OIDC Identity Federation in pictures

by Roland Hedberg at
IIW XXIII

According to Wikipedia

- A **federation** (information technology) is a group of computing or network providers agreeing upon standards of operation in a collective fashion.

- The term "**identity federation**" is by design a generic term, and is not bound to any one specific protocol, technology, implementation or company. One thing that is consistent, however, is the fact that "federation" describes methods of identity portability which are achieved in an open, often standards-based manner – meaning anyone adhering to the open specification or standard can achieve the full spectrum of use-cases and interoperability.

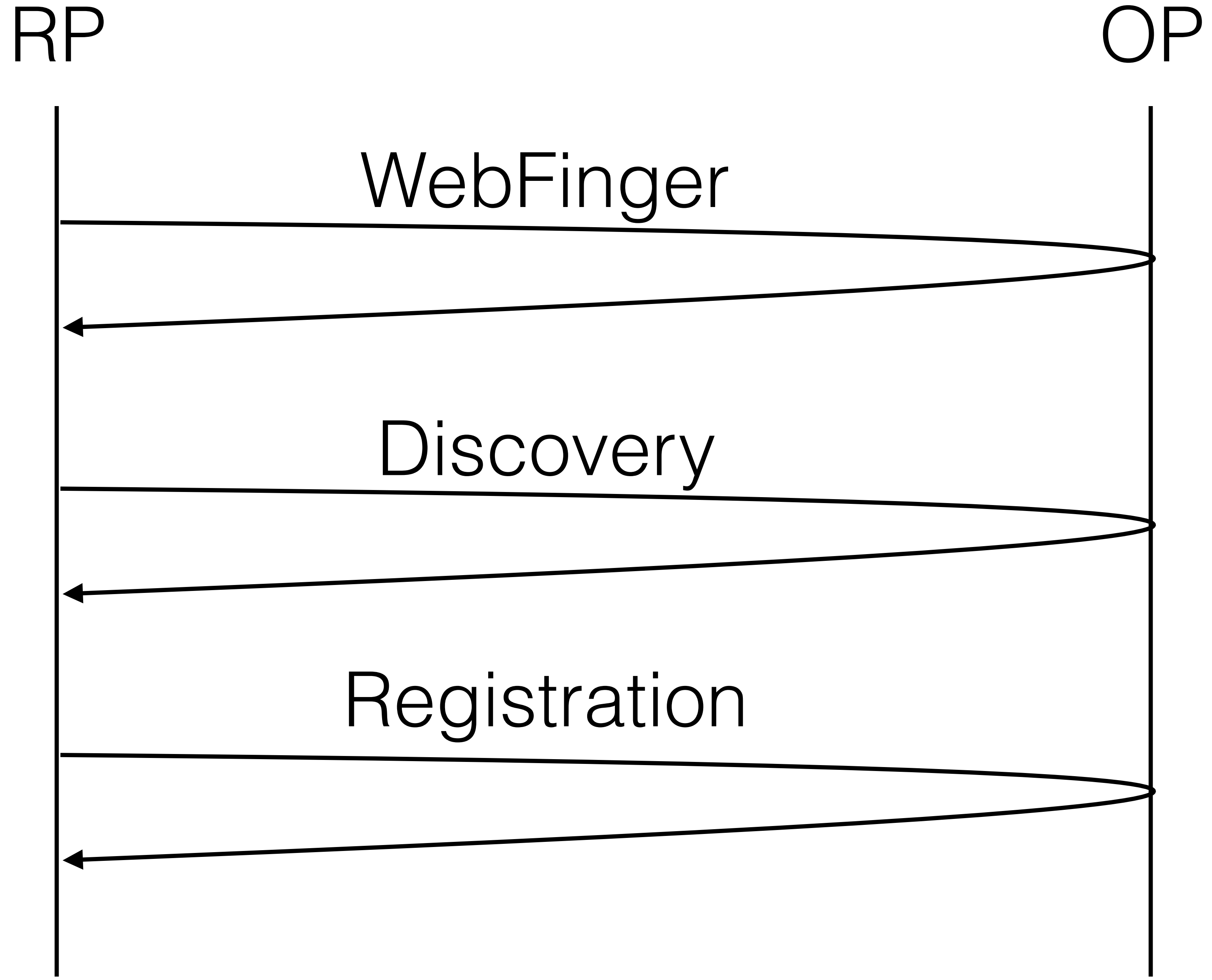
OIDC IDENTITY FEDERATION

- Allow dynamic discovery and registration without losing trust.
- Enforcement of federation and organization policies
- Allow delegation of entity registration
- Metadata transport and origin independent
- Metadata Self-contained

