OIDC federation

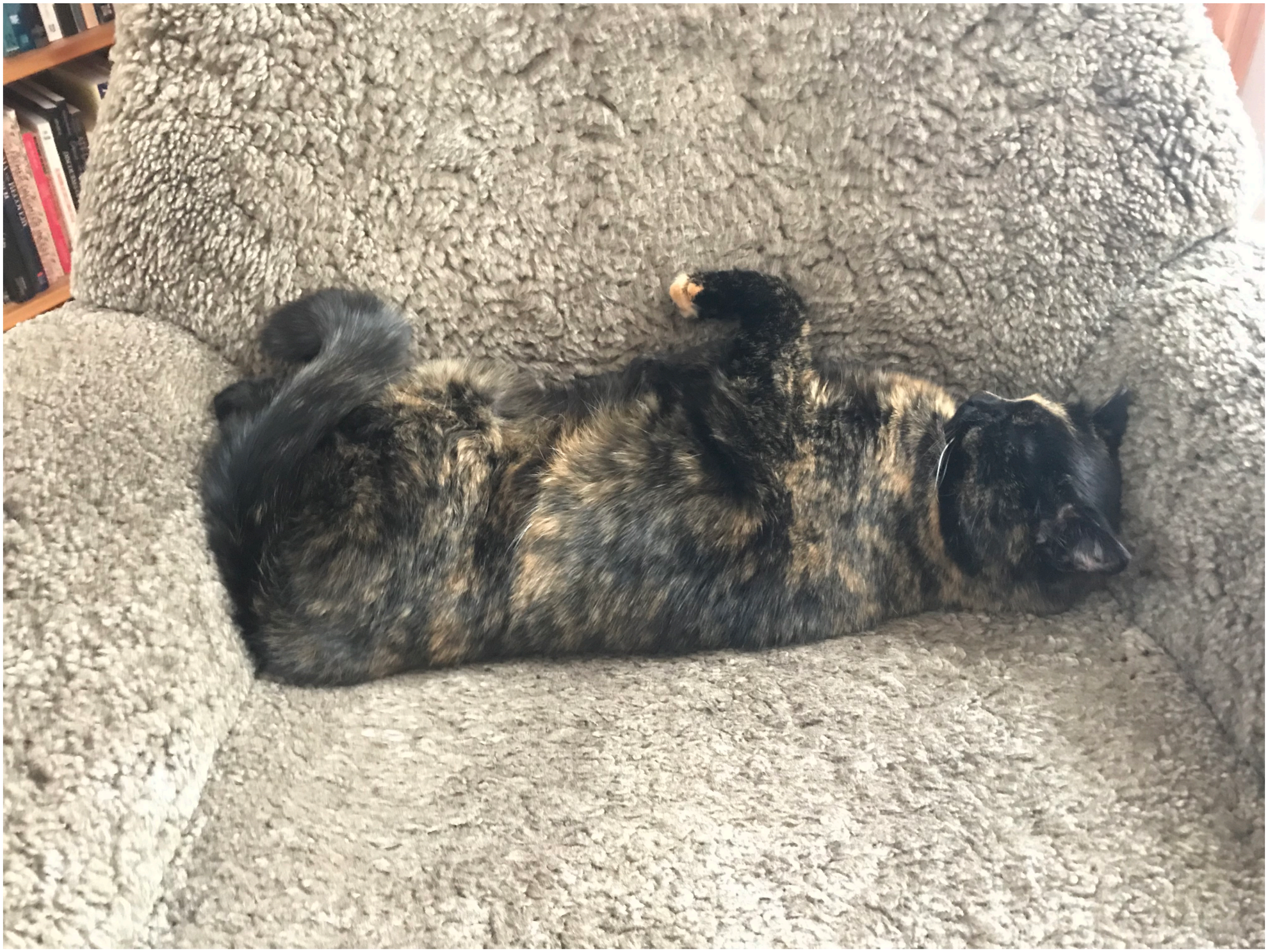
Roland Hedberg@TNC19

Background

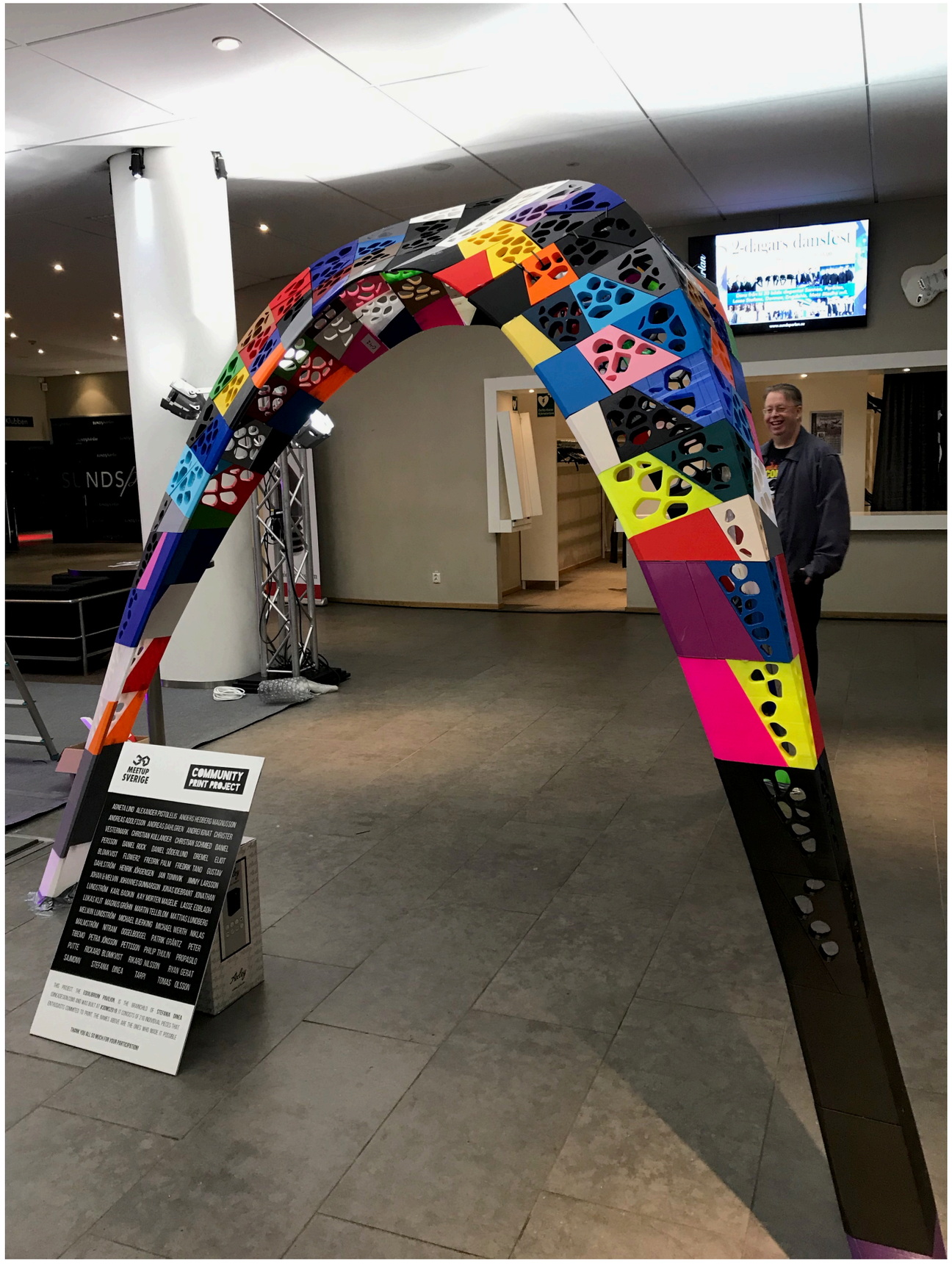
- SAML2 federations as used by R&E have a number of issues regarding metadata.
- OIDC has no support for multi lateral federations

GOAL: Extend OIDC to be able to support multi lateral federations bearing in mind the SAML2 metadata issues.

