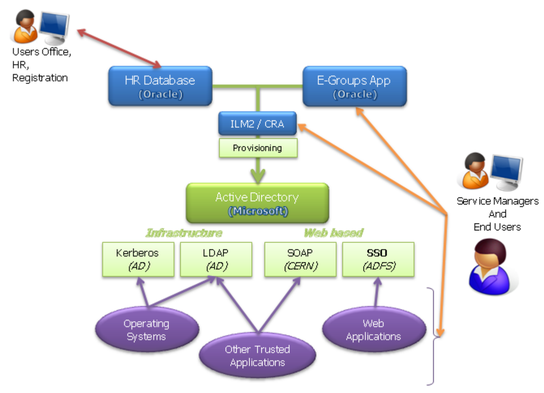
1000 things you always want to know about SSO but you never dare to ask

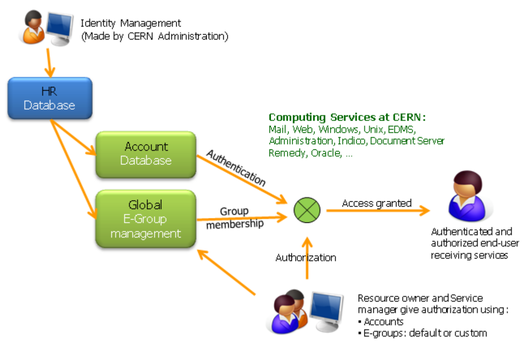
16th International Conference on Accelerator and Large Experimental Control Systems (ICALEPCS 2017)

Luis Rodríguez Fernández

CERN Authentication

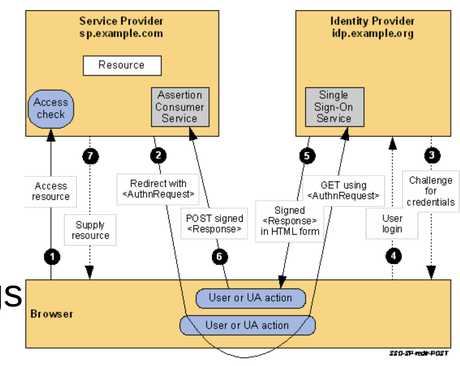
- Enhanced SSO solution for CERN Web Applications
- Authentication methods
  - Standard
    - Forms
    - Kerberos or Windows
    - Certificates
  - Two Factor (strong auth)
    - Smartcard
    - Yubikey
    - SMS One Time Password
    - Google Authenticator
- Federation
- Public Services
  - Google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

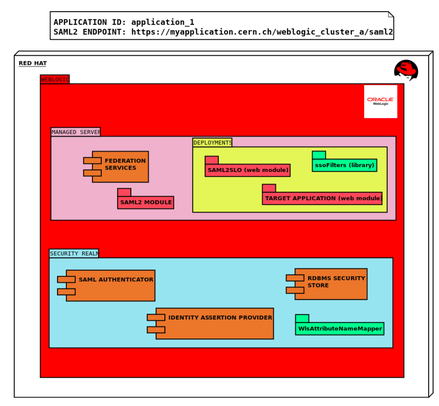


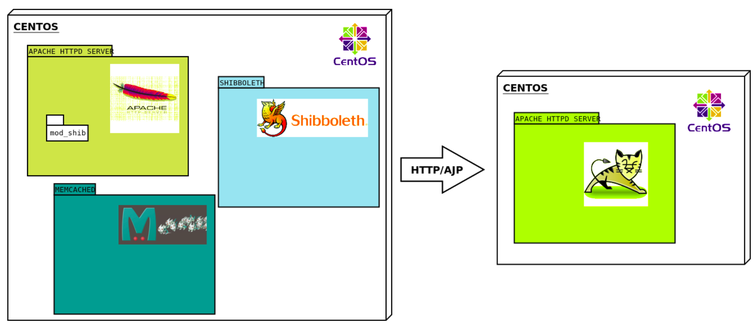


SAML2

- **S**ecurity **A**ssertion **M**arkup **L**anguage
- **OASIS**
  - **O**rganization for the **A**dvancement of **S**tructured **I**nformation **S**tandards
- **CERN SAML2 SSO**
  - Web Browser SSO Profile
    - SP-Initiated SSO: Redirect/POST Bindings
  - Oracle WebLogic applications
    - SAML2 module
  - Other
    - Shibboleth

