
OpenID Connect

by Roland Hedberg

From OAuth2 to OpenID Connect



- ❖ OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol.
- ❖ It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

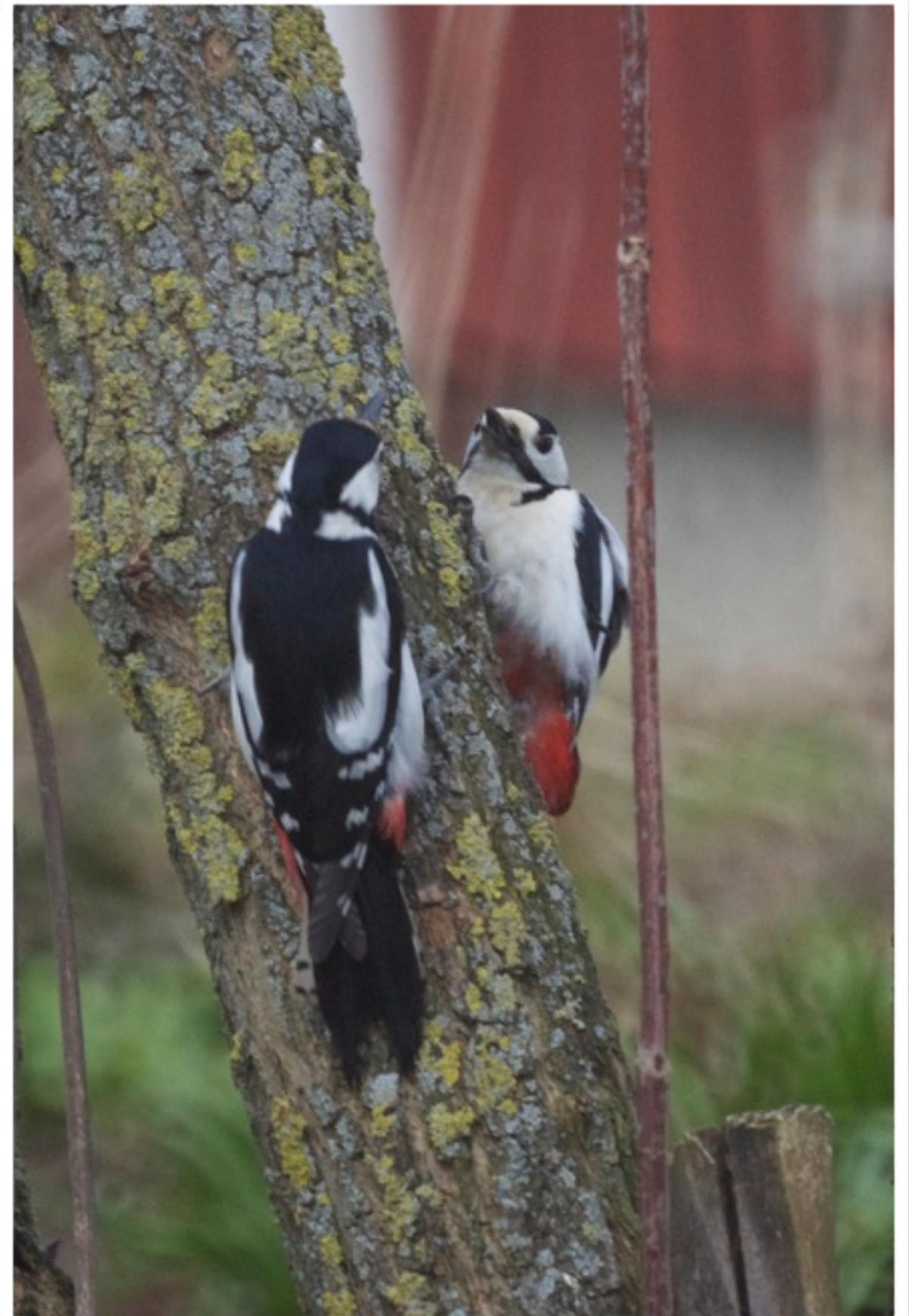
The differences

- ❖ Only authorization grant and implicit grant flows
- ❖ Dynamic provider discovery and client registration
- ❖ ID Token
- ❖ Additions / Clarifications / Constrictions
- ❖ UserInfo endpoint

