# Identity Provider Operator's Guide

For federated Identity Providers to interact with Internet2 Identity Services, It will require the Identity Provider to be configured as shown in the 'Service Details' section below. This will automatically happen if the Identity Provider is supporting the Research & Scholarship category.

We support the SAML2 deployment profile for federation interoperability from Kantara, described here: https://kantarainitiative.github.io/SAMLprofiles/saml2int.html.

## Identity Services SP Service Details

SAML EntityID: https://login.at.internet2.edu/Saml2/proxy_saml2_backend.xml

| Friendly Name | SAML Attribute Name | Required? |
|---|---|---|
| eduPersonPrincipalName (ePPN) | urn:oid:1.3.6.1.4.1.5923.1.1.1.6 | Yes |
| mail | urn:oid:0.9.2342.19200300.100.1.3 | Yes |
| displayName | urn:oid:2.16.840.1.113730.3.1.241 | Yes* |
| givenName | urn:oid:2.5.4.42 | Yes* |
| sn (surname) | urn:oid:2.5.4.4 | Yes* |
| affiliation (scoped) | urn:oid:1.3.6.1.4.1.5923.1.1.1.9 | No |

**NOTE:** This service requires signed **responses** and will reject assertions where only the assertion itself is signed. This is to help mitigate against signature wrapping attacks and is in compliance with the "SAML V2.0 Implementation Profile for Federation Interoperability" standard published here (specification IIP-SP13).
* Some form of name must be sent. The displayName attribute will be used if it is sent. Otherwise, givenName and sn must be sent and will be concatenated to form the 'Name'.

## Is your organization in the InCommon federation?

You can look up your home organization here to see what its current status is. The presence of the 'Federation' tag will indicate that you have an IdP in the federation.
You can learn more about joining the InCommon Federation here.

## See What You are Releasing

If you'd like to see the attributes Identity Services is receiving from your Identity Provider, use this page to choose your identity provider and you will be directed to a page showing that information.

## Research & Scholarship

This service uses Research & Scholarship entity category.
We encourage you to take this opportunity to support the Research & Scholarship (R&S) entity category. When you support R&S, you release the attribute bundle to the entire category of Service Providers (which are vetted by InCommon or one of our sister federations that are part of eduGAIN).

The R&S attribute bundle includes the following required data elements.

- *shared user identifier*
- *person name*
- *email address*

and one optional data element:

- *affiliation*

For more information, see item #5 on the R&S entity category description.

There is a wiki page that provides detailed information and instructions on how to configure your IdP to release the R&S attributes to all R&S Service Providers.

## Understanding WAYF

We use a 'Where-are-you-from' service that includes multiple federations. To understand more about this, please read the Challenges in Federated WAYF Services white paper.

## Troubleshooting

- If you are receiving an error, "**opensaml::FatalProfileException**", this is regularly caused by a few issues.
    - It can be caused by the IdP not signing the SAML responses. Please refer to the "**NOTE**" segment in the Identity Services SP Service Details section above. Other causes for this error are unverifiable signatures and invalidly formatted assertions.
    - It can be caused by the 'SubjectConfirmationData Address' in the '<saml:Subject>' to be set to a non IP address value.