OIDC Identity Federation in pictures

by Roland Hedberg at
NORDUnet Conference 2016

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

The players

The good, the bad and the ugly

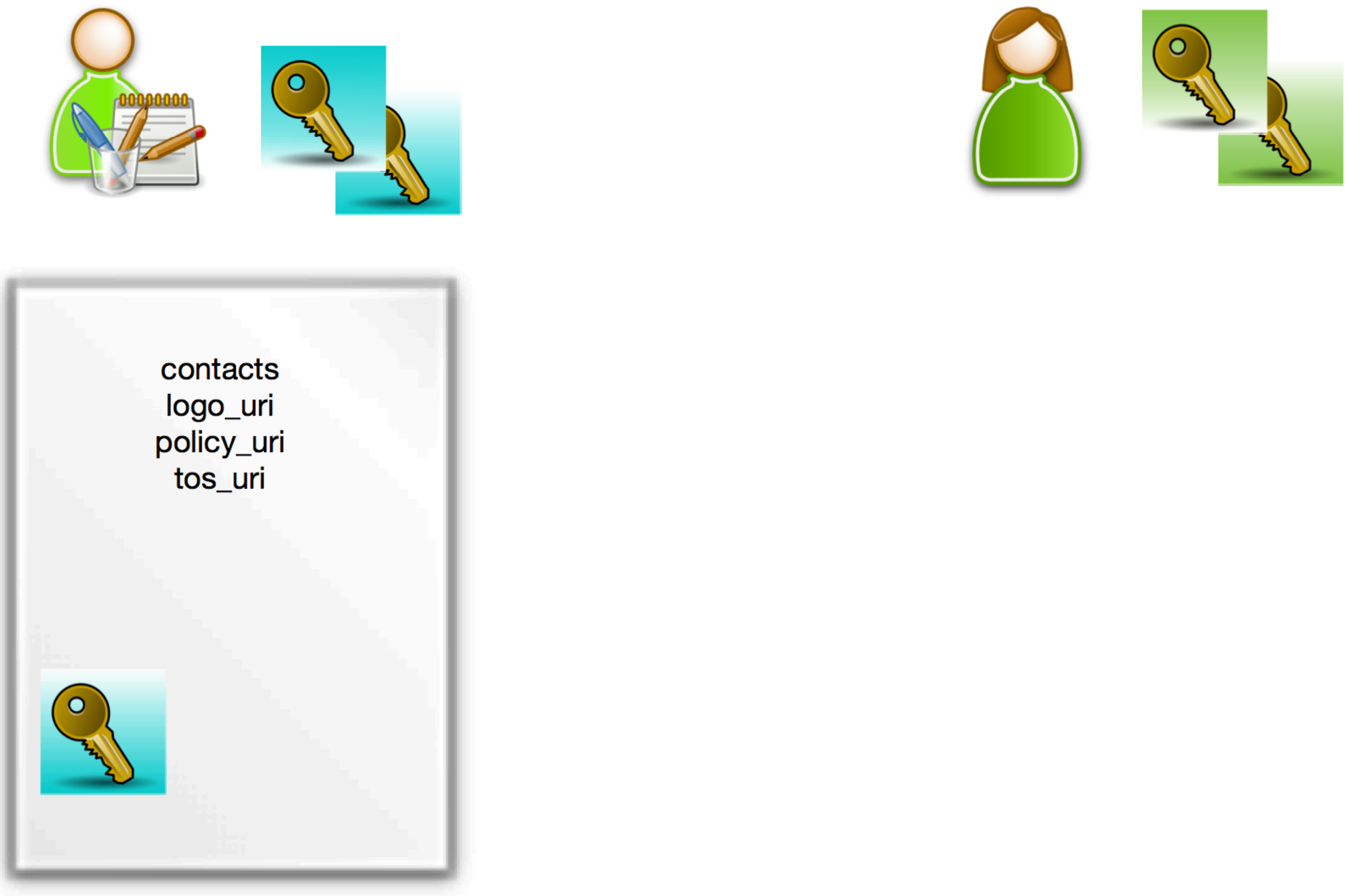
System adminstrator

IT Architect

Federation Operator