Flows

- ❖ Authorization code
 - ❖ code
- ❖ Implicit
 - ❖ id_token
 - ❖ id_token token
- ❖ *Hybrid* (authorization code with a twist)
 - ❖ code id_token
 - ❖ code token
 - ❖ code id_token token

Dynamic provider discovery and client registration



Dynamic discovery and registration

1. Find the provider
2. Discover provider configuration info
3. Register client

1. Find the provider

- ❖ Webfinger (RFC 7033)
 - ❖ User identifier -> URL
 - ❖ carol@example.org ->

GET /.well-known/webfinger?

resource=acct:carol@example.com&

rel=http://openid.net/specs/connect/1.0/issuer

HTTP/1.1

Host: example.com

Webfinger response

HTTP/1.1 200 OK

Access-Control-Allow-Origin: *

Content-Type: application/jrd+json

```
{  
  "subject" : "acct:carol@example.com",  
  "links" :  
  [  
    {  
      "rel" : "http://openid.net/specs/connect/1.0/issuer",  
      "href" : "https://openid.example.com"  
    }  
  ]  
}
```

2. Discover provider info - query

GET /.well-known/openid-configuration HTTP/1.1

Host: openid.example.com

2. Discover provider info - response

- ❖ issuer
- ❖ jwks_uri
- ❖ *endpoints*
- ❖ *functions supported*
- ❖ *support for signing/encrypting algorithms*
- ❖ *policy/tos*

Required information

- ❖ issuer
- ❖ jwks_uri
- ❖ authorization_endpoint
- ❖ token_endpoint (*)
- ❖ response_types_supported
- ❖ subject_types_supported
- ❖ id_token_signing_alg_supported

demo

3. Client registration

- ❖ uris
- ❖ application information
- ❖ support for signing / encrypting algorithms
- ❖ key material
- ❖ server behavior
- ❖ client behavior

required information

❖ `redirect_uris`

Client registration response

- ❖ client_id
- ❖ possibly client_secret *and if so* client_secret_expires_at
- ❖ and the Authorization servers view of things

An Authorization Server

- ❖ MAY add fields the client didn't include.
- ❖ MAY reject or replace any of the Client's requested field values and substitute them with suitable values.
- ❖ MAY ignore values provided by the client, and MUST ignore any fields sent by the Client that it does not understand.

A Client can not

- ❖ modify a registration
- ❖ delete a registration

ID Token



ID Token

- ❖ a security token that contains Claims about the **Authentication** of an End-User by an Authorization Server when using a Client, and potentially other requested Claims.
- ❖ is represented as a JSON Web Token (JWT)

