OIDC federations

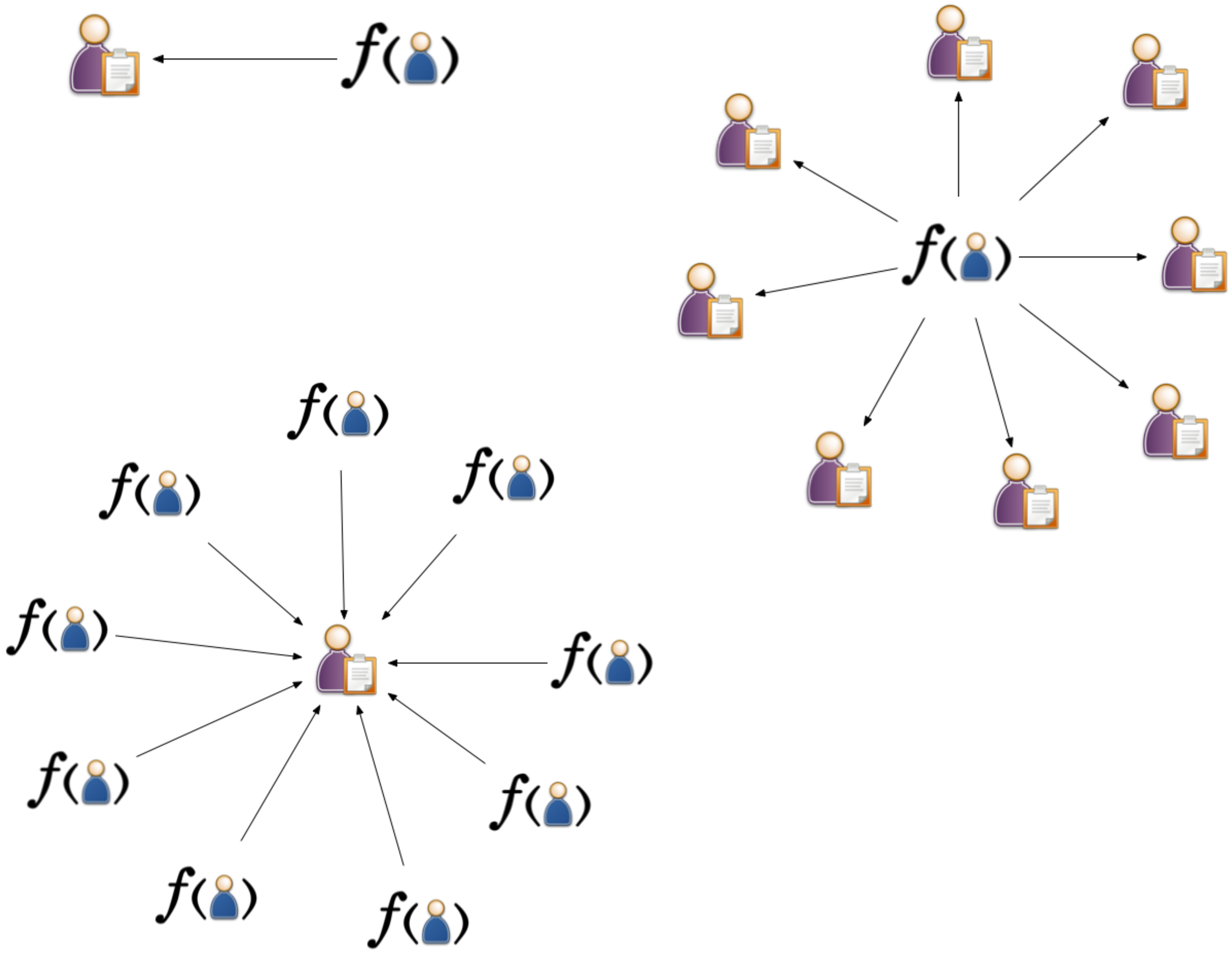
Roland Hedberg, 28 October 2020

What we’re not trying to solve

One RP to one OP

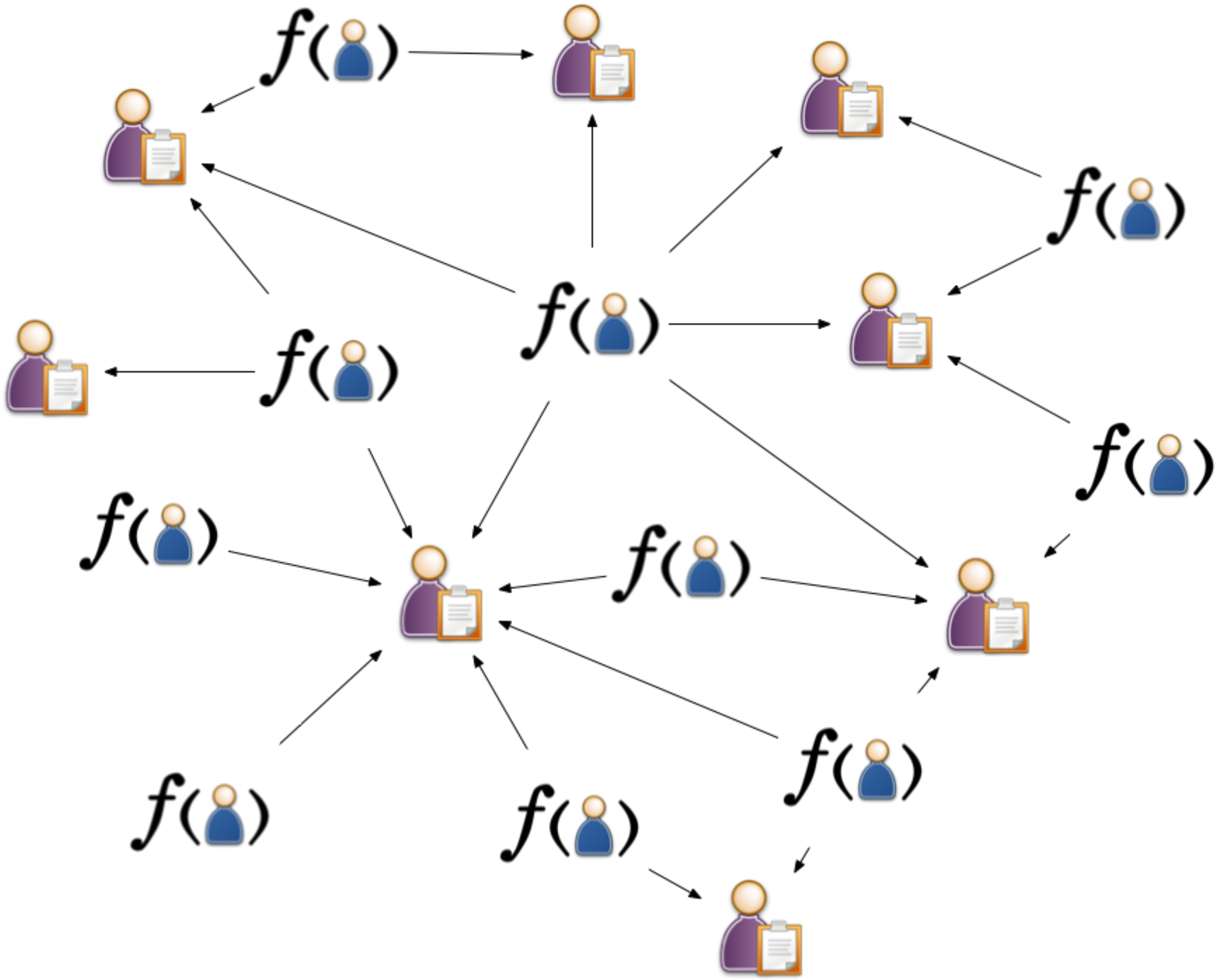
One RP to many OPs

Many RPs to one OP



What we do want to solve

Many RPs to many OPs (multilateral federation)



What the OIDC federation specification adds

- Entity statements
- Trusted 3rd party (trust anchor)
- Trust chains
- Explicit/automatic client registration
- Metadata policies

