# UK Pathfinder Certification Authority

## Identity Provider Operational Requirements

v0.9  25 May 2017

This document summarises the requirements for an Assent IdP to be connected to the COI for Pathfinder task 3.2.

An organisation running an IdP compliant with these requirements can join the COI.

Why?

- Users can generate internationally trusted certificates - accepted by all international e-infrastructures such as WLCG, PRACE, EGI, OSG, XSEDE, Globus, etc.
- LoA is high enough to give access to other resources, e.g. SCARF

Organisations self-assert compliance with these requirements, but are held legally responsible as members of Assent.

| **Abbr.** | **Expansion/meaning** |
|---|---|
| AP | Authentication Profile |
| COI | Community Of Interest |
| IdM | Identity Management (system), typically a staff/members database managing users' accounts and credentials |
| IdP | Externally facing identity provider (registered in Assent) |
| IGTF | Interoperable Global Trust Federation, www.igtf.net |
| LoA | Level(s) of Assurance |

## Requirements

The authoritative list of requirements is [1], where one should look for entries marked "BIRCH"; this table aims to summarise these plus highlight a few implementation features specific to Pathfinder.  The reference is to the section number in [1].

| **#** | **Ref** | **Requirement** | **Priority** | **Description** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| R1 | AP3.1 | Uniqueness | MUST | Each user presents a unique and persistent id to services |
| R2 | AP3.1 | Traceability | MUST | Records are kept to be able to trace each account to a the user’s real-life identity |
| R3 | AP3.1 | Traceability | MUST | Users can authenticate only while the traceability is retained |
| R4 | AP3.1 | Traceability | SHOULD | IdP should notify the CA when the traceability is lost (see below) |
| R5 | AP3.1 | Identity | MUST | Users MUST have shown official photo id (e.g. passport, driver’s licence) *in person* in order to get an account on the IdM.[1] |
| R6 | | Identity | MUST | Attributes MUST be published according to the table below |
| R7 | AP5 | Incident resolution | MUST | The organisation running the IdP MUST participate in the resolution of incidents.[2] |

## Notification on loss of traceability

It is a requirement that the IdP be able to trace the user’s certificate identity to their real-life identity through the organisational (IdM) account behind the IdP - at any time during the validity of the certificate, and for a period afterwards of no less than XX months.

If the user ceases to be a member of the organisation running the IdP, the organisation MUST thus ensure that the user can no longer obtain a certificate - however, it must retain the records required for traceability.

This gives rise to requirement R4:  If the traceability is lost/unavailable, not only must the user not be able to obtain a certificate, but the certificate must be revoked - thus, the organisation must notify the CA as soon as possible after the loss of traceability.  This notification can be automated, or it can be done by a human.  The notification applies to all users with valid certificates as well as to users whose most recent certificate has expired within XX months.

If the Organisation cannot satisfy R4, it MUST notify the CA upon registration of the IdP.  In this case, the CA will only issue short lived credentials for the users using that IdP.

[1] The IdM MAY accommodate other users but these MUST NOT be able to obtain certificates through the IdP; it is the responsibility of the organisation running the IdP to ensure that they are filtered out.

[2] It is RECOMMENDED that the organisation comply with SIRTFI [2]

## Attributes

A specific set of attributes should be published by the IdP in order to support the above implementation. This information MUST be published in the attributes described in this table; however, for many of the purposes there is a choice of attributes that will fulfil

| **Purpose** | **Attribute** | **OID/URN** [3], [4] | **Req.** |
|---|---|---|---|
| Uniqueness and Traceability | eduPersonUniqueID | 1.3.6.1.4.1.5923.1.1.1.13 | |
| | SAML2 persistent id | urn:oasis:names:tc:SAML:2.0:nameid-format:persistent | |
| | eduPersonTargetedId | 1.3.6.1.4.1.5923.1.1.1.10 | |
| Name | commonName | 2.5.4.3 | |
| | sn<br>givenName | 2.5.4.4<br>2.5.4.42 | |
| | displayName | 2.16.840.1.113730.3.1.241 | |
| Organisation | organization | 2.5.4.11 | |
| | schacHomeOrganization | 1.3.6.1.4.1.25178.1.2.9 | |
| | eduPersonScopedAffiliation | 1.3.6.1.4.1.5923.1.1.1.9 | |
| Principal | eduPersonPrincipalName | 1.3.6.1.4.1.5923.1.1.1.6 | |
| SIRTFI[3] | | | |

# References

[1] https://www.igtf.net/ap/authn-assurance/
[2] SIRTFI https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home
[3] http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.htm
[4] SAML2 core

[3] It is not required to publish the security contact to the CA.

# Example SAML

# Changelog

| When | Version | Who | What |
|---|---|---|---|
| 25.05.15 | 0.9 | J Jensen | Published to PMA |