

eduPersonTargetedID



Use of the `eduPersonTargetedID` attribute – **as well as SAML 2.0 persistent NameIDs in general** – should be phased out and replaced with the `pairwise-id` attribute from the [OASIS SAML 2.0 SubjectID Attributes Profile](#).

The content (attribute value) of the `eduPersonTargetedID` attribute is defined to be a SAML 2.0 persistent NameID (cf. [MACE-Dir SAML Attribute Profiles](#), section 3.3.1.1, lines 390-393), i.e., an XML structure. Abstractly it's a 3-tuple made up of the IDP's entityID, the SP's entityID and the subject-specific part. It could be called a "service-specific pseudonym" in that it's an opaque identifier that differs for each service a subject is accessing.

Deprecation

The `eduPersonTargetedID` SAML Attribute has officially been [deprecated](#). No new deployments should be making use of this attribute and any existing deployments should make plans to migrate to the SAML `pairwise-id` attribute. The new replacement attribute is simpler and therefore preferable in all regards: It's a simple attribute with simple string values (instead of a complex XML data structure), it has a single, consistent way of requirements signalling from the Service Provider and a single, consistent on-the-wire representation. It is also defined in an official OASIS SAML 2.0 Profile, not merely part of a community "standard" (`eduPerson`), and not specific to *edu-anything*. So transitioning to the `pairwise-id` SAML attribute should be started ASAP.

This deprecation should come as no surprise to anyone as the `eduPersonTargetedID` SAML Attribute – as container for persistent NameIDs – was essentially obsoleted in 2005 🚩 when SAML 2.0 defined a standard method to send this same data structure in the `Subject` element of the SAML Assertion.

Issues

- All forms of `eduPersonTargetedID` attribute **as well as all forms of the SAML 2.0 persistent NameID itself** suffer from a *case folding* issue (when using base64 encoding) that may lead to identifier collisions at Service Providers not treating identifiers as case-sensitive. Consider this an informal Security Advisory against any use of this attribute (or persistent NameIDs in general).
- [saml2int](#) – the Interoperable SAML 2.0 Deployment Profile, a normative part of eduID.at via the [SAML WebSSO Technology Profile](#) – states in Version 0.2 that persistent NameIDs should be transmitted in the `Subject` of the SAML Assertion, **not** as an `eduPersonTargetedID` Attribute (value). So use of `eduPersonTargetedID` within eduID.at actually constitutes a formal policy violation.
- Also note that the new version of [saml2int](#) goes much further and states that:

SPs MAY support legacy or historical `<saml:NameID>` and `<saml:Attribute>` identifier content for compatibility reasons but MUST NOT require their use.