

Federated authentication in Keystone Identity Service

Paweł Pamuła

supervisor:
Marek Denis



1

OPENSTACK CLOUD

OPENSTACK CLOUD



HORIZON
DASHBOARD

KEYSTONE



**IDENTITY
SERVICE**

NOVA



**COMPUTE
NODE**

GLANCE



**IMAGE
SERVICE**

SWIFT



**OBJECT
STORE**

QUANTUM



NETWORKING

CINDER



**VOLUME
SERVICE**

OPENSTACK CLOUD



HORIZON
DASHBOARD

KEYSTONE



**IDENTITY
SERVICE**

NOVA



**COMPUTE
NODE**

GLANCE



**IMAGE
SERVICE**

SWIFT



**OBJECT
STORE**

QUANTUM



NETWORKING

CINDER



**VOLUME
SERVICE**



2

KEYSTONE IDENTITY SERVICE

● KEYSTONE IDENTITY SERVICE

- establishes identity

- grants privileges

- provides a catalogue of services



3

KEYSTONE WORKFLOW

AUTHENTICATION WORKFLOW



User



Keystone



Database



Service



AUTHENTICATION WORKFLOW



User



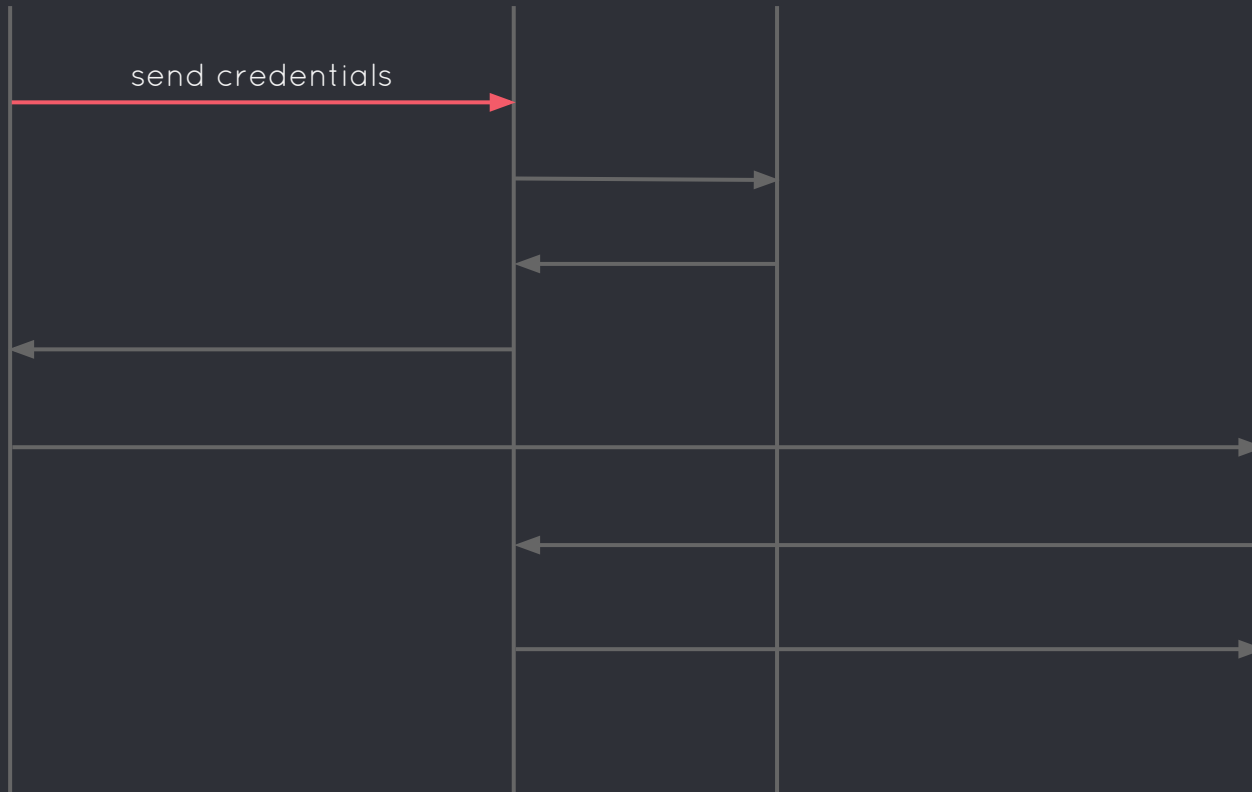
Keystone



Database



Service



AUTHENTICATION WORKFLOW



User