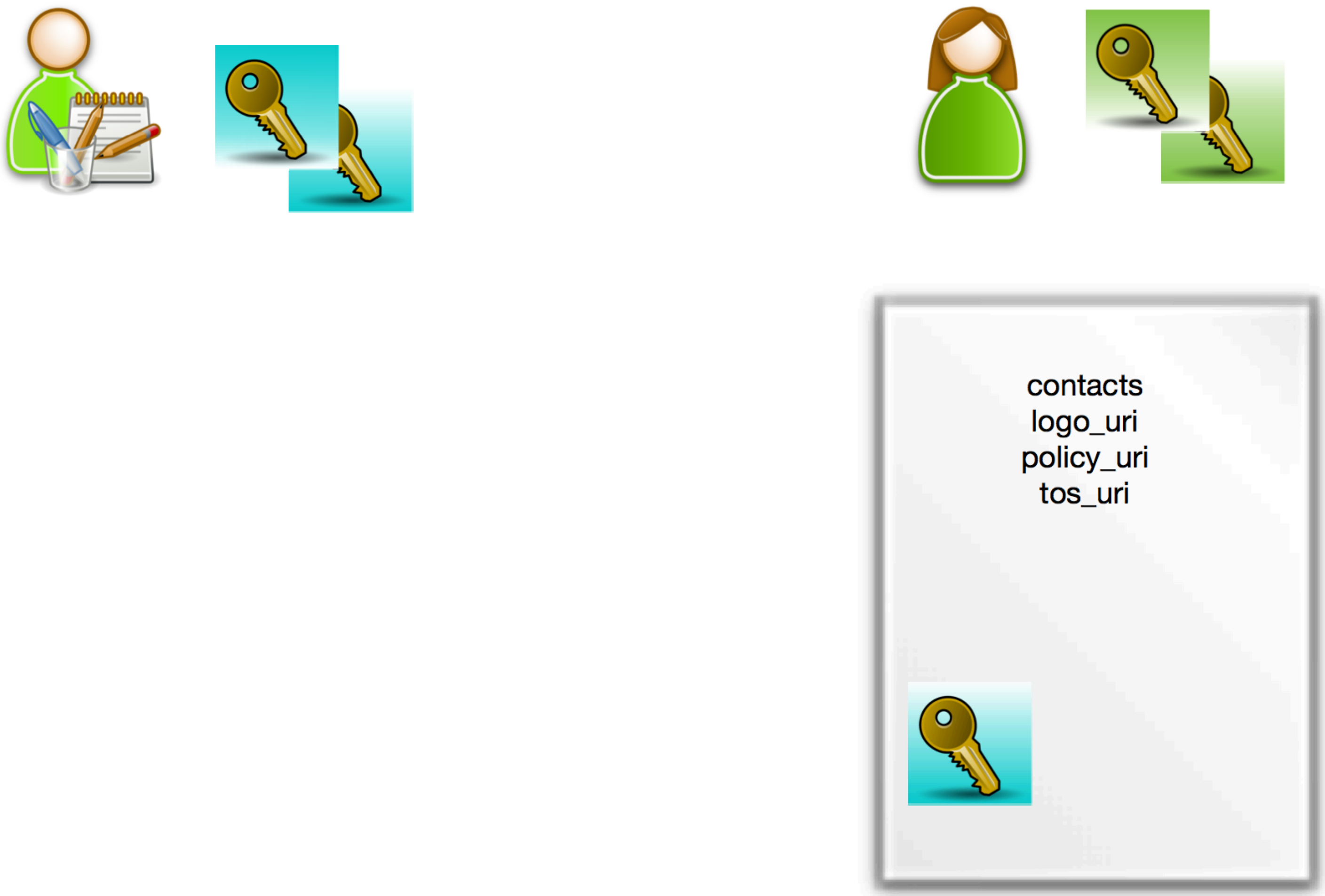
Organization and FO

Organization wide information



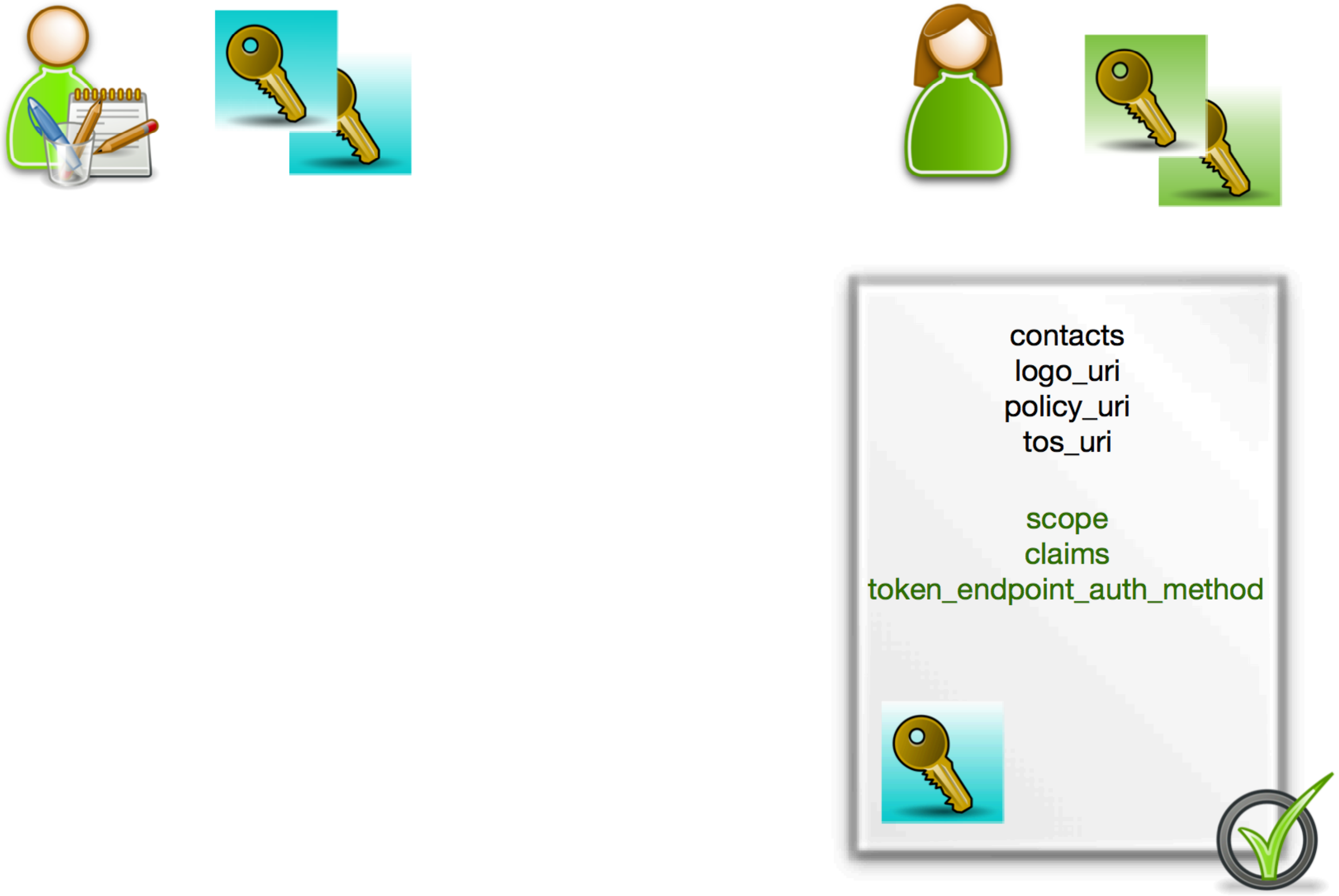
contacts
logo_uri
policy_uri