OIDC extensions



Going from P2P to multilateral federation

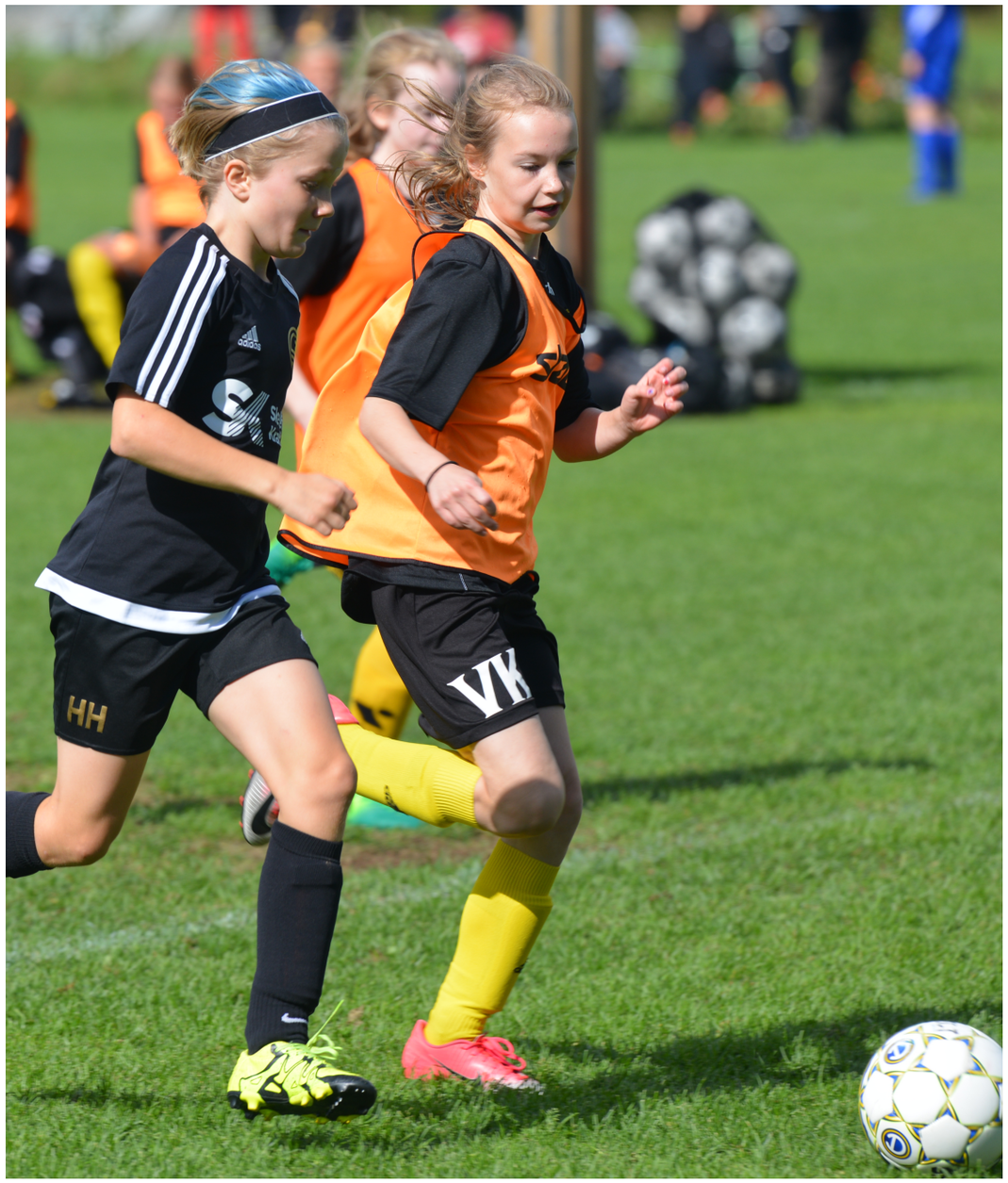


Already in OIDC

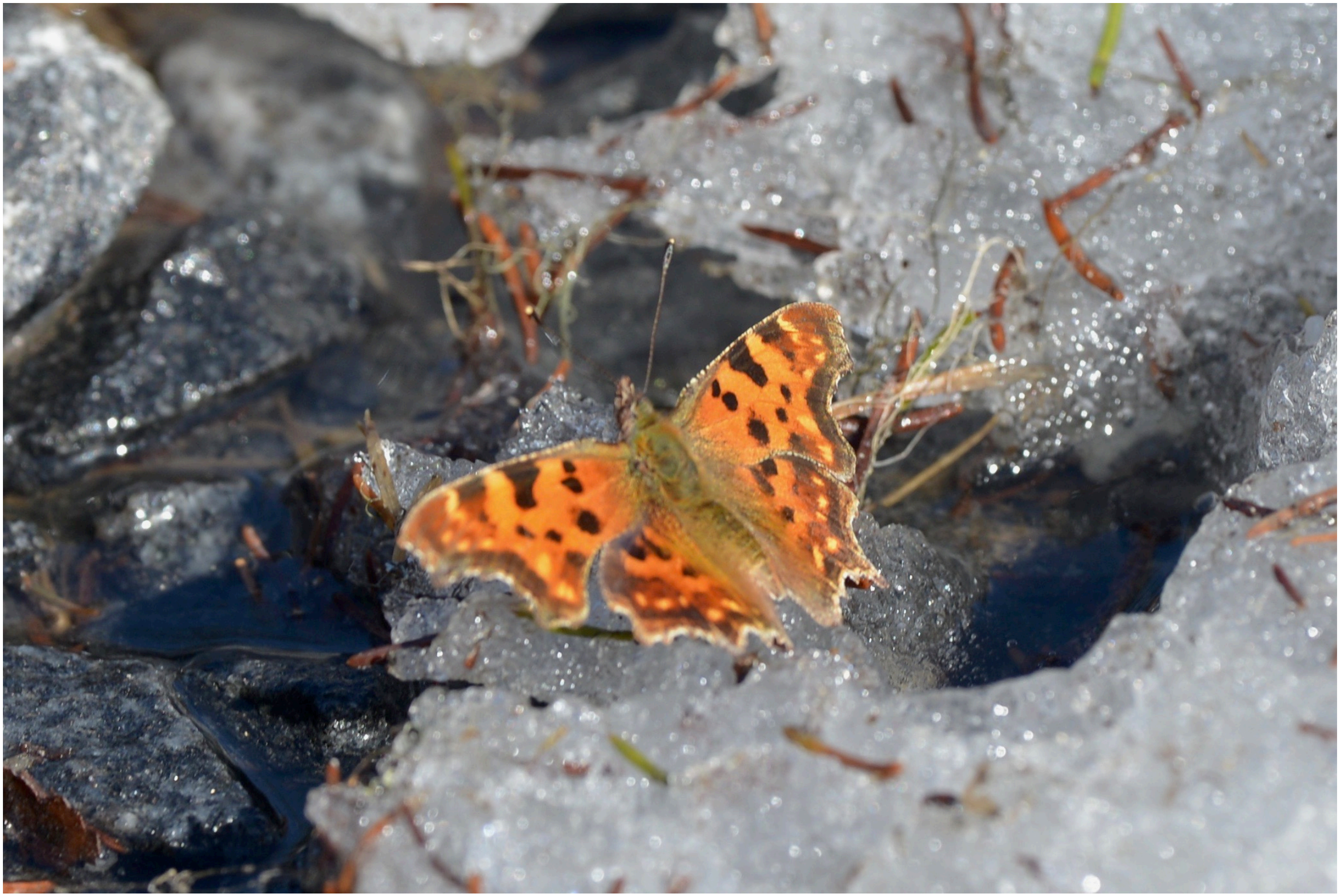
- Get the information when you need it (issuer discovery) !
- Dynamic client registration - if you want it !
- **BUT!** unverified information

Trusted information

- Correctness
  - Tamper resistance
  - Policy conformant
- Based on a trusted 3rd party (trust anchor)



SAML2 federation metadata issues



SAML2 vs OIDC

Two entities that trust the same trust anchor belongs to the same federation.

