OpenID Connect Identity Federations at lightning speed

Author

Maarten Kremers, SURFnet maarten.kremers@surfnet.nl

Keywords

Identity federation, Identity Management, OpenID-Connect, eduGAIN, new technology.

Abstract

OpenID Connect (OIDC) is a simple identity layer on top of the OAuth 2.0 protocol, which acts in a similar way like SAML2 as a protocol for identification and authentication.

Current identity federations in the academic area are, with almost no exception, SAML2 based. There is however a strong and rising interest for using OpenID Connect as a protocol for identification and authentication. The OpenID Connect protocol is being perceived as a simpler, JSON/REST based protocol, and is being designed, besides web-based applications, to also support native apps and mobile applications. OpenID Connect is adopted by the large players in the industry, like Amazon, Google, Facebook & Microsoft. Furthermore the REFEDS Survey 2016 showed a great interest from federations for supporting OpenID Connect[1].

There is, however, no support for building federations in the basic standards of OpenID Connect, for identity federations as we know them currently in the academic area.

Roland Hedberg et al [2], have written a specification for creating an identity federation using OpenID Connect, hereby taking into account some lessons learned from the identity federations as we know them know.

The GN4-2 Trust & Identity Next Generation Technology task [3] is taking the next step by further implementing and developing the specification, with as goal to create running implementations with the tools needed to run it as a federation and the creation of a technology profile for eduGAIN. Our first set of objectives are planned for June 2017.

In this presentation we will present – in lightning talk style – an overview of the work done from the start in 2016 to June 2017, with the topics around:
* Use cases at the levels of campuses, federations and inter-federation
* Implementations & further standardisation
* R&E Federation specific components (attribute groups, “entity categories”)
* Planned pilots
* The next steps

With this presentation we want to enlighten anybody interestested in identity federations on this next generation T&I work and gather feedback.

Acknowledgements

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 731122 (GN4-2).

The author is deeply indebted to the whole GN4-2 Joint Research Activity 3 (JRA3) Team, especially the people active in the OIDC-federation subtask.

References

[1] REFEDS Survey 2016 - https://geant.app.box.com/s/8f30ptw5houmauurfqfupw3ruz3x9enu
[2] OIDC Federation 1.0 - https://github.com/rohe/pyoidc/blob/master/oidc_fed/oidcfed.txt
[3] GN4-2 T&&I OIDCfed https://wiki.geant.org/display/gn42jra3/T3.1A+OpenID+Connect+Federation

Author Biography

Maarten Kremers joined SURFnet in 2007 and is a Technical Product Manager Trust & Identity. He is involved as project member and project manager in the innovation and development of collaboration and identity management infrastructure SURFconext. Furthermore he is currently leading the GN4 Trust & Identity task on the next generation T&I technology development, amongst others on user centric identity management, cross-sector federations and OpenID Connect for identity federations. He holds a MSc degree in Information Management from Tilburg University.