Contribution ID: **13** Type: **Full presentation: long (25 mins.)**

Orpheus - Managing differences in the variety of OpenID Providers

Tuesday, 3 November 2020 10:00 (25 minutes)

Background

OpenID Connect is widely used in modern Authentication and Authorization Infrastructures including the infrastructures of multiple EU projects like the European Open Science Cloud and also EGI. Also in the non-academic world everyone moves to OpenID Connect (e.g. Google, Apple, IBM).

Despite its wide adoption OpenID Connect is very complex. OpenID Connect is an identity layer on top of OAuth2; there is a core profile for OpenID Connect, but also additional profiles; there are extensions for OAuth2; there are several draft extensions for both OAuth2 and OpenID Connect; all of these might be supported by OpenID Connect Providers, but also might not. And because OpenID Connect finds wide adoption there are naturally a lot of different providers, that all support different aspects. Some might even support certain features, but with small violations of the specification / draft. All of this makes it difficult if one has to deal with multiple providers.

Orpheus

Opheus is a web based tool for analysing and characterising OIDC Provider- and Relying Party implementations of OpenID Connect.

For that Orpheus supports specifically features targeted at developers and operators of OpenID Connect based infrastructures:

- Comparison of OIDC providers
- Analysis of the supported features of OIDC providers
- Live testing capabilities for testing the claimed features
- No implementation effort
- Live testing capabilities for many different flows
- Authorization Code Flow
- Device Code Flow
- Refresh Flow
- Token Revocation Flow
- Debugging functionionality:
- Perform a working OIDC flow.
- All relevant data including all the communication between the parties is given.
- User - Developer Interaction:
- Help debugging OIDC related problems.
- Multiple reasons for failed authorization:
  - misconfigured OIDC client
  - released attributes by the home identity provider
  - user's account missing attributes
  - ...
- Hard to debug, because linked to account and real identity.
- User can perform OIDC flow against orpheus and share all relevant data in a privacy compliant way with the developer.

Orpheus focuses on a universal approach so large numbers of OpenID providers can be supported. It is easy to add new providers and to extend the list of comparable features.

Future Work

The current development focuses on making orpheus more modular so it can be used more easily for the different use cases. Also more features will be added in the future. An idea for a future extension is to provide a public API that gives information which features are supported by the different providers.

Primary authors: ZACHMANN, Gabriel; Dr HARDT, Marcus (Karlsruhe Institute of Technology); Dr STEVANOVIC, Uros (KIT-G)

Presenter: Dr STEVANOVIC, Uros (KIT-G)

Session Classification: How to make your service more secure?