tos_uri

Transfer to FO



contacts
logo_uri
policy_uri
tos_uri

FO: verifies, modifies and signs

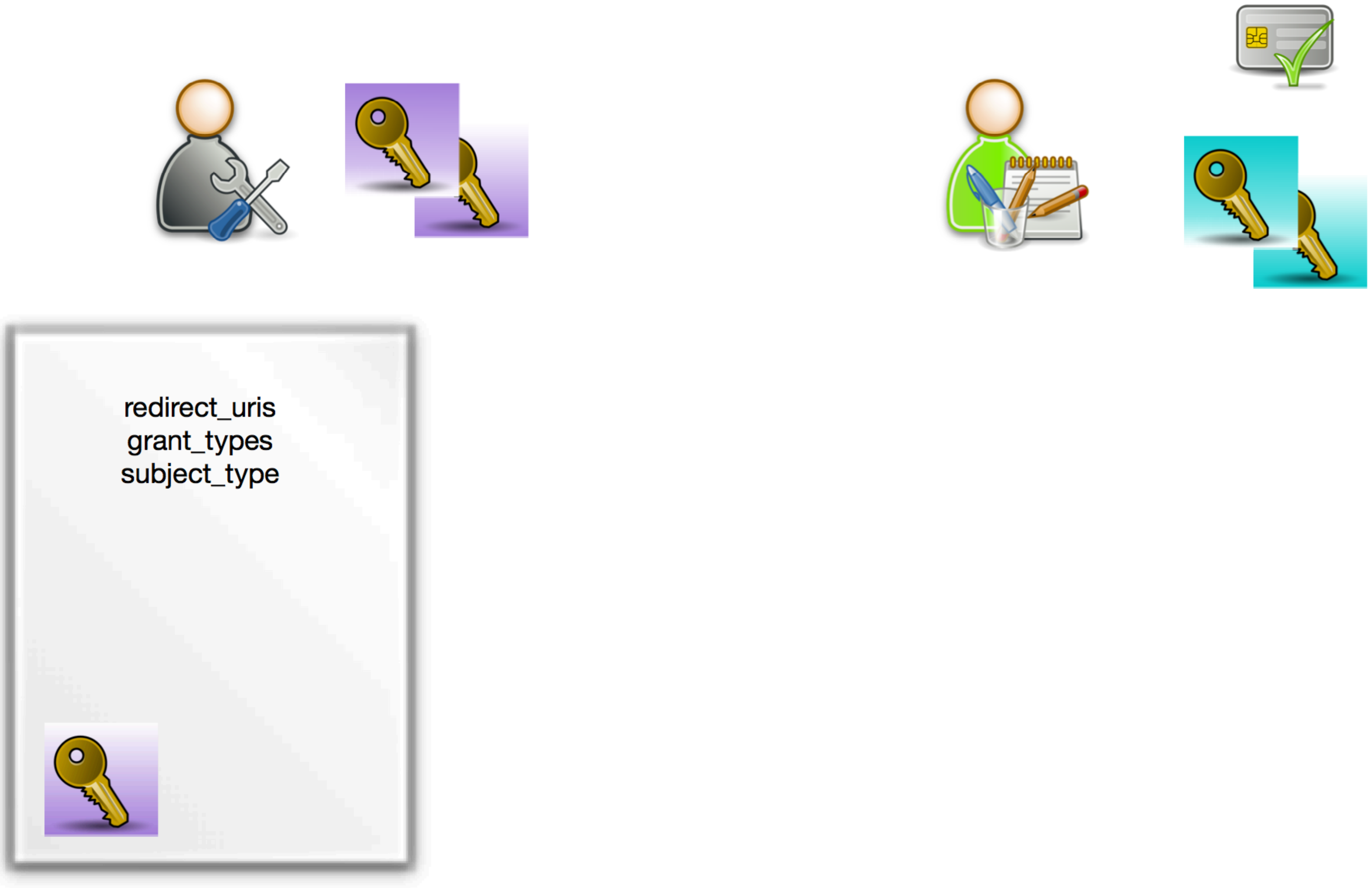