Entity statement

Is a JSON Web Token

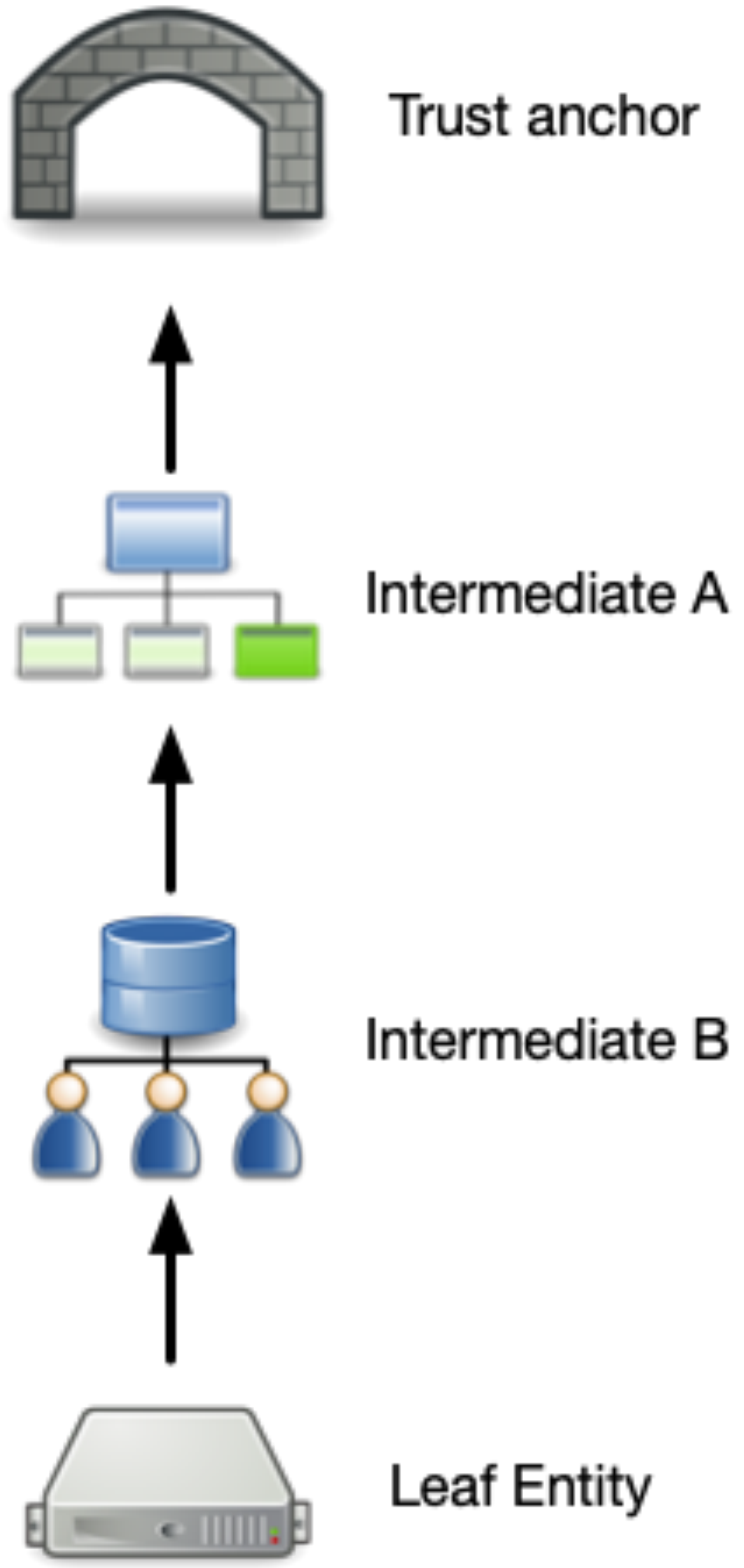
- iss
- sub
- iat
- exp
- aud

- authority_hints
- jwks
- metadata
- metadata_policy

- constraints
- crit
- policy_crit

Federation structure

- A federation can be shallow (leaf entity immediately below trust anchor) or deep (one or more intermediates between the leaf entity and the trust anchor).



