Contribution ID: **11** Type: **Presentation short (15 min)**

mytoken - secure and long term authentication (without refresh tokens)

Tuesday, 19 October 2021 14:40 (15 minutes)

Background

OpenID Connect (OIDC) is the technological basis of many modern Authentication and Authorisation Infrastructures, which are currently being used and established in multiple European projects. Also, the non-academic sector (e.g. Microsoft, Google, Apple, IBM) moved to OIDC.

Despite OIDC being mostly used within web browser based applications, support for the command line and for API usage are required for complex workflows. The oidc-agent
tool was our first step to enabling OIDC's "Access Tokens" on the command line. Access Tokens are short lived, with a life-time of usually one hour.

Use-cases that involve long running jobs, however, require authentication capabilities throughout their entire runtime, thereby challenging the security concept of short lived tokens.

Mytoken

This contribution addresses complex scenarios (e.g. compute jobs), in which access tokens need to be obtained over extended time spans, e.g. to load and store data or to access other resources.

We introduce a client-server solution and a new token type, called mytoken. Mytokens are easy to use, (can be) long lived, and allow limiting the functionality of the token, to address security concerns that arise from long living tokens.

The mytokens themselves are very flexible, as they can be
- used for easily obtaining access tokens on any device
- easily transferred to other devices
- created non-interactively from another mytoken
- easily passed around without giving up security
- restricted according to the use case.

Mytokens may have **capabilities** and **restrictions**. Capabilities define
well-defined actions for which a mytoken may be used (e.g. obtain an
Access Tokens, obtain another mytoken), while restrictions may be used for
a fine grained access control, for example:

- Time range in which a mytoken may be used
- Location (IP, Geo-IP) from where the mytoken may be used
- OIDC (AT scope, audience) to specify what kind of Access Tokens may be obtained
- Number of usages for a specific action

Mytokens can contain lists of restrictions, which allows to easily
define a mytoken, that could:
1. Allow job submission in the first hour after creation of the mytoken
2. Allow data access in the first two hours after creation

3. Allow nothing for one day
4. Allow data access (store output) between 24 and 36 hours after creation.

By submitting my abstract, I agree that my personal data is being stored in accordance to conference Privacy Policy

Most suitable track

Delivering services and solutions

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

Presenter: HARDT, Marcus (KIT-G)

Session Classification: Innovating Services Together - Presentations