eduPersonUniqueID

⊘ Use of the `eduPersonUniqueID` attribute should be phased out and replaced with the `subject-id` attribute from the OASIS SAML 2.0 SubjectID Attributes Profile.

Issues

- The eduPersonUniqueID attribute suffers from a *case folding* issue (due to allowing use of both upper and lower case characters) that may lead to identifier collisions at Service Providers not treating identifiers case-insensitively. Consider this an informal Security Advisory against any use of this attribute.
- Also note that newer versions of saml2int – which is a formal part of the eduID.at policy via the Technical Profile – go much farther and state that:

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