Appearing in a metadata file (yes I know about mdq) means you are part of a federation.

SAML2 vs OIDC

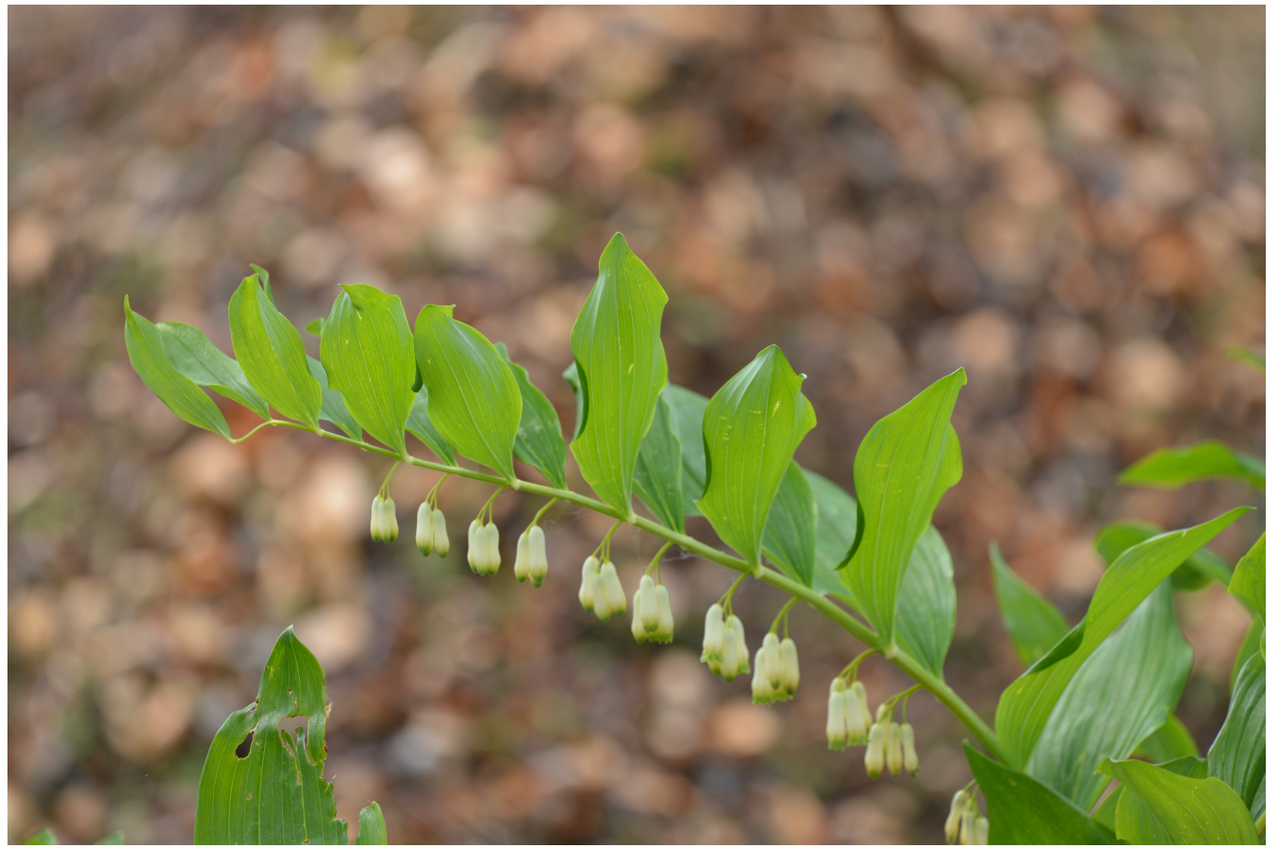
The federation operator sets the boundaries of what is acceptable.

