# Attribute-based Policy Config

## Attribute-based Policy Configuration at Scale

Today administrators of identity provider (IdP) middleware in the InCommon Federation configure attribute release policy based on the identity (entityID) of service providers (SPs). I'm happy to say those days are numbered. A new approach to user attribute release based on entity attributes has arrived. This new technique promises to scale better, by relieving administrators from the burden of having to rely on policy files that are inherently difficult to maintain.

This idea isn't new. Access control based on user attributes (as opposed to user identifiers) remains the holy grail of identity and access management systems throughout the enterprise. Unfortunately, federation has only made this problem worse, not better.

At the level of the federation entity (i.e., the IdP or the SP), the stars have aligned so that policy based on entity attributes is a reality:

- A SAML V2.0 Metadata Extension for Entity Attributes already exists and is being deployed around the world as we speak.
- SAML middleware increasingly supports entity attributes at both the IdP and the SP, and at the discovery service as well. Shibboleth is leading the way in this area. The Shibboleth IdP, for instance, has supported entity attributes since v2.3.4.
- Federation operators everywhere are beginning to decorate entity descriptors in SAML metadata with entity attributes of significant value.

The Research & Scholarship (R&S) Category in the InCommon Federation is an initial effort along these lines. To support R&S, IdP administrators configure for attribute release once, for all R&S SPs, both present and future.

The kicker, however, will most certainly be *self-asserted entity attributes*. Once administrators are able to tag their metadata with arbitrary entity attributes, they will certainly do so in unique and interesting ways. In the same way metadata tagging has been found to increase the value of other types of information (research papers, blog articles, photographs, etc.), self-asserted entity attributes will cause the information content of SAML metadata to skyrocket.

The sooner we get there, the better.