



# OAuth protocol for CERN Web Applications

CERN openlab Summer Student  
Supervisor: Luis Rodriguez Fernandez  
IT-DB-IMS

Emil Kleszcz  
([emil.kleszcz@cern.ch](mailto:emil.kleszcz@cern.ch))

> **18/08/2016**

*Background image: Shutterstock*



- › How CERN Java Web Application can make use of OAuth2 protocol?
- › Comparison of SAML2 and OAuth2 protocols,
- › Providing SSO (Single Sign-On),
- › Integrate with current infrastructure.



**vs**



# Challenges

- › **Find the best solution: easy to maintain and secure**
- › **SAML2 has some limitations:**
  - For instance, logout protocol session fails if one or more participants fail in the session (solution delete cookies)



# Single Sign-On (SSO)

## CERN Single Sign-On

Sign in with a public service account



Sign in with an external public service

*Reminder: you have agreed to comply with the CERN computing rules*



To use this feature, you must own an account in one of the public services available below.

OpenID

Please click on your preferred account provider:

facebook

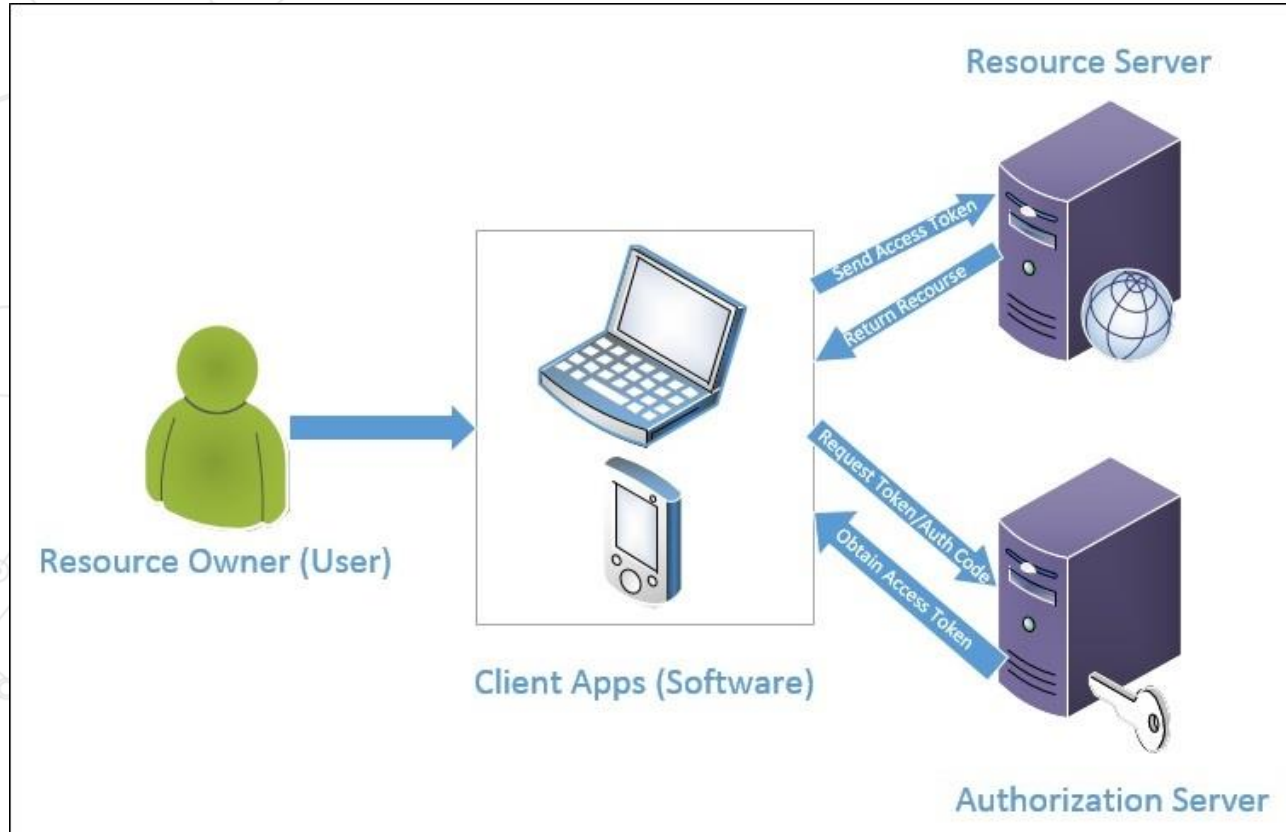
Google™

Windows Live

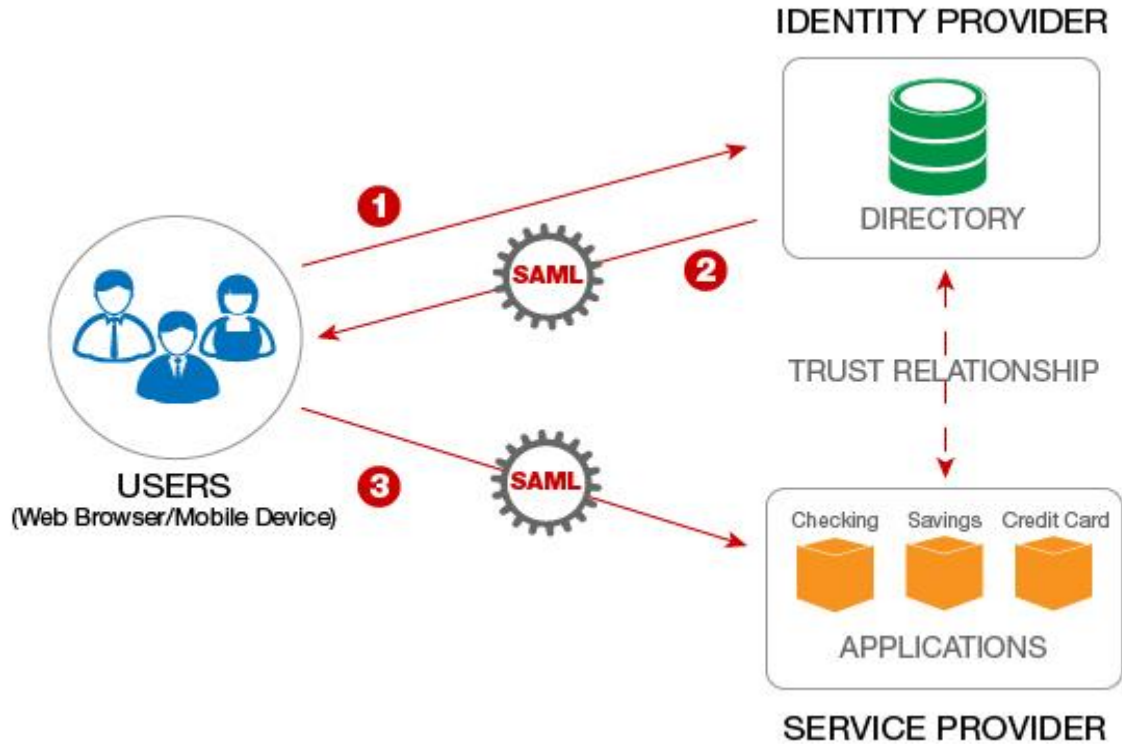
YAHOO!

orange™

# OAuth2



# SAML2



# Best solution?



# Comparison (pros & cons)

- › **OAuth 2.0 - simpler and more standardized solution (native),**
- › **SAML2 - more complete specification (web),**
- › **Both work fine for SSO,**
- › **They are complementary.**





# Results & Future

- › **Proof of Concept: [github.com/tr0k/OAuth2LibPoc](https://github.com/tr0k/OAuth2LibPoc)**
- › **Entries on blog ([db-blog.web.cern.ch](http://db-blog.web.cern.ch))**
- › **Testing on Oracle Java Cloud**



# Thank you for attention 😊