An entitys complete metadata must be accepted by the federation operator for the entity to be allowed into the federation.

SAML2 vs OIDC

Can use the aggregated/ distributed claims functionality

3rd party information has to be added by the Federation Operator



SAML2 vs OIDC

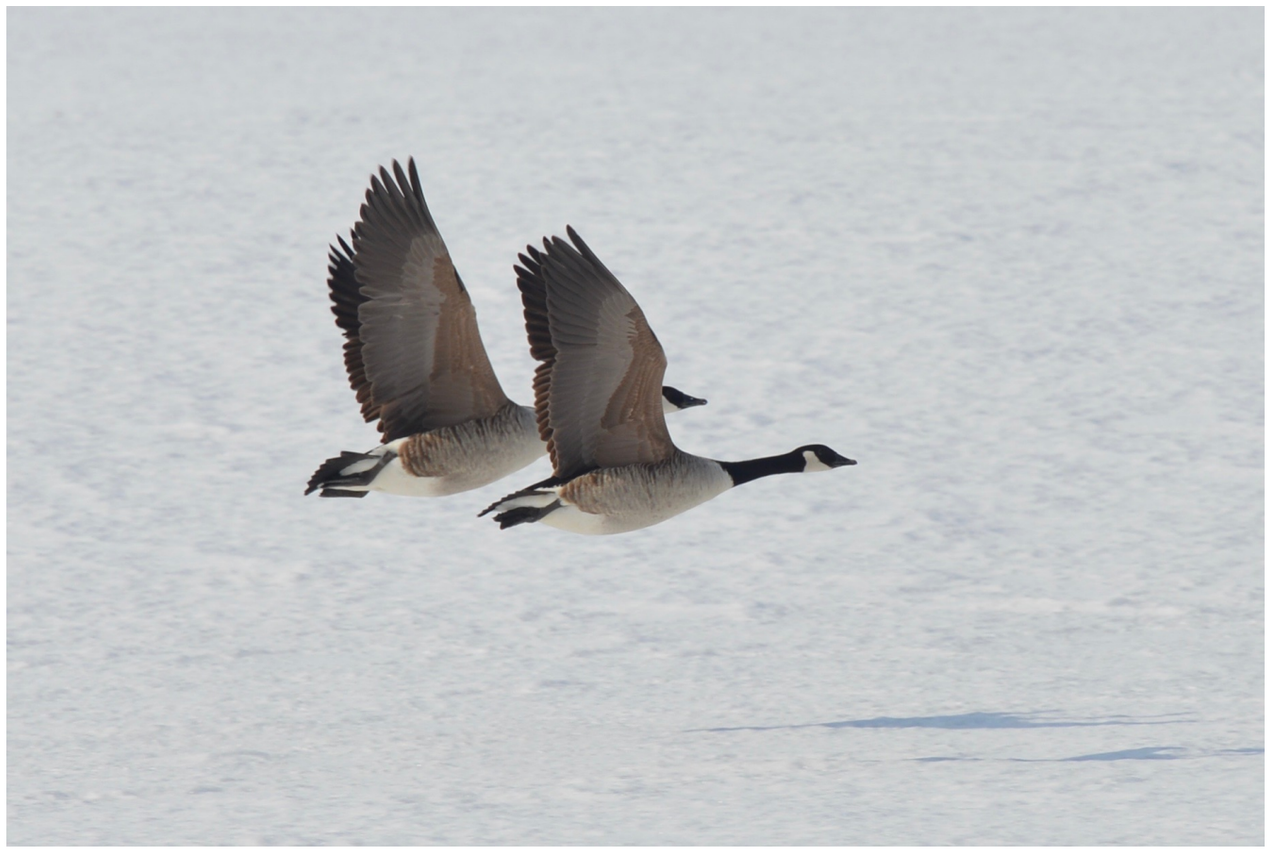
There is no drawback to belong to more then one federation.