Trust Chain Collection

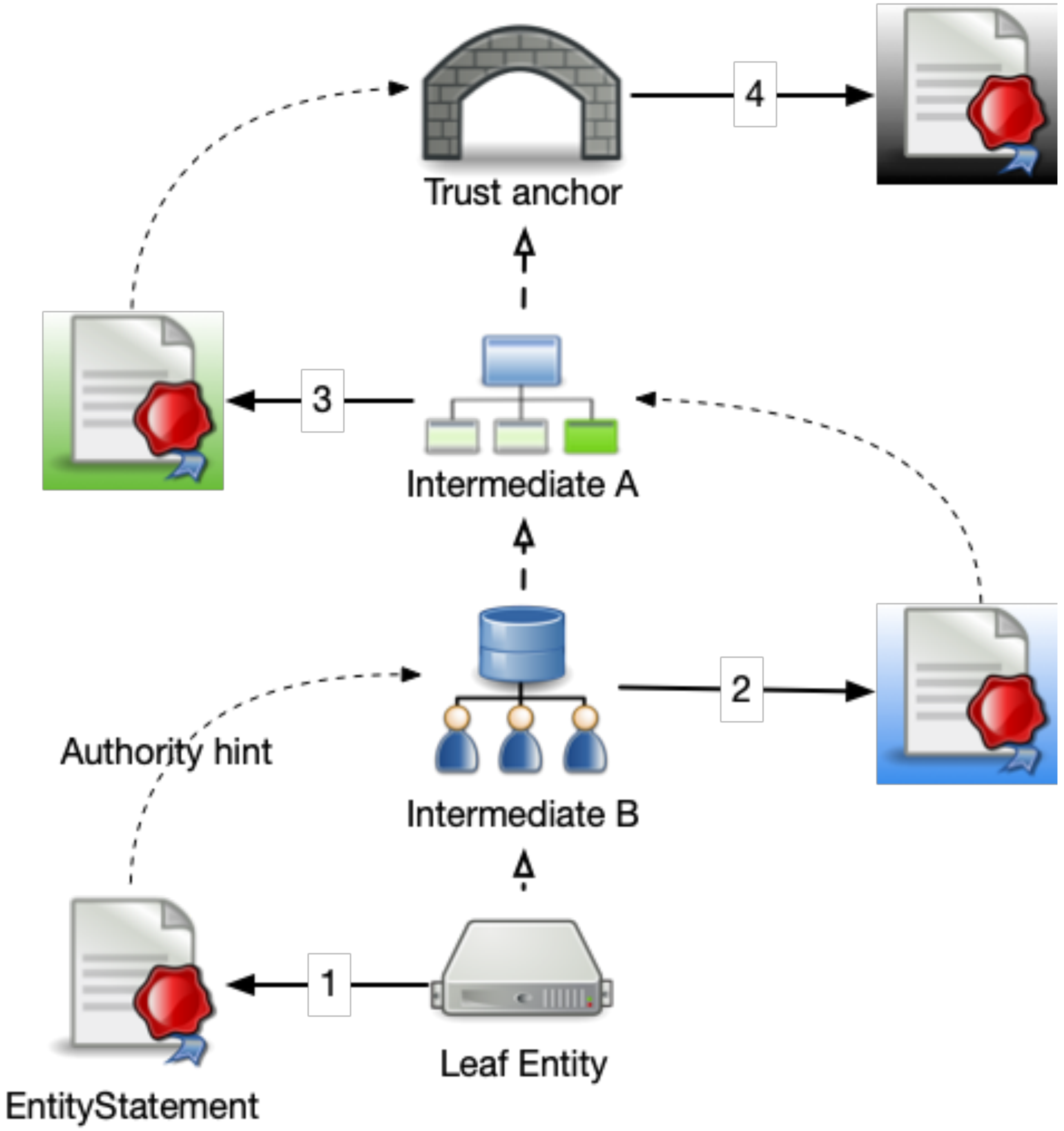
1. Start with a self-signed entity statement about an entity.

