriate metadata and often get confirmation they've imported the changes. The dotted lines above show the flow of metadata from Identity Providers to the Service Providers.



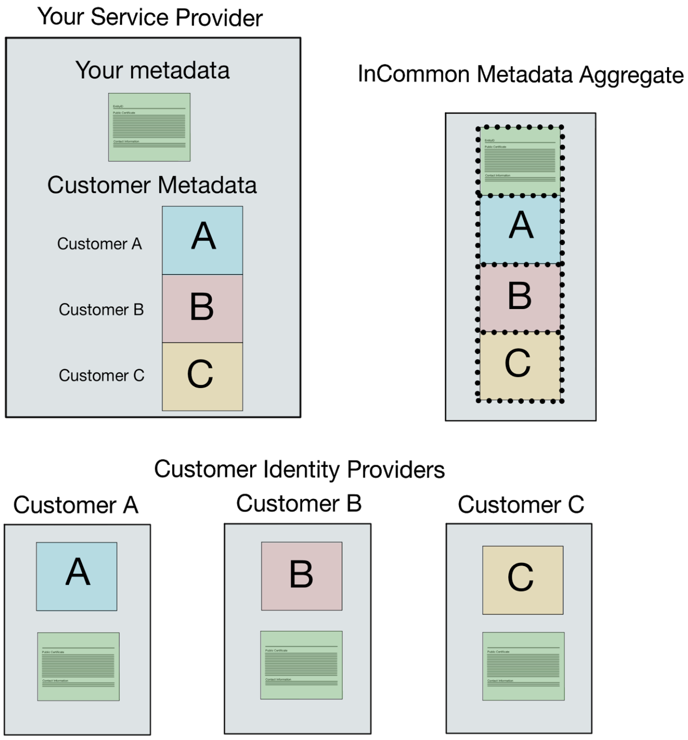
Are manual metadata exchanges are risky or difficult? Manually updating metadata when you have one or two customers may not seem like a burden, but as your customer base expands to dozens or hundreds it can become a huge problem. Not only can it be a time-consuming affair, if not done quickly and properly the inevitable result is unplanned downtime for your service.

Securely exchanging metadata can also be a problem. How can you be sure that you're getting the correct copy? Phishing and other scams eliminate email as a secure mechanism. Downloading the metadata directly from the site is not secure either. As with SSL certs, the only secure manner to trust metadata is with a trusted third party, which is what InCommon provides.

InCommon can make this process easier and more secure.

4. Federated Identity with InCommon

InCommon is a group of research and higher education organizations and partners who agree to exchange server metadata in a more efficient model. It allows you and your customers to retrieve one another's metadata in a secure and automated manner. The dotted lines within the aggregate indicate the metadata stored within the aggregate are copies.



The federation eases distribution of your metadata changes

There are several circumstances when you may need to change your metadata. When keys expire, you'll need to update your keys within your metadata, and then all of your customers will also need that metadata with the updated keys. Updating your metadata, then manually contacting dozens (if not hundreds) of customers and waiting for them to respond by making manual changes is difficult and not effective or secure. With InCommon, you simply need to make the change, upload it to the InCommon Aggregate, and your customers will be updated automatically.

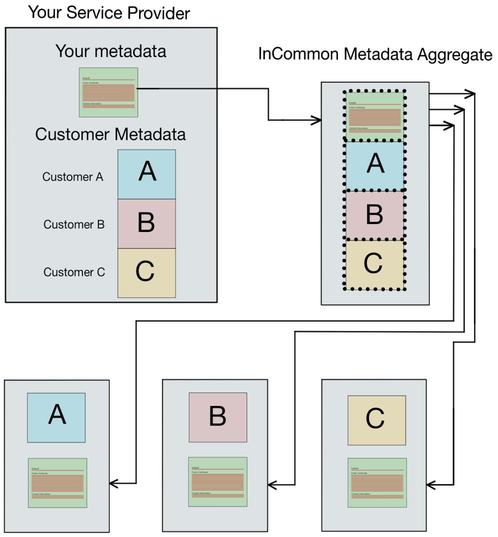
Other times may be more urgent, for example when

- Compromised keys that must be changed immediately. Any failure by any customer to update metadata will result in an outage for customers. With InCommon it is an automatic process.