CHAIN OF TRUST

- Trusted 3rd party
- Chain of verifiable claims
- Metadata construction

Client - Server setup



Common metadata

- signing_keys
    - A JSON Web Key Set (JWKS) [RFC7517] representing the public part of the entity's signing keys.
- signing_keys_uri
    - Location where a JWKS representing the public part of the entity's signing keys can be found. SHOULD return the Content-Type "application/jose" to indicate that the JWKS is in the form of a JSON Web Signature (JWS) [RFC7515] using the JWS Compact Serialization.
- metadata_statements
    - JSON array containing a list of metadata statements.
- metadata_statement_uris
    - JSON object where the names are the federation identifiers and the values are URLs pointing to metadata statements connected to each federation.
- signed_jwks_uri
    - This is the signed version of the "jwks_uri" parameter defined in OpenID Connect Dynamic Client Registration 1.0. SHOULD return the Content-Type "application/jose" to indicate that the JWKS is in the form of a JWS using the JWS Compact Serialization. The key used to sign the JWKS can be found among the keys published in "signing_keys" or fetched from "signing_keys_uri"

Specific client metadata

- scopes
  - JSON array containing a list of the RFC6749 [RFC6749] scope values that this clients expects to use.
- claims
  - JSON array containing a list of the Claim Names of the Claims that the OpenID Client wants values for.

Notation

- ms_X
    - Metadata Statement signing request by X without signing keys and signed metadata statements.
- SK[X]
    - Signing keys that belongs to X
- X(MS)
    - Metadata Statement signed by X

Metadata statements

- Simple signed metadata statement

A(ms_B + SK[B])

- Compounded metadata statement

B(ms_C + SK[C] + A(ms_B + SK[B]))

Constructing metadata

- If the same claims appear in MS_a and MS_b ($b > a$, $a=0,..,n$, $b=0,..,n$) then unless the value in MS_b is less or equal to the value in MS_a then the value in MS_b should be ignored.

- <=

  - If the values are strings they are less or equal if they are equal.

  - if the values are lists then for each value in MS_b there MUST be a corresponding value in MS_a that is less or equal.

