How to set up attributes and release for the Jisc Certificate Service

This page only applies if you are in the UK Access Management federation *and* your organisation uses the Jisc Certificate service (https://www.jisc.ac.uk/certificate-service)

Once registered with the certificate service your authorised users can sign in using the institutional login. This page will help you set up OpenAthens to enable that - for instructions about using the Sectigo Certificate Manager, see https://support.sectigo.com/Com_KnowledgeProductPage?c=Sectigo_Certificate_Manager_SCM.

As with other resources, we don't know anything about the internal workings of the certificate manager service and can only help you with setting up the attributes and related release policy we've been told it requires.

Minimum requirements

- You will need domain / owner level access to the OpenAthens admin area
- If you use restrictive mode you will need to add this resource to the permission set(s) used by the users you have authorised on the service - you may prefer to create one specifically for those few users and this resource.
- You will need to be able to release some attributes that you would not usually release, such as an email address, so relevant users must have data in those fields
- You have registered for the certificate service via: https://www.jisc.ac.uk/certificate-service

Required attributes

- `urn:oid:1.3.6.1.4.1.5923.1.1.1.6` (eduPersonPrincipalName)
- `urn:oid:0.9.2342.19200300.100.1.3` (email address)

Optional additional attributes

- `urn:oid:2.5.4.42` (first name)
- `urn:oid:2.5.4.4` (last name)

Creating and populating these attributes if they don't already exist

The good news is that you will already have data in at least three of the four fields (email, first and last names). You may already have data in a field you use for eduPersonPrincipalName, but at most you'll need to add something to use for it. The thing where they've got weird-looking attribute names is handled in the release section.

EduPersonPrincipalName (EPPN) is something that looks like an email address, but isn't one. Unfortunately the handy looking email address field is about the only thing we can't reuse for this. What you'll need is either an existing field that has something unique to the user in it, or to create a new one in the schema editor for this - the good news is that the field only needs to be populated for the authorised users of the certificate service.

The following assumes you need to create a new attribute to use for EPPN - if you have a field that isn't an email address you can use such as staff ID number you can move on to the release section

1. Go to Preferences > Schema editor
2. Drag a text attribute into the personal account schema
3. Give it the following details
    a. target name: `urn:oid:1.3.6.1.4.1.5923.1.1.1.6`
    b. display name: `eduPersonPrincipalName`
    c. Options: Releasable
    d. Click Done and then Save changes

Now make sure there is data in that field for each authorised user of the certificate service. It can be firstname.lastname if you like, but anything that is different for each user (and does not contain an '@' character is ok).

The good news is that you may already have data some of the four fields as they include email, first and last names. You may need to add an attribute and a mapping for the other one. The thing where they've got weird attribute names is handled in the release section.

EduPersonPrincipalName is something that looks like an email address, but isn't one. Unfortunately the handy looking email address field is one of the things we can't reuse for this (can't use anything with an '@'). What you'll need is either an existing field that has something unique to the user in it, or to create a new one in the schema editor for this - the good news is that the field only needs to be populated for the authorised users of the certificate service.

As this needs to be released, you will have to set up any schema attributes before adding any mappings:

1. Go to Preferences > Schema editor
2. Drag a text attribute into the personal account schema
3. Give it the following details
    a. target name: `urn:oid:1.3.6.1.4.1.5923.1.1.1.6`
    b. display name: `eduPersonPrincipalName`
    c. Options: Releasable
    d. Click Done and if there are no more to add click Save changes

Repeat the above for any of the other attributes you don't already map to releasable attributes (the minimum other attribute in this case is email address). As they are likely to be used under different names for other services in the future, you may prefer to give them more generic target names such as email, firstname, and so on.

Next you will need to add mappings from your local source to the schema attributes as relevant (since only schema attributes can be releasable):

1. Go to Management > Connections and select the relevant local authentication connector on the left
2. Go to the attributes tab
3. Add rule > add a mapping rule
4. Give it the following details (using eduPersonPrincipalName as the example):
    a. Target name (should find the schema attribute as you start typing): `urn:oid:1.3.6.1.4.1.5923.1.1.1.6`
    b. Local attribute name: as defined in your local source
    c. Display name: eduPersonPrincipalName
    d. Check that there is a tick appearing next to releasable
    e. Click done and if there are no more to add click Save changes

Repeat for any others that you need to map

Release policy updates

As these are not attributes you want to send to everyone, you will need to add a resource specific policy:

1. Go to Preferences > Attribute release
2. Click the 'Add a resource policy' button and search for "Sectigo Certificate Manager"
3. Click on the attributes you want to release - the ones representing emailAddress and EPPN, and optionally First name and Last name
4. Unless you have created them in the schema editor to have the required attribute names you will need to click on advanced and go to the attribute aliases section to release them with the expected names:
    a. In the left hand box select the orginal target name (e.g. emailAddress)
    b. In the right hand box enter the desired target name from the list of required and optional attributes above (e.g. `urn:oid:0.9.2342.19200300.100.1.3`)
5. When you've set them all up click on Done and then Save at the top of the page

Test

You can test at

https://cert-manager.com/customer/JISC/ssocheck/

Troubleshooting

- I mapped an attribute but it's not releasable
    - Either you have not set the schema attribute as releasable in the schema editor or you have not correctly mapped your local attribute to the schema attribute.
        - The schema attribute must exist before you set up the mapping
        - Attribute names are case sensitive
- I get a denied message from the certificate manager or test page
    - Unless it says you you are not registered with them it will be to so with not releasing the required attributes
        - Check that the account has values against the relevant fields
        - Check that the release policy is releasing all the attributes (you must release them as well as adding relevant aliasses)
        - Check the attribute aliases for typos
- I get a denied message from OpenAthens
    - You probably have restrictive mode enabled and have not added the "Sectigo Certificate Manager" to any permission set used by the account