1000 things you always want to know about SSO but you never dare to ask

Luis Rodríguez Fernández

CERN Authentication

- Enhanced SSO solution for CERN Web Applications
- Authentication methods
  - Standard
  - Forms
  - Kerberos or Windows
  - Certificates
  - Two Factor (strong auth)
  - Smartcard
  - Yubikey
  - SMS One Time Password
  - Google Authenticator
  - Federation
  - Public Services
  - Google
  - Facebook
  - Live
  - Yahoo
  - Orange

SAML2

- Security Assertion Markup Language
- OASIS
- Organization for the Advancement of Structured Information Standards
- CERN SAML2 SSO
- Web Browser SSO Profile
- SP-Initiated SSO Profile
- Oracle WebLogic applications
- SAML2 module
- Other
- Shibboleth

OAuth2

- Started by Blaine Cook: Twitter OpenID implementation
- Standard developed within the IETF (rfc6749)
- Internet Engineering Task Force
- No “out-of-the-shelf” solutions
- CERN OAuth2 Authorization Service
  - Client Credentials Grant
  - "Machine-to-Machine" authentication (e.g. java)
  - Resource Owner & Authorization Server
  - ORDS (Oracle Rest Data Services)
  - Different grants supported
  - Suitable for user-agent-based clients (e.g. javascript)

Challenges

- Applications integration
- Ad hoc auth/authz solutions
- Legacy
- Commercial solutions
- Heterogeneous developer community
- Web
- Desktop
- Controls
- Sysadmins
- Different platforms
- Virtual machines (openstack)
- Containers (magnum, openshift)
- One solution does not fit all scenarios
  - /web/ui → SAML2
  - /api → OAuth2

References

- Luis Rodríguez Fernández (December 2013). UKOUG. Weblogic as a Service Provider for CERN Web Applications [http://cern.ch/go/8Tjx]
- Emil Kleszc (September 2016). OAuth protocol for CERN Web Applications [http://cern.ch/go/D89g]
- Albin Stjerna (August 2017). IT-DB storage API [https://github.com/cerndb/storage-api]

Acknowledgements

- All the CERN IT-DB members and specially the IMS section: Borja Aparicio, Lukas Gedvila, Arash Khodabandeh, Antonio López, Nicolas Marescaux, Damian Moskalik, Antonio Nappi, Miroslav Potocky, Paul Smith, Aimilios Tsouvelakakis, Artur Wiecek.
- Oracle openlab team: Cris Pedregal, Pauline Mahrer, Jean Phillippe Breyssse, David Ebert
- Special thanks to:
  - álvaro gonzález álvarez
  - albin stjerna
  - emil kleszc
  - emmanuel ormmancey