The players

The good, the bad and the ugly

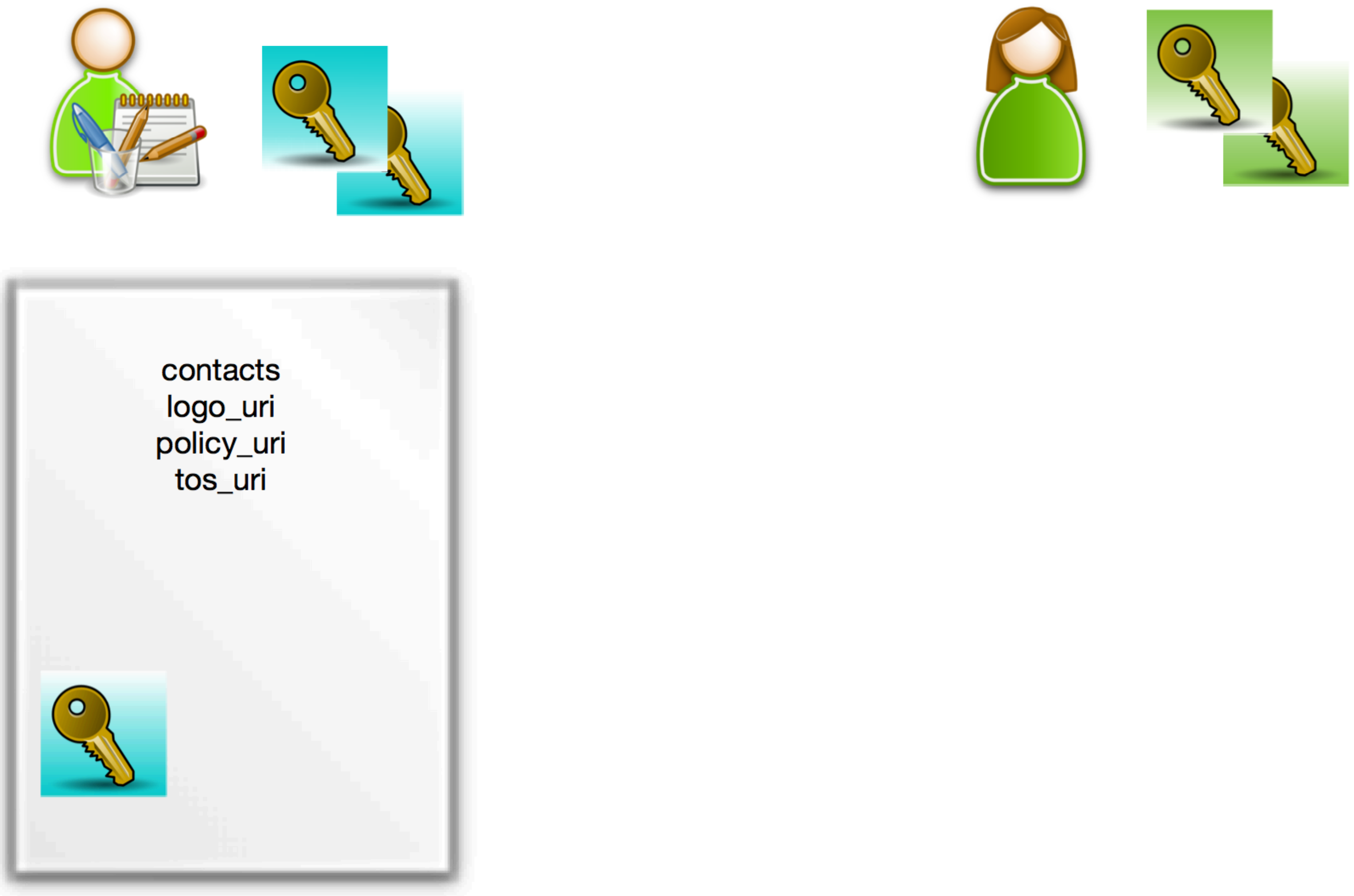
System adminstrator

IT Architect

Federation Operator