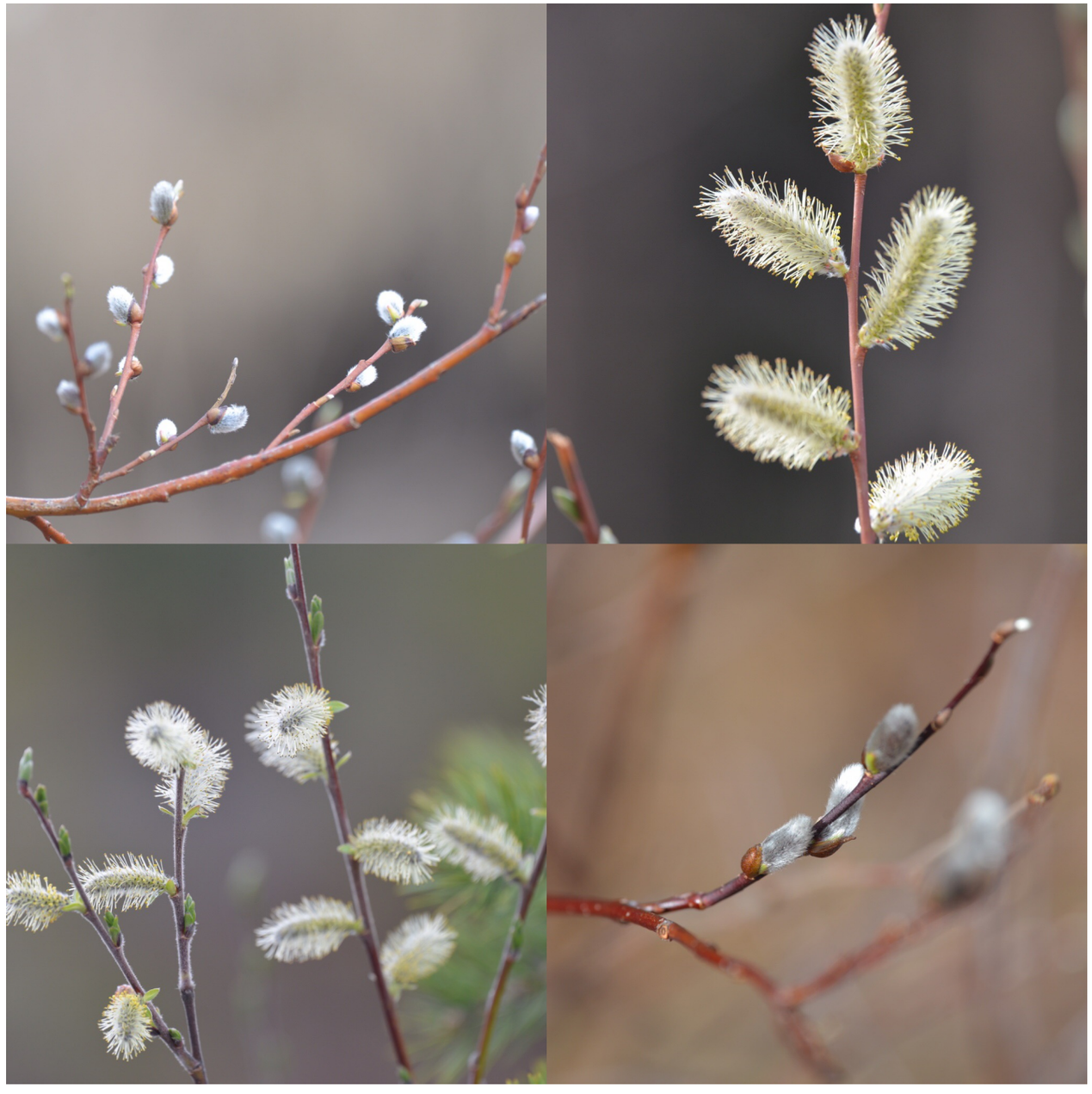
It is rare that an entity belongs to more then one federation. Given EduGain it is actually recommended that an entity should only belong to one.

SAML2 vs OIDC

There is no negotiation on metadata

The RP proposes and the OP decides (explicit client registration)





QUESTIONS ?