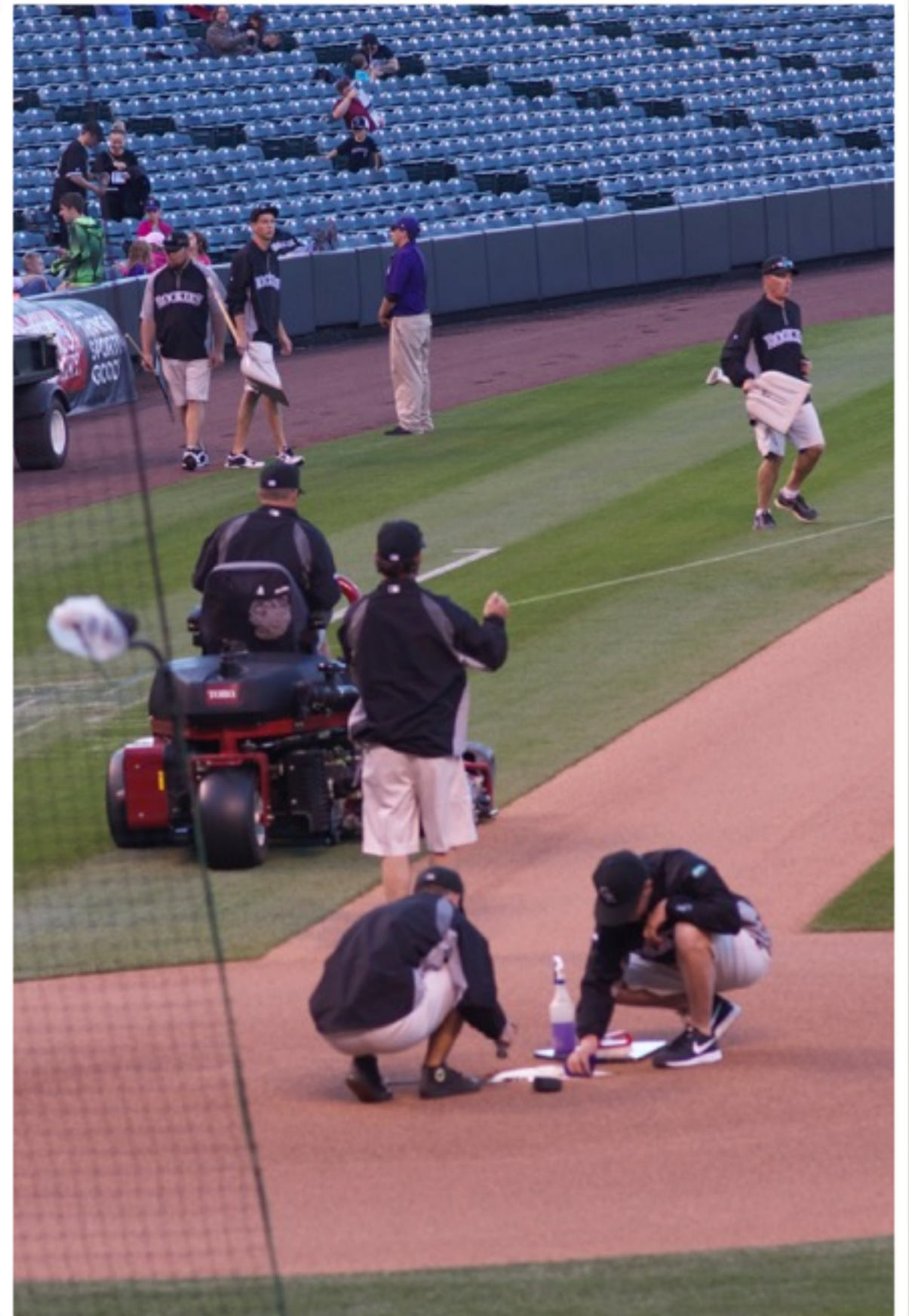
ID Token claims -required

- ❖ iss - Issuer Identifier for the Issuer of the response
- ❖ sub - Subject Identifier
- ❖ aud - Intended audience
- ❖ exp - Expiration time
- ❖ iat - Issued at
- ❖ auth_time - Authentication time
- ❖ nonce

ID Token claims - optional

- ❖ acr - Authentication Context Class Reference
- ❖ amr - Authentication Method References
- ❖ azp - Authorized party