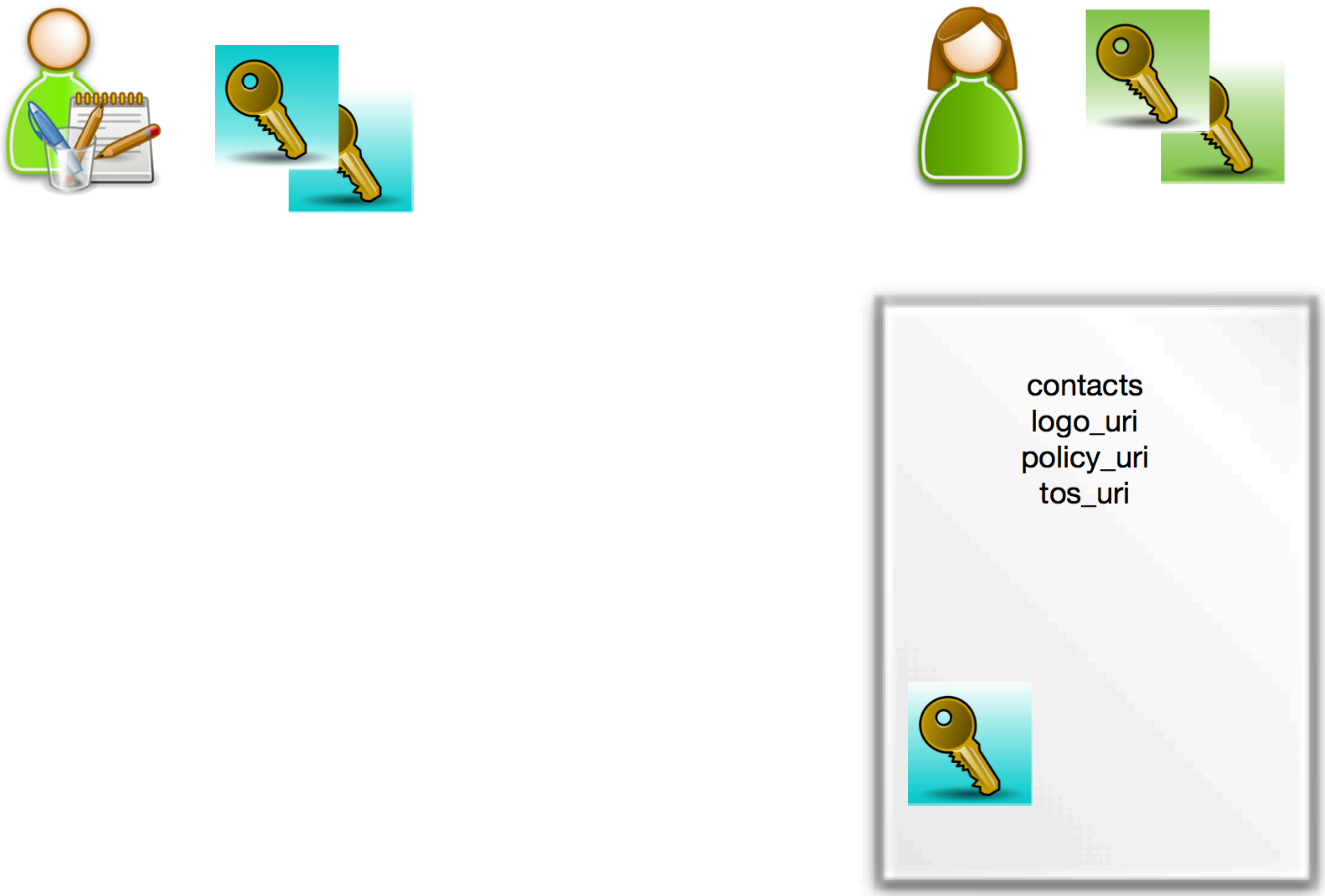
Organization and FO

Organization wide information



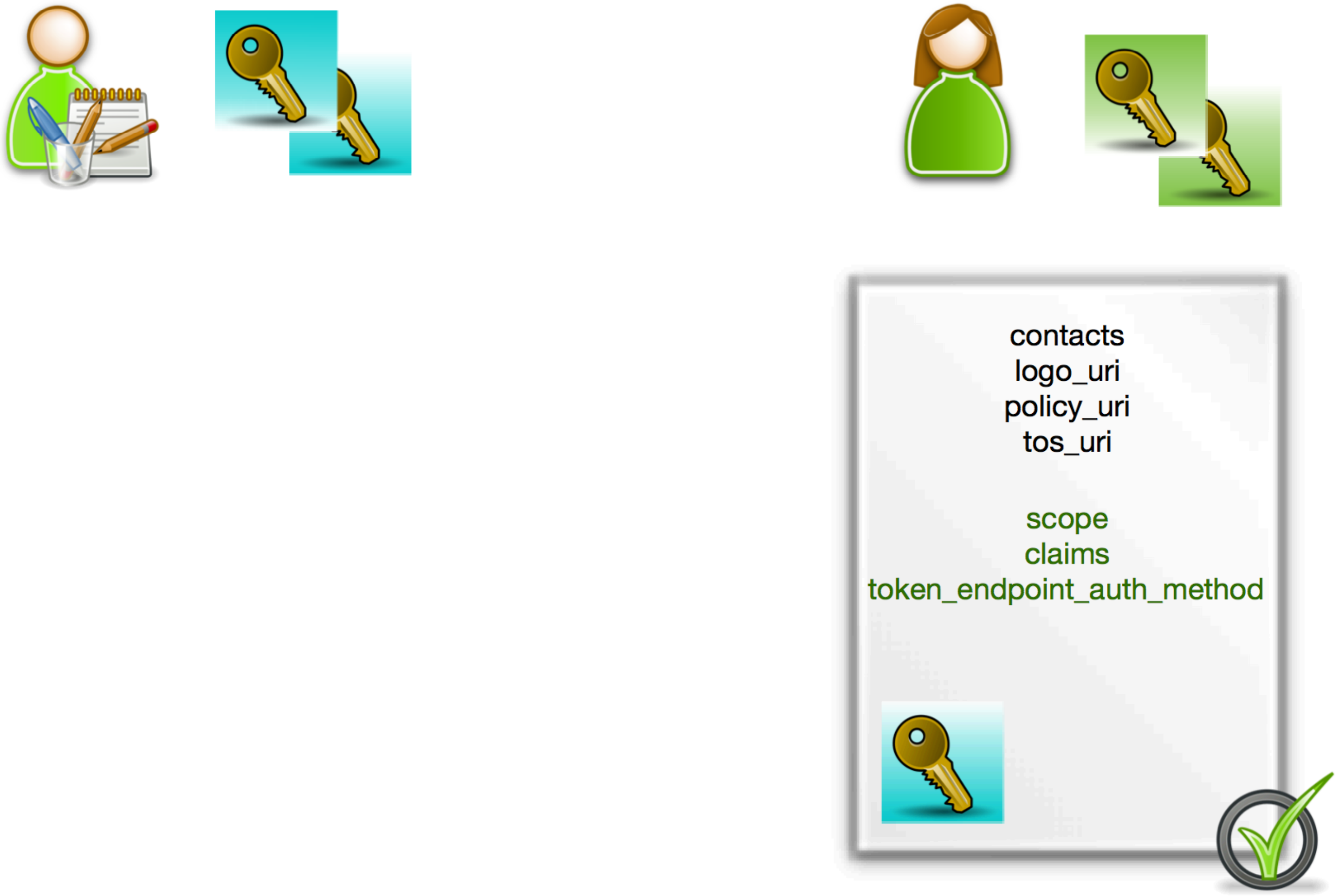
contacts
logo_uri
