OIDC Fed and around - status update

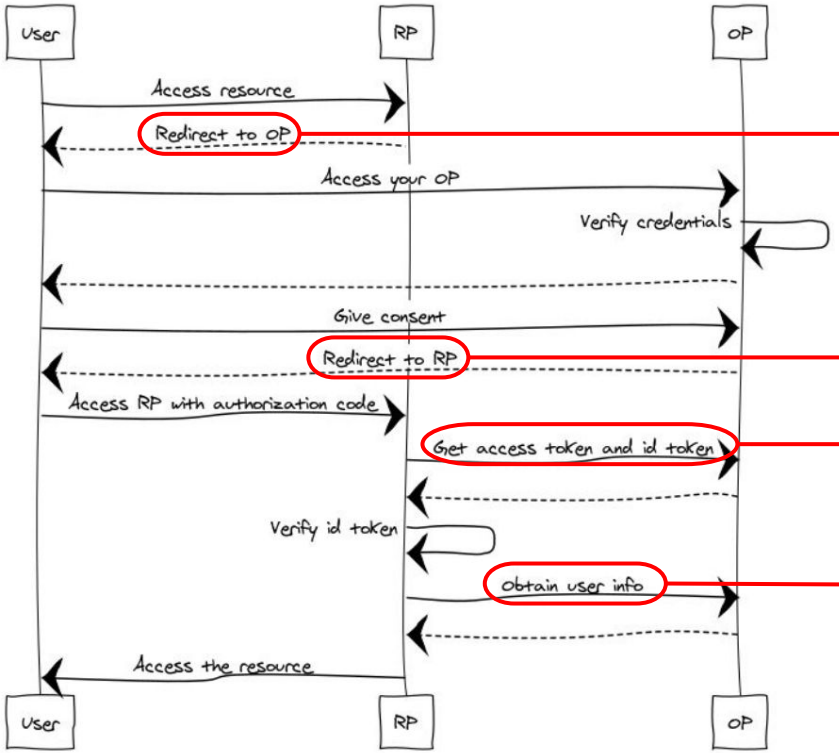
Davide Vaghetti
GEANT OIDCFed Team (GN4-2 JRA3 Task 3 1.A)
AARC JRA1 T3
Consortium GARR

REFEDS, Linz
May 29th, 2017

OIDC: Actors

- The **User** who wants to access a protected resource, either by himself or through an application.
- The **Relying Party** (often called the Client) is the entity that will request and use an access token.
- The **OIDC Provider** (OP) is the entity that will release the access token.

OIDC: OP and RP needs to know about each other



RP redirect the user to the OP's **authorization_endpoint**

OP redirect the user to the RP's **redirect_uri**

RP exchange the code for an access_token at the **token_endpoint** (and authenticate…)

RP requests user claims at the OP's **userinfo_endpoint**

OpenID Connect Discovery and Dynamic Client Registration

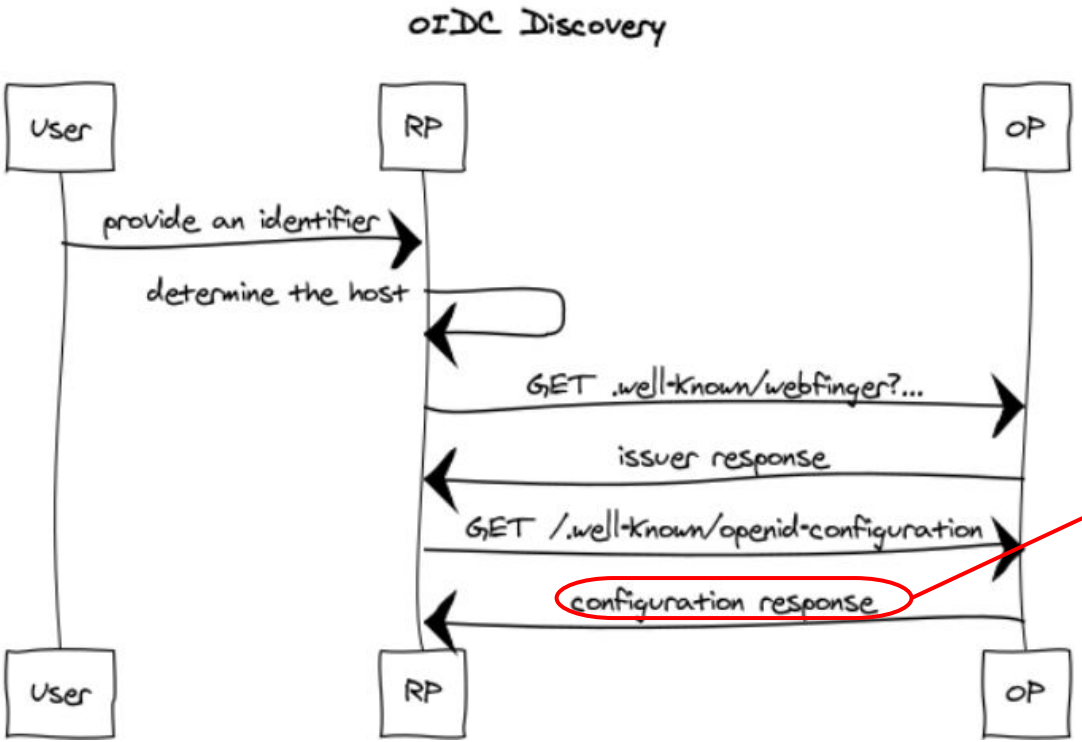
http://openid.net/specs/openid-connect-discovery-1_0.html

