Guide: eduPersonPrincipalName (ePPN)

eduPersonPrincipalName

This guide is intended to give you some ideas about how to generate an eduPersonPrincipalName (ePPN) for users.

Video

You can find a video introduction to ePPN on Skolfederation's YouTube channel here (in Swedish).

eduPerson

eduPersonPrincipalName is defined in eduPerson 1.0, OID:1.3.6.1.4.1.5923.1.1.1.6
A scoped identifier for a person. It should be represented in the form "user@scope" where 'user' is a name-based identifier for the person and where the "scope" portion MUST be the administrative domain of the identity system where the identifier was created and assigned. Each value of 'scope' defines a namespace within which the assigned identifiers MUST be unique. Given this rule, if two eduPersonPrincipalName (ePPN) values are the same at a given point in time, they refer to the same person. There must be one and only one "@" sign in valid values of eduPersonPrincipalName.

ePPN

In Skolfederation, ePPN must:

- be properly scoped with a domain name owned by the Member Organization.
- uniquely represent a single user.
- never be reassigned.

One way to achieve this is, for example, to use a Base36 alphanumeric number that is stored as a string and padded with zeros on the left for sorting. ePPN is incremented for every new user. If we use a length of 6 (36^6), that gives us 2,176,782,336 ePPNs before overflow occurs. Either append the scope, an owned domain, before storing the ePPN, or do it later, e.g., in the IdP.

Example Scripts

This example shows how you can add the attribute to users by utilizing scripts. The script is built so that it should be possible to run it with a scheduler.

ePPN for Google Workspace on Github
ePPN for Microsoft AD on Github