contacts
logo_uri
policy_uri
tos_uri

scope
claims
token_endpoint_auth_method

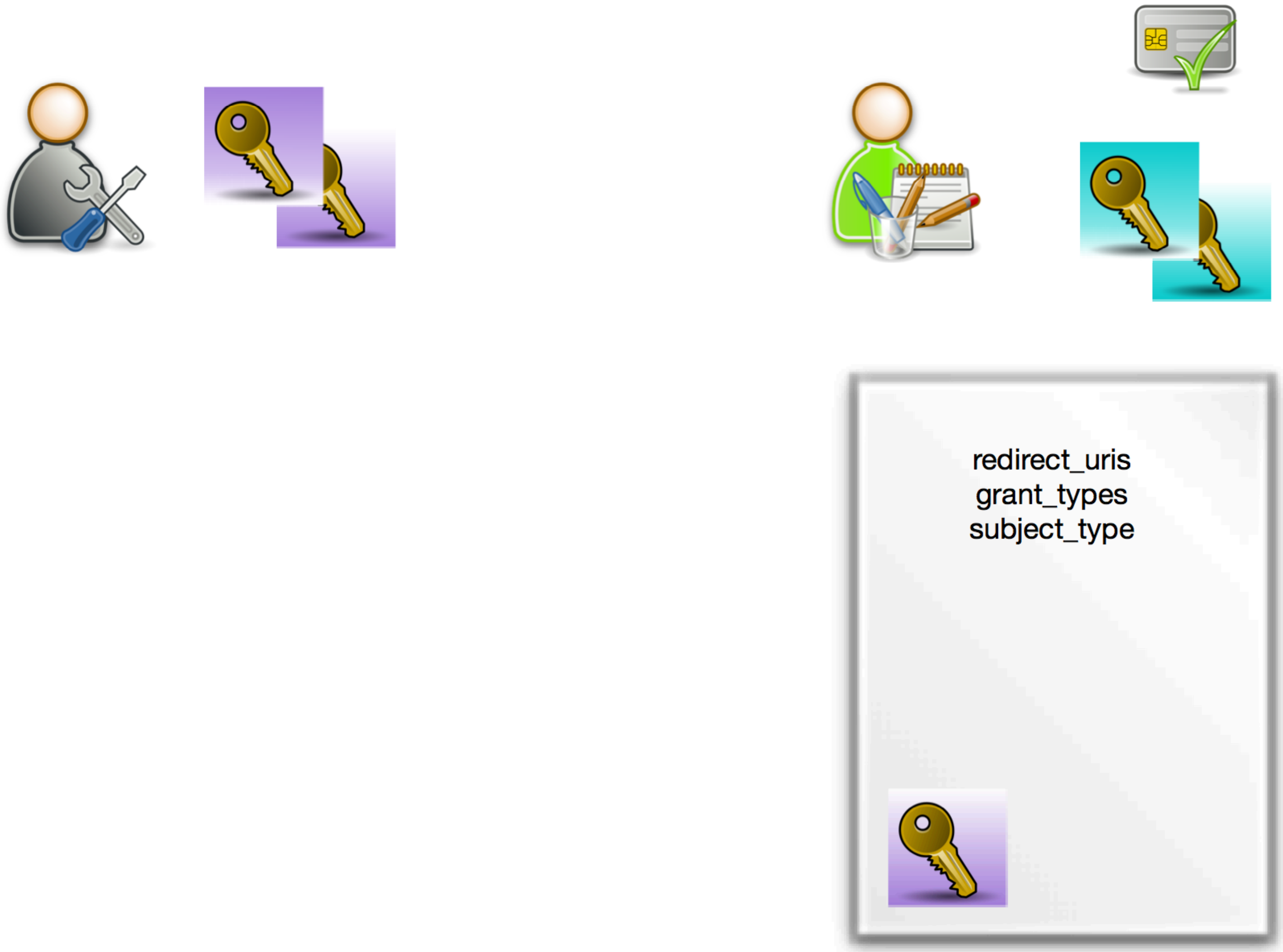
Within an organization