a mechanism for an OpenID Connect Relying Party to discover the End-User's OpenID Provider and obtain information needed to interact with it, including its OAuth 2.0 endpoint locations

http://openid.net/specs/openid-connect-registration-1_0.html

defines how an OpenID Connect Relying Party can dynamically register with the End-User's OpenID Provider, providing information about itself to the OpenID Provider, and obtaining information needed to use it, including the OAuth 2.0 Client ID for this Relying Party

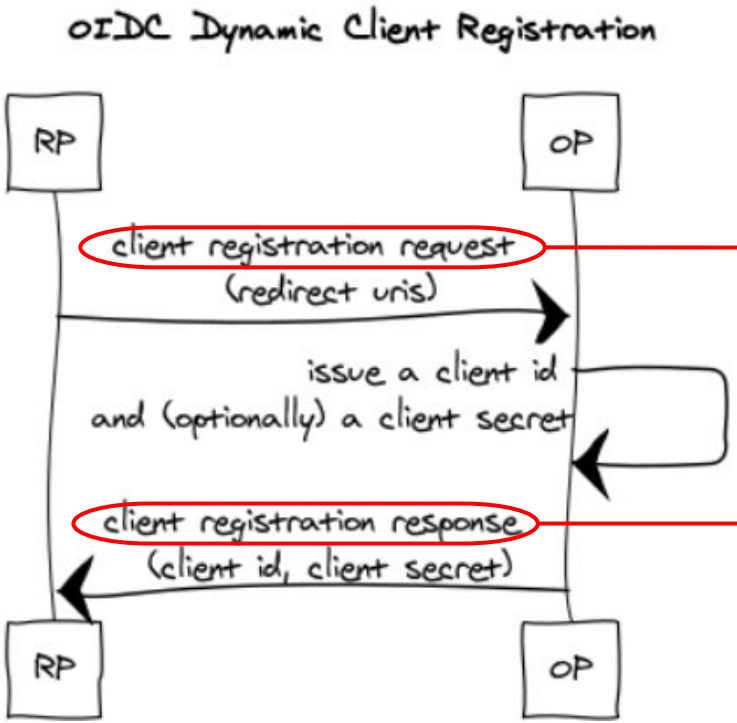
OpenID Connect Discovery 1.0



The **RP** receives and consumes the **OP** metadata (provider configuration).

No trust information is provided.

OpenID Connect Dynamic Client Registration 1.0



The **OP** receives a client registration request from the **RP**.

No trust information is provided.

The **OP** sends a client registration response to the **RP**.

No trust information is provided.

OpenID Connect Federation 1.0 - draft 03

http://openid.net/specs/openid-connect-federation-1_0.html

The OpenID Connect standard specifies how a Relying Party (RP) can discover metadata about an OpenID Provider (OP), and then register to obtain client credentials. During discovery and registration there is no automated mechanism for the OP or the RP to verify the information exchanged during this process. All the information is self-asserted.

In an identity federation context, this is not sufficient. The participants of the federation must be able to trust information provided about other participants in the federation.

This document describes ***how an identity federation can be built around a trusted third party, the federation operator****.*

Metadata statements

A metadata statement asserts metadata values about an entity (client or server).

Components:

- **signing_keys**: A JSON Web Key Set (JWKS) representing the public part of the entity's signing keys.
- **(signed) metadata_statements**: JSON object where the names are federation identifiers and the values a signed JSON documents containing compounded metadata statements rooted in that federation. There is one value per name.

Davide Vaghetti
davide.vaghetti@garr.it

GÉANT
Networks · Services · People
www.geant.org

This work is part of a project that has applied for funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).