Research and Scholarship Attribute Bundle

Research & Scholarship Attribute Bundle

Identity providers are encouraged to release the *R&S attribute bundle* to all R&S service providers:

> Configure your IdP to release the R&S attribute bundle now!

- *Identifiers*
  - `eduPersonPrincipalName`
  - `eduPersonTargetedID`
- *Mail attribute*
  - `mail`
- *Person name attributes*
  - `displayName`
  - `givenName`
  - `sn` (surname)
- *Authorization attribute*
  - `eduPersonScopedAffiliation`

It is easy to configure a Shibboleth IdP to release the R&S attribute bundle to all R&S SPs. If, however, you are using SAML software that does not support entity attributes, consider releasing the Essential Attribute Bundle to all SPs instead.

> **Supporting the Research & Scholarship Category**
>
> An identity provider (IdP) supports the Research & Scholarship (R&S) Category if, for some subset of the IdP's user population, the IdP releases a minimal subset of the R&S attribute bundle to R&S service providers without administrative involvement, either automatically or subject to user consent.

Minimal Subset of the R&S Attribute Bundle

The following attributes constitute a *minimal subset of the R&S attribute bundle*:

- `eduPersonPrincipalName`
- `mail`
- `displayName` OR (`givenName` AND `sn`)

For the purposes of access control, a *non-reassigned persistent identifier* is REQUIRED. If your deployment of `eduPersonPrincipalName` is non-reassigned, it will suffice. Otherwise you MUST release `eduPersonTargetedID` (which is non-reassigned by definition) in addition to `eduPersonPrincipalName`. In any case, release of both identifiers is RECOMMENDED.

An Optimization

A sufficiently capable IdP deployment can optimize attribute release based on the `<md:RequestedAttribute>` elements in SP metadata:

- If a service provider lists the `eduPersonPrincipalName` attribute in metadata, and the IdP's deployment of `eduPersonPrincipalName` can be reassigned, then the IdP MUST release both `eduPersonPrincipalName` and `eduPersonTargetedID` to the SP regardless of whether `eduPersonTargetedID` is listed in metadata.
- If a service provider lists **any** of the person name attributes in metadata, the identity provider MUST release some form of person name, either `displayName` or `givenName` + `sn`.

Beyond the two special cases noted above, *an identity provider is NOT REQUIRED to release any attribute not listed in metadata*.