Entity specific information



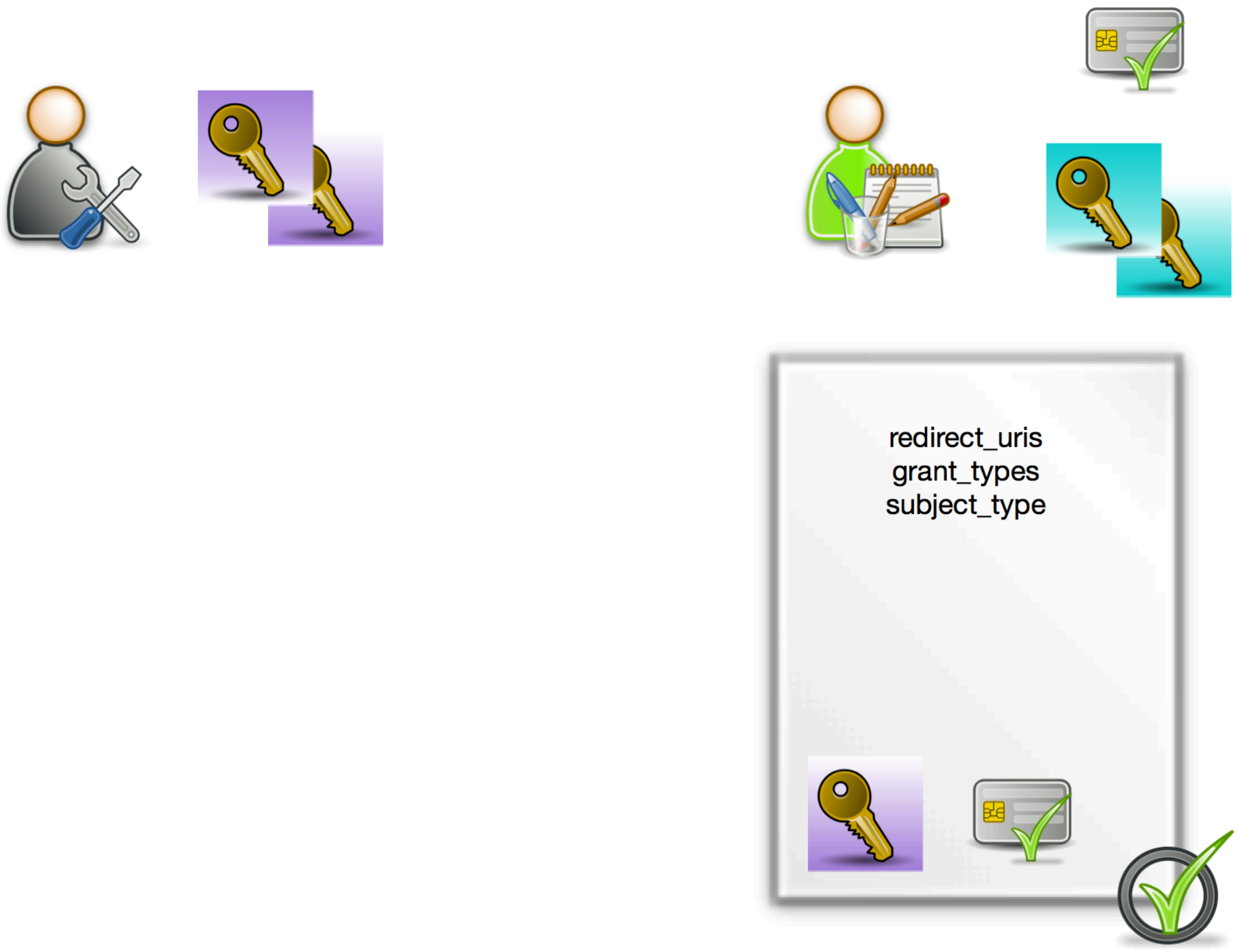
redirect_uris
grant_types
subject_type

Transfer to Organization coordinator (OC)