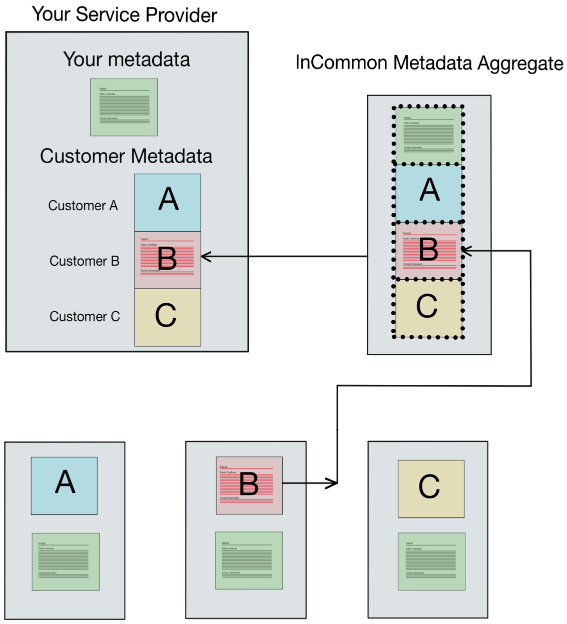
Some changes won't be urgent, but are still important.

- Information such security contacts or administrator contacts need to be updated. InCommon makes this easier on all parties involved.
- Changes to endpoint information.

Regardless of the metadata change needed, with InCommon you have only one step to take: upload your new metadata to the Incommon metadata aggregate. Your customers should automatically download and install the changes. As the diagram below shows, the updated metadata is automatically distributed to your customers.



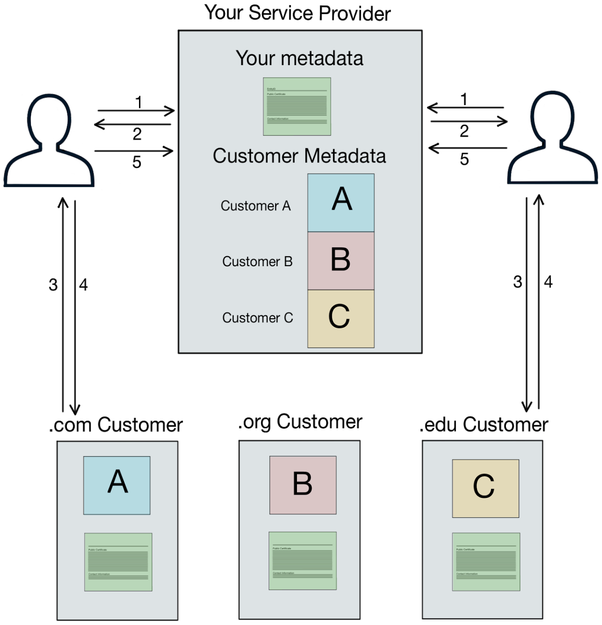
Likewise, the diagram below demonstrates the mechanism for a customer to make changes. In this case, Customer B needs to update contact and protocol information in their metadata. They merely need to upload their updated metadata copy to the Incommon Metadata Aggregate and the change will be automatically incorporated within your service provider. This saves time that would otherwise be spent coordinating and installing changes.



5. Federated Login Process with InCommon

The InCommon process involves metadata exchange, so the login process itself is the same process used in most non-federated environments. InCommon is not involved in the login process itself, only the metadata exchanges that make the SAML login process possible.

How does the login process work after I'm in InCommon?



The user generally logins in the following way:

1. User goes to your site
2. Your site redirects the user to the user's home identity provider
3. The user authenticates to the identity provider
4. The identity provider then generates a SAML assertion for the user
5. And the user passes that onto your service provider, where authorization takes place.

While there are sometimes other mechanisms in play, *InCommon is not involved in the login process.*

How do I keep track or identify users coming from so many different places? The Identity Providers will send you pre-defined attributes for users so you can know what to expect to identify and authorize your users as necessary. After a user authenticates via their Identity Provider, attributes for that user are sent to your Service Provider:

Attribute Name	Attribute Value
eduPersonUniqueID *	smith2748@univ.edu
eduPersonPrincipalName * †	j.smith@univ.edu
eduPersonTargetedID * †	d26543fhTiM
displayName * †	John Smith
givenName †	John
sn †	Smith
mail †	j.smith@univ.edu
eduPersonScopedAffiliation †	student@univ.edu
eduPersonEntitlement	urn:mace:univ.edu:dept:csi

Identifier Attributes

Personal Attributes

Authorization Attributes

* Not to be confused with the e-mail attribute.

† Research and Scholarship attributes

6. Joining InCommon - Summary

Easier administration. InCommon provides an automatic update for metadata changes, easing the time and administrative burden for Service Providers. It allows InCommon Partners to access resources without the need for continual central IT configuration.

Secure exchange of metadata. The compromise of an organization's SP (or IdP) does not breach the security of the SAML protocol exchanges used throughout the InCommon Federation. Through Participants consuming, regularly refreshing, and verifying the InCommon metadata aggregate, the Federation's framework remains trustworthy.

Improved scalability. When adding new InCommon customers, there's no need to distribute your metadata. You can simply point them to the InCommon Aggregate.