policy_uri
tos_uri

Transfer to FO



contacts
logo_uri
policy_uri
tos_uri

FO: verifies, modifies and signs

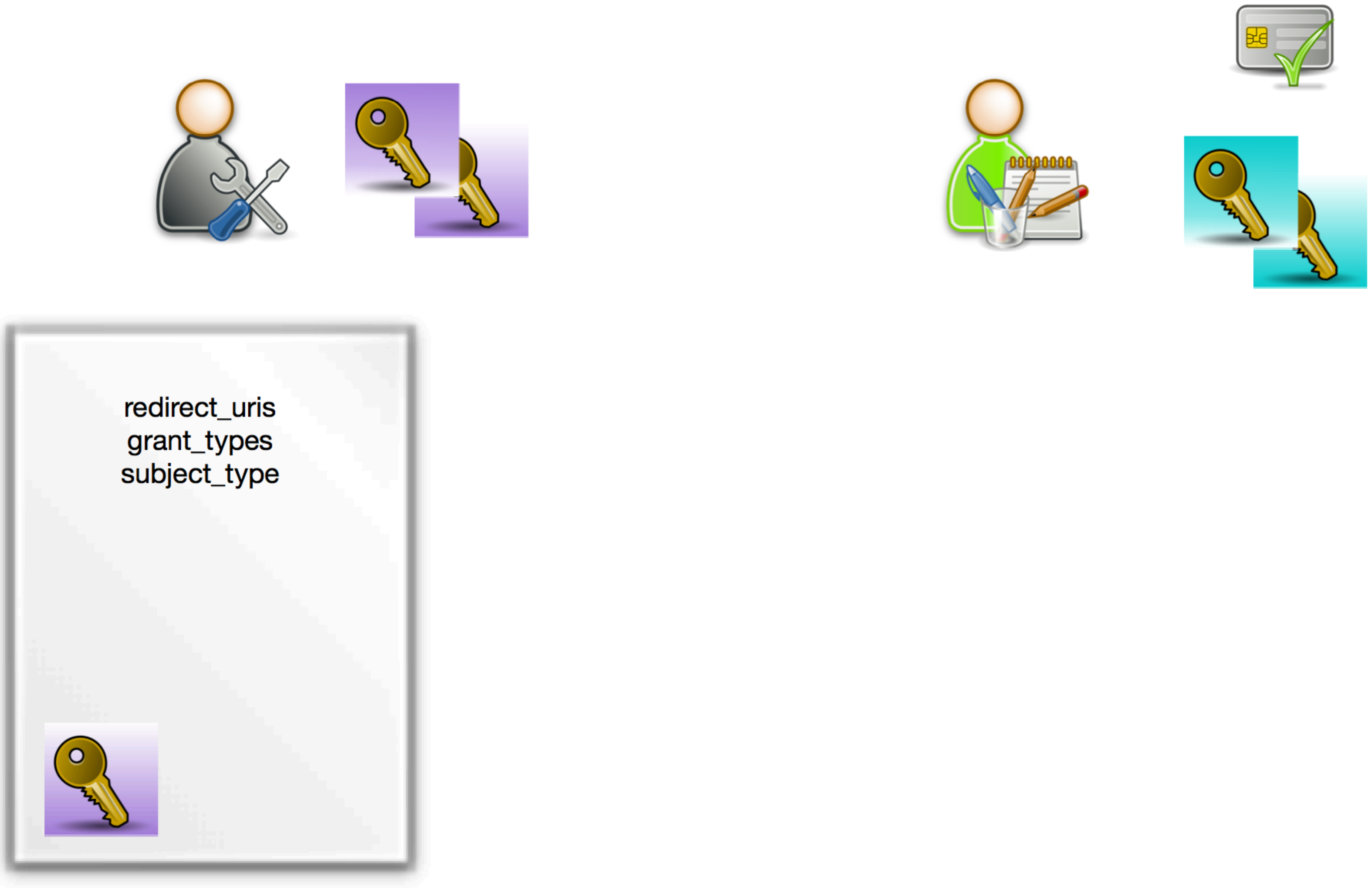