2. Use the authority_hints in the entity statement to find superiors.

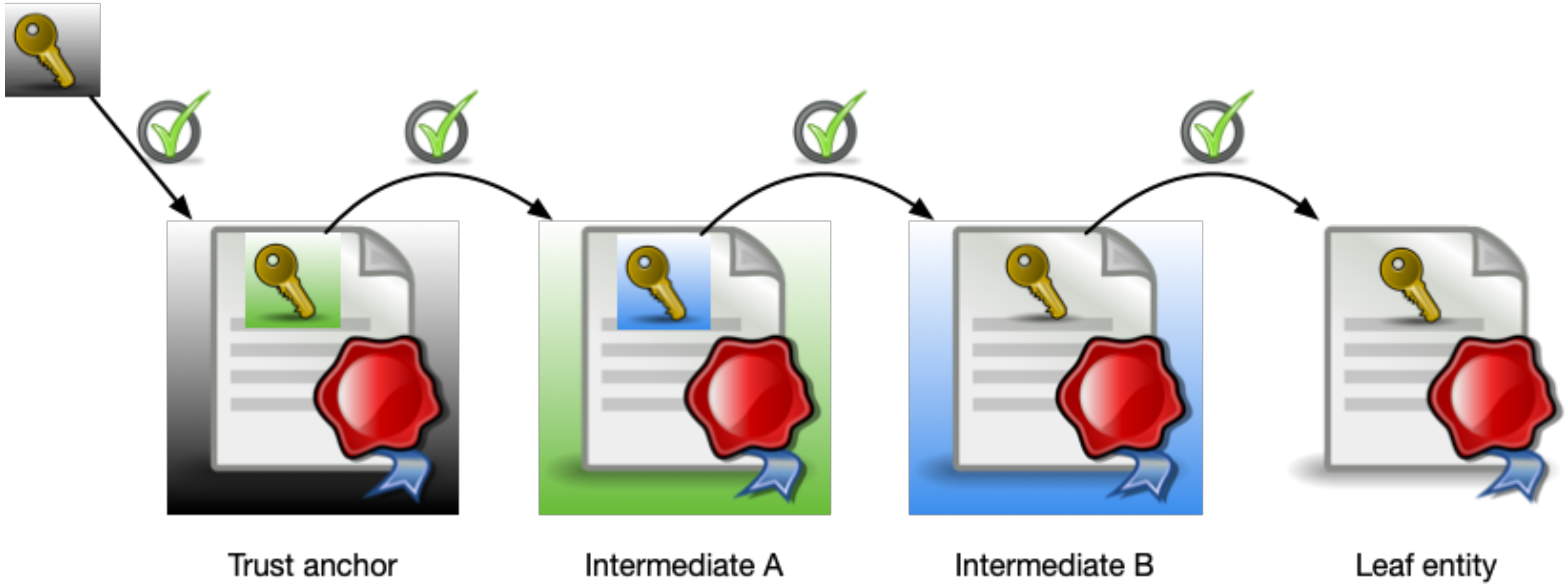
3. Ask the superiors for their information, about the issuer of the entity statement, in the format of an entity statement.