Additions/ Clarifications/ Constrictions



OAuth2 Authorization Request - details

Parameters

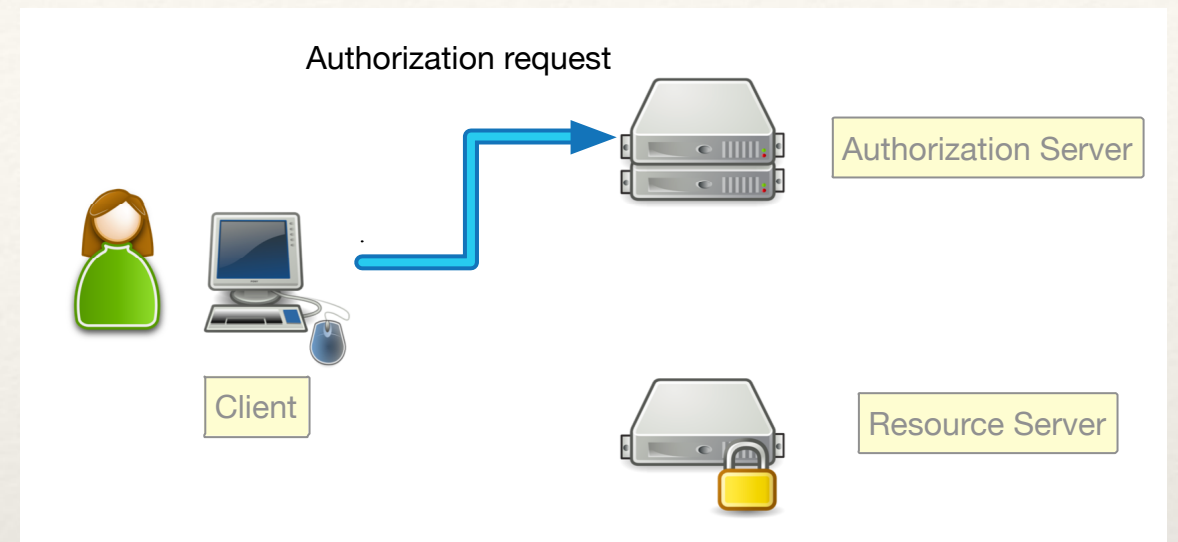
client_id

redirect_uri

response_type

scope

state



GET

http://example.com/authorization?state=1521671980316802035&redirect_uri=https://example.org/authz_cb&response_type=code&client_id=SFEBuhC7sp3a

Authentication Request - OpenID Connect extensions

- ❖ response_mode - The mechanism to use for returning parameters
- ❖ nonce - Associates client session with ID Token
- ❖ *Signed/encrypted Authentication Request*
- ❖ *End-user interactions*
- ❖ *Response details*

Signed/encrypted Authentication Request

- ❖ request - by value
- ❖ request_uri - by reference
- ❖ Single self-contained parameter
- ❖ Signed and / or encrypted (JWT)

End-user interactions

- ❖ display - How to display pages to End-User
- ❖ prompt - If the End-User should be prompted for re-authentication/consent
- ❖ max_age - allowed max time since last authentication
- ❖ ui_locales - End-User's preferred languages and scripts
- ❖ id_token_hint - ID Token previously issued
- ❖ login_hint - login identifier the End-User might want to use
- ❖ acr_values - requested Authentication Context Class Reference values

Response details

- ❖ claims
 - ❖ user_info
 - ❖ id_token
- ❖ claims specification
 - ❖ null
 - ❖ essential
 - ❖ value
 - ❖ values

UserInfo endpoint



User info

Set of standard claims

- | | | |
|----------------------|------------------|-------------------------|
| ❖ sub | ❖ profile | ❖ zoneinfo |
| ❖ name | ❖ picture | ❖ locale |
| ❖ given_name | ❖ website | ❖ phone_number |
| ❖ family_name | ❖ email | ❖ phone_number_verified |
| ❖ middle_name | ❖ email_verified | ❖ address |
| ❖ nickname | ❖ gender | ❖ updated_at |
| ❖ preferred_username | ❖ birthdate | |

claims types

- ❖ Normal
- ❖ Aggregated
- ❖ Distributed

Links to documents

- ❖ OpenID Connect Core 1.0 incorporating errata set 1
- ❖ OpenID Connect Discovery 1.0 incorporating errata set 1
- ❖ OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 1