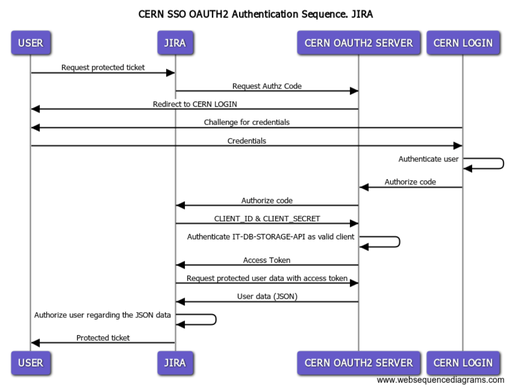


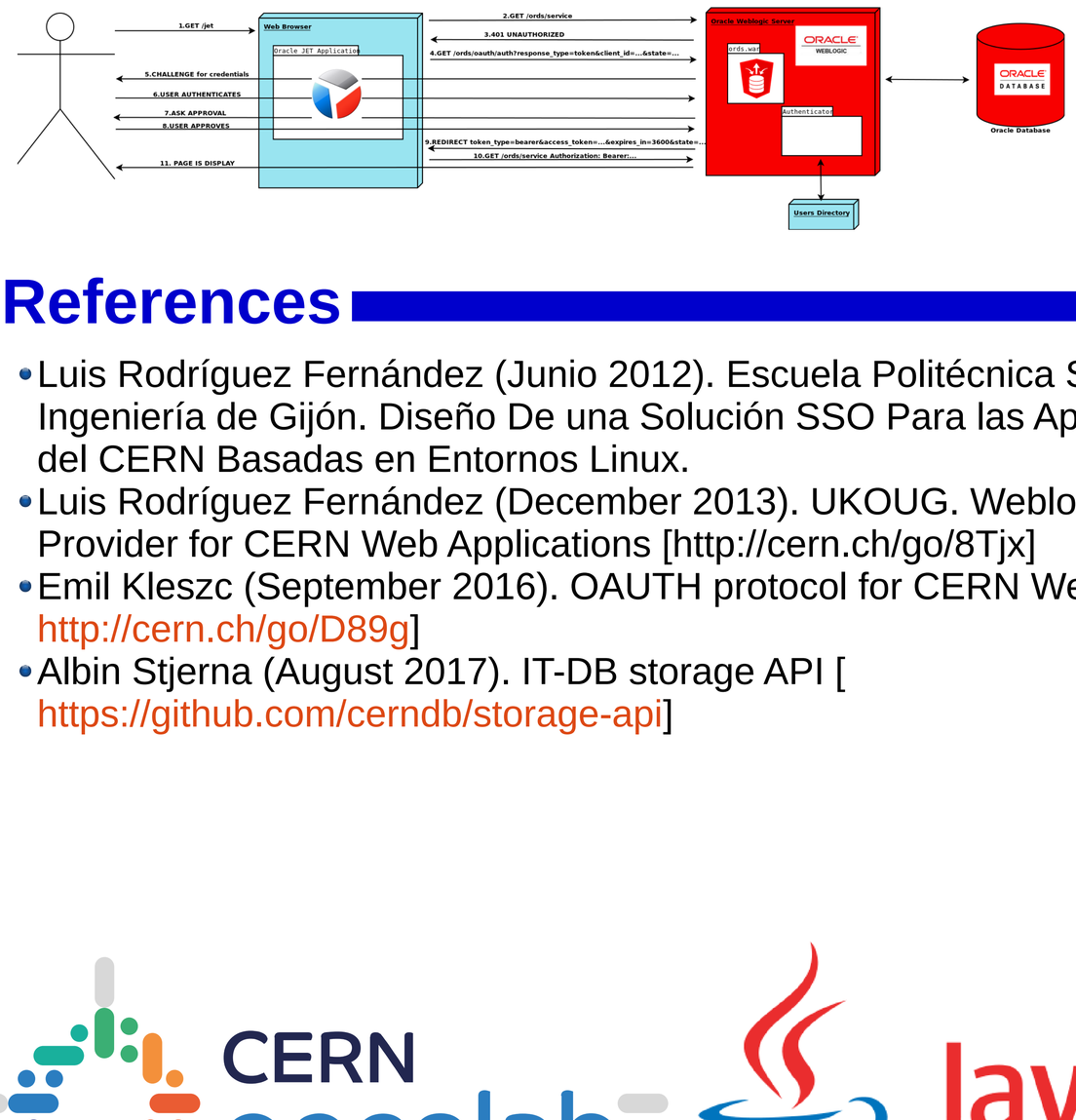




OAUTH2

- Started by Blaine Cook: Twitter OpenID implementation
- Standard developed within the IETF (rfc6749)
  - **I**nternet **E**ngineering **T**ask **F**orce
- No “out-of-the-shelve” solutions
- **CERN OAUTH2 Authorization Service**
  - Client Credentials Grant
    - “Machine-to-Machine” authentication (e.g. java)
    - Resource Owner & Authorization Server
  - **ORDS (O**racle **R**est **D**ata **S**ervices)
    - 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 (Junio 2012). Escuela Politécnica Superior de Ingeniería de Gijón. Diseño De una Solución SSO Para las Aplicaciones Web del CERN Basadas en Entornos Linux.
- 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 Gedvilas, Arash Khodabandeh, Antonio López, Nicolas Marescaux, Damian Moskalik, Antonio Nappi, Miroslav Potocky, Paul Smith, Aimilios Tsouvelekakis, Artur Wiecek.
- **Oracle openlab** team: Cris Pedregal, Pauline Mahrer, Jean Phillipe Breysse, David Ebert
- **Special thanks to**:
  - Álvaro González Álvarez
  - Albin Stjerna
  - Emil Kleszc
  - Emmanuel Ormmancey