4. If the superior is the trust anchor. - BREAK

5. GOTO 2



Trust Chain Verification



Explicit client registration

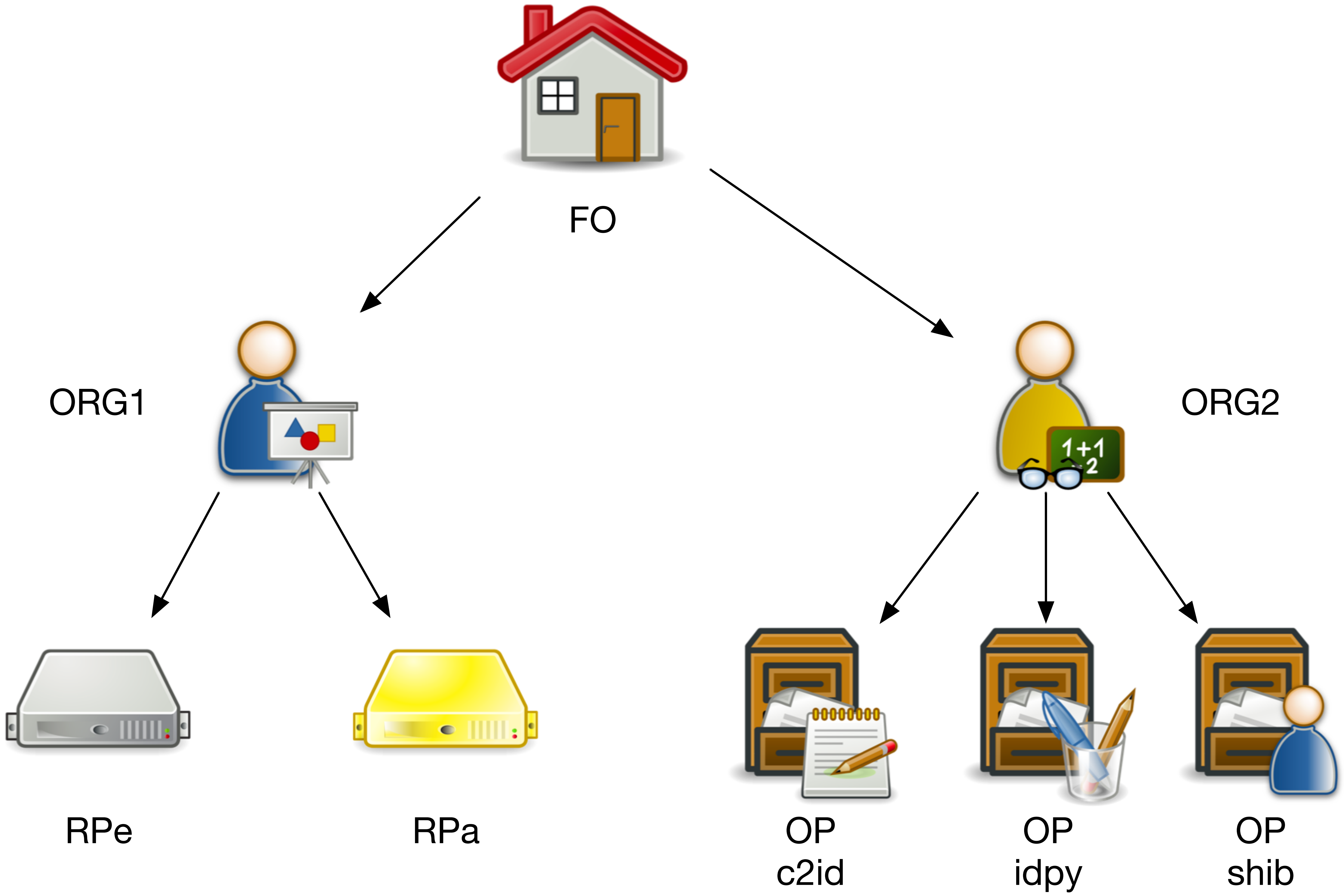
- Like OIDC core dynamic client registration but with entity statements instead of metadata.
- Both request (metadata) and response (metadata_policy) uses entity statements.

Automatic client registration

- First message sent from the RP to the OP is an authentication request (not counting the provider information discovery).
- The authentication request contains a request object by value, by reference or by using PAR.
- The client_id in the authentication request is the RP’s entity_id.
- Using the entity_id the OP can fetch and verify the RP’s metadata as described earlier.
- Once it has the RP’s metadata it can verify the signature of the request object.

Interoperability testing 1&2

Setup



Interoperability testing - OPs

RP used = oidcrp

	IdPy	C2ID	SHIBBOLETH
Entity statements	✓	✓	✓
Trust chain collection	✓	✓	✓
Trust chain validation	✓	✓	✓
Explicit client registration	✓	✓	✓
Automatic client registation	✓	✓	✓
Metadata policies			