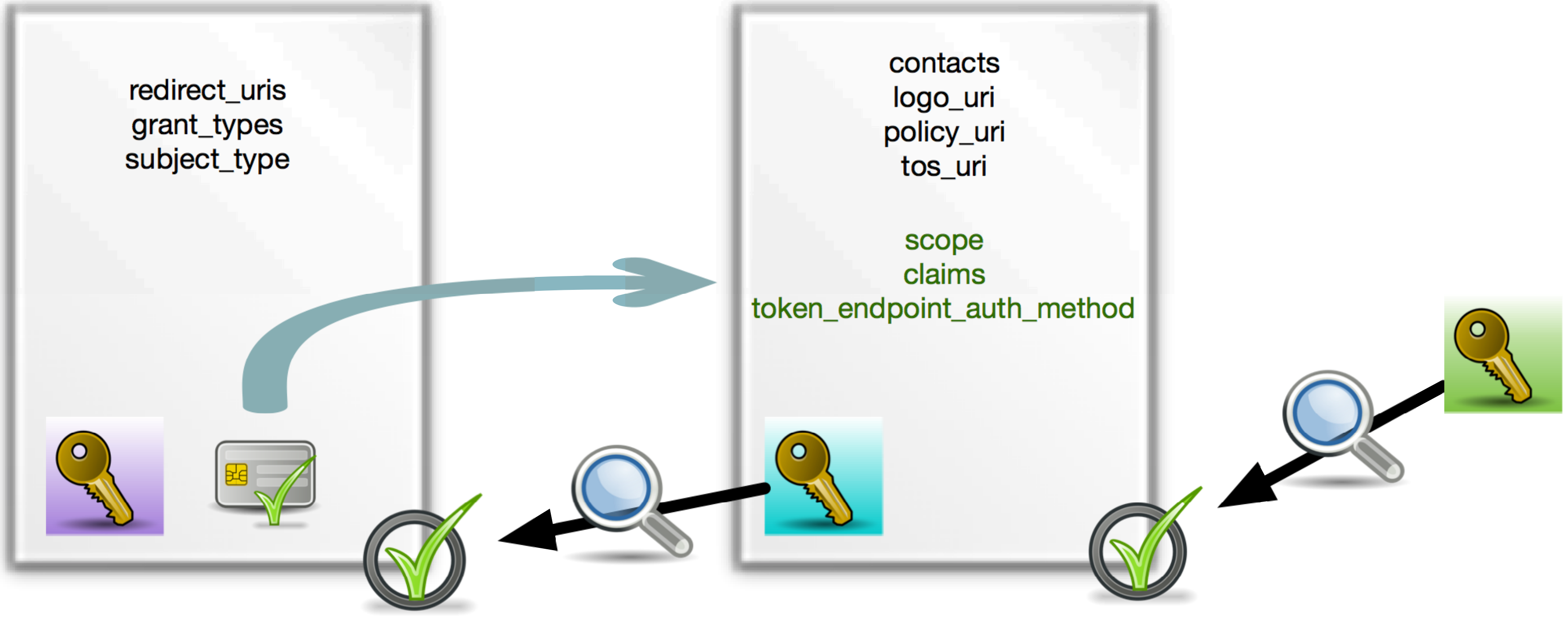
redirect_uris
grant_types
subject_type

OC: verifies, modifies and signs



redirect_uris
grant_types
subject_type

Unpacking a metadata statement

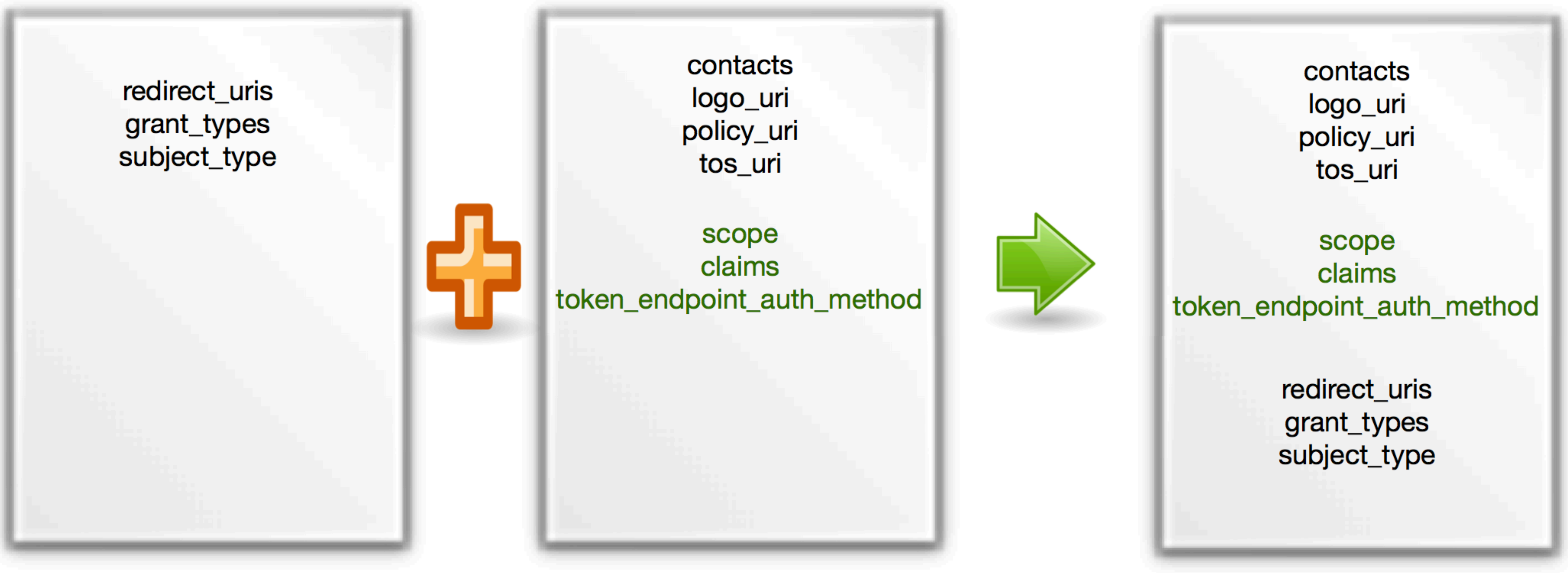


redirect_uris
grant_types
subject_type

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