contacts
logo_uri
policy_uri
tos_uri

scope
claims
token_endpoint_auth_method

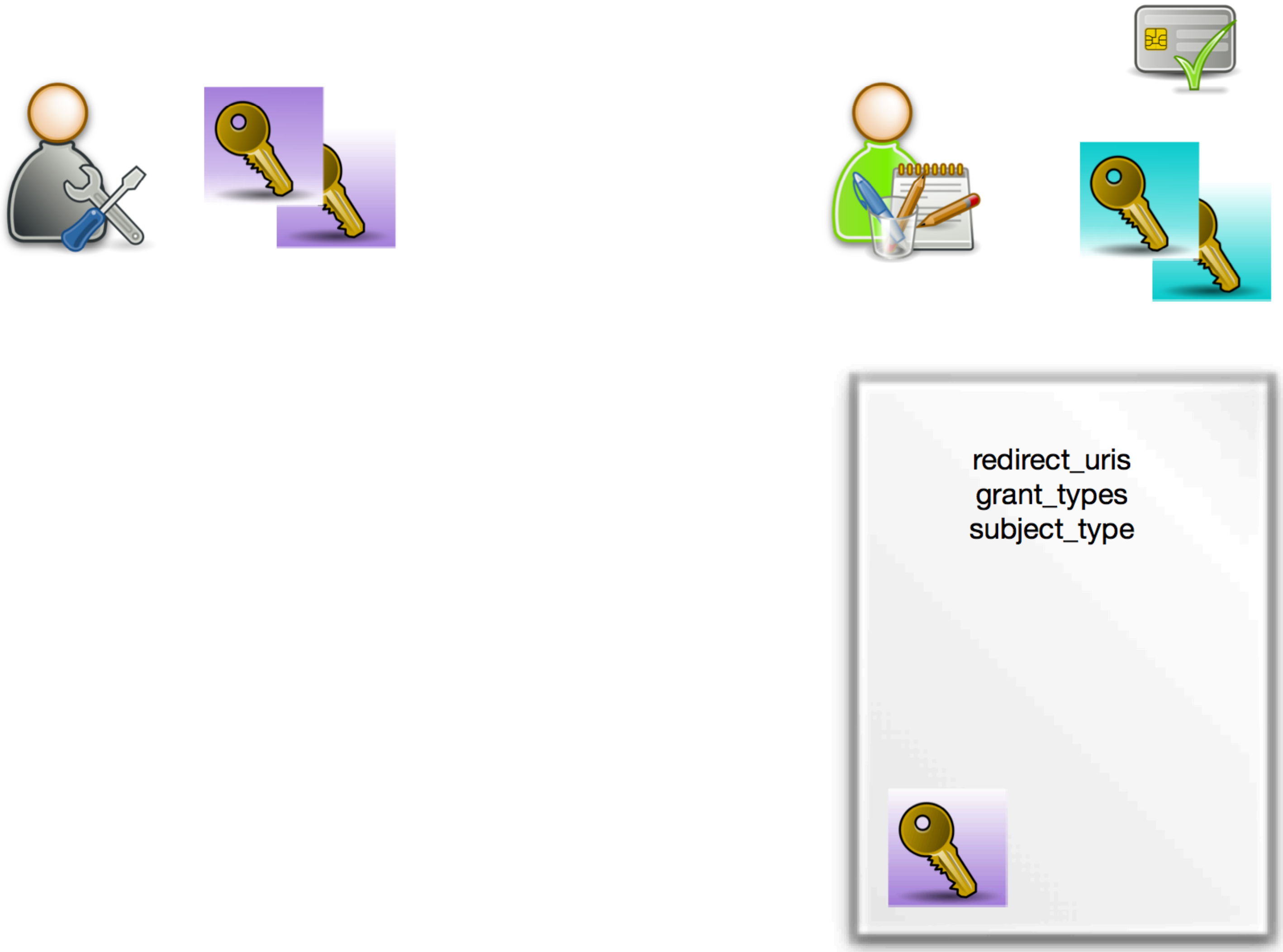
Within an organization

Entity specific information

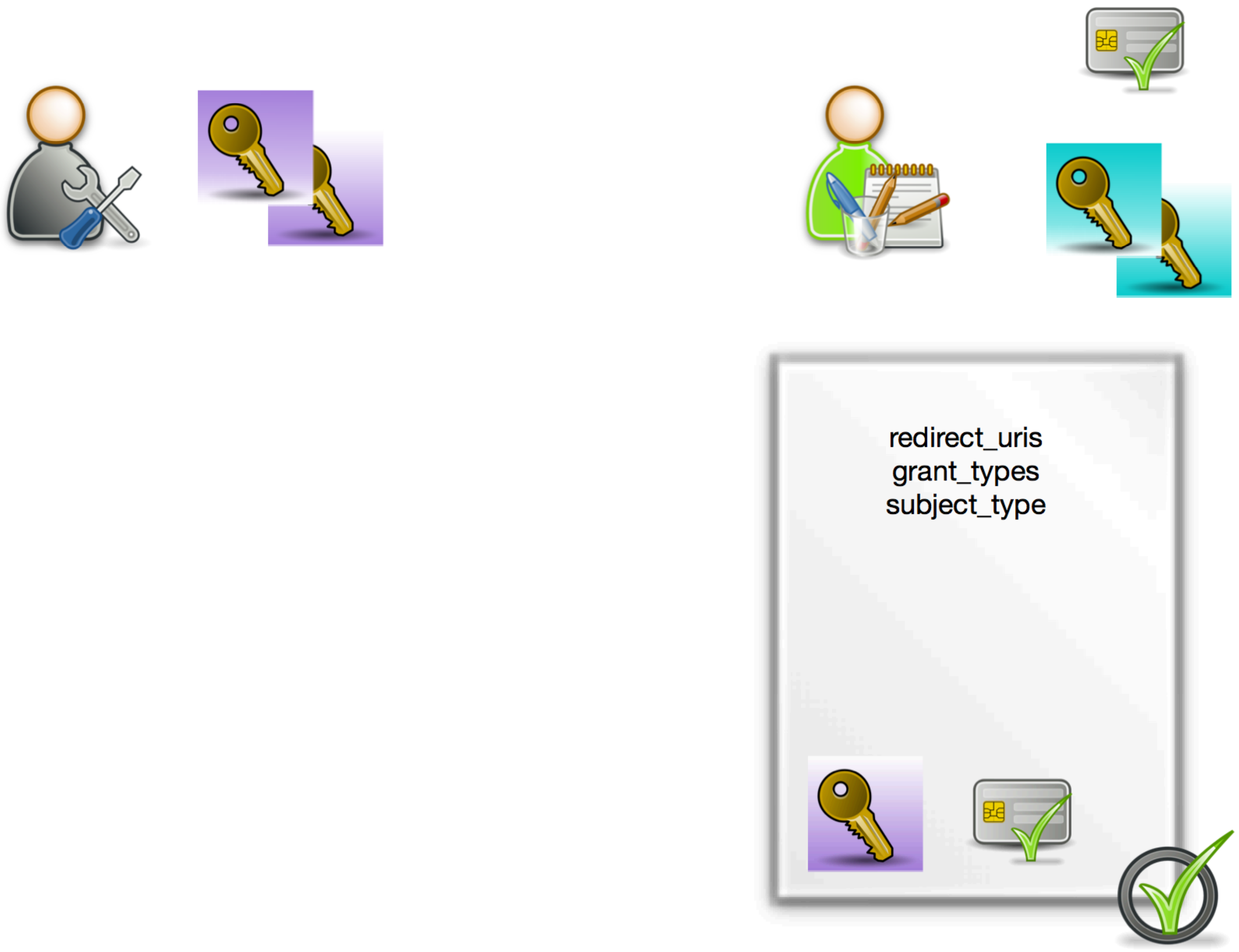


redirect_uris
grant_types
subject_type

Transfer to Organization coordinator (OC)

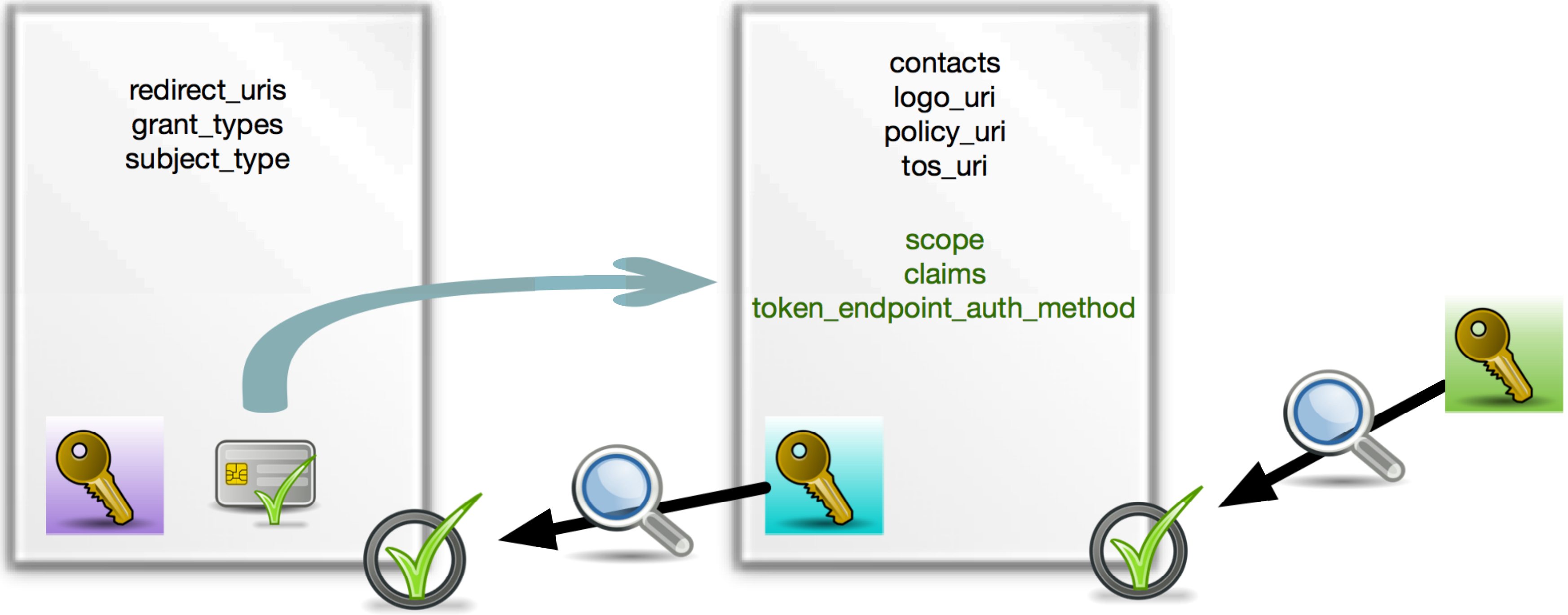


OC: verifies, modifies and signs



redirect_uris
grant_types
subject_type

Unpacking a metadata statement

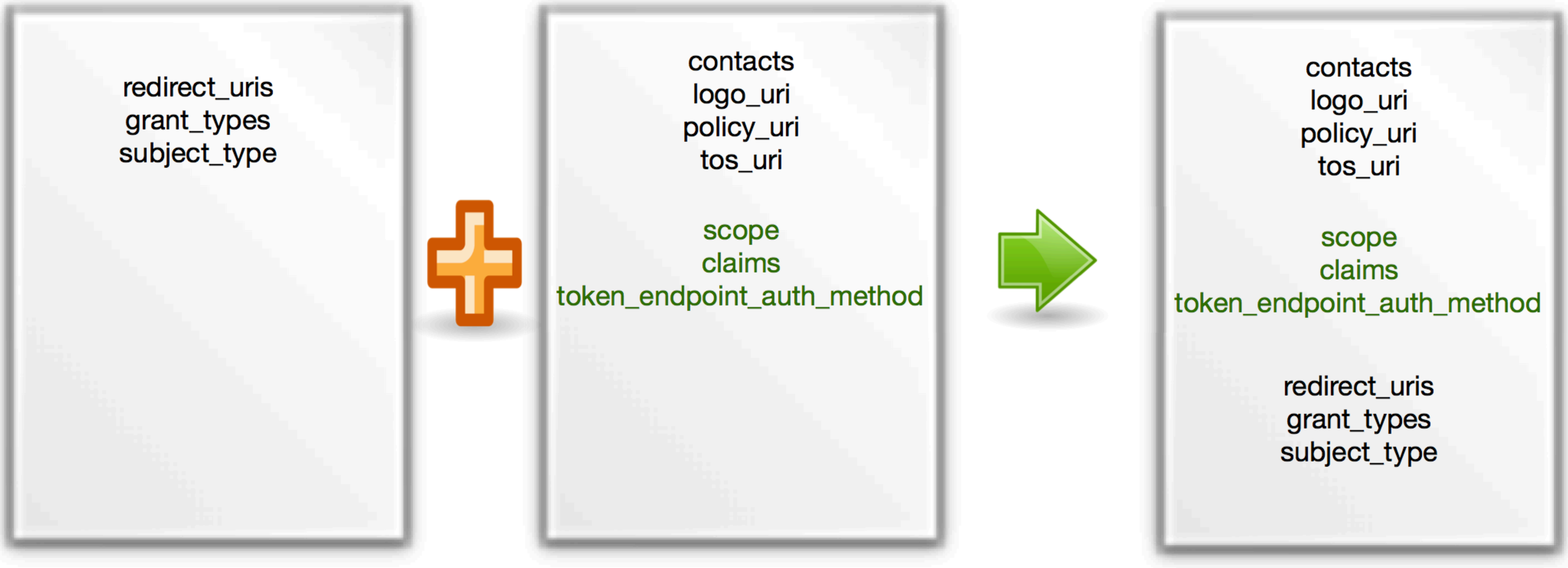


redirect_uris
grant_types
subject_type

contacts
logo_uri
policy_uri
tos_uri

scope
claims
token_endpoint_auth_method

Gathering the metadata



redirect_uris
grant_types
subject_type

contacts
logo_uri
policy_uri
tos_uri

scope
claims
token_endpoint_auth_method

contacts
logo_uri
policy_uri
tos_uri

scope
claims
token_endpoint_auth_method

redirect_uris
grant_types
subject_type

OIDC IDENTITY FEDERATION

- Allow dynamic discovery and registration without losing trust.
- Enforcement of federation and organization policies
- Allow delegation of entity registration
- Metadata transport and origin independent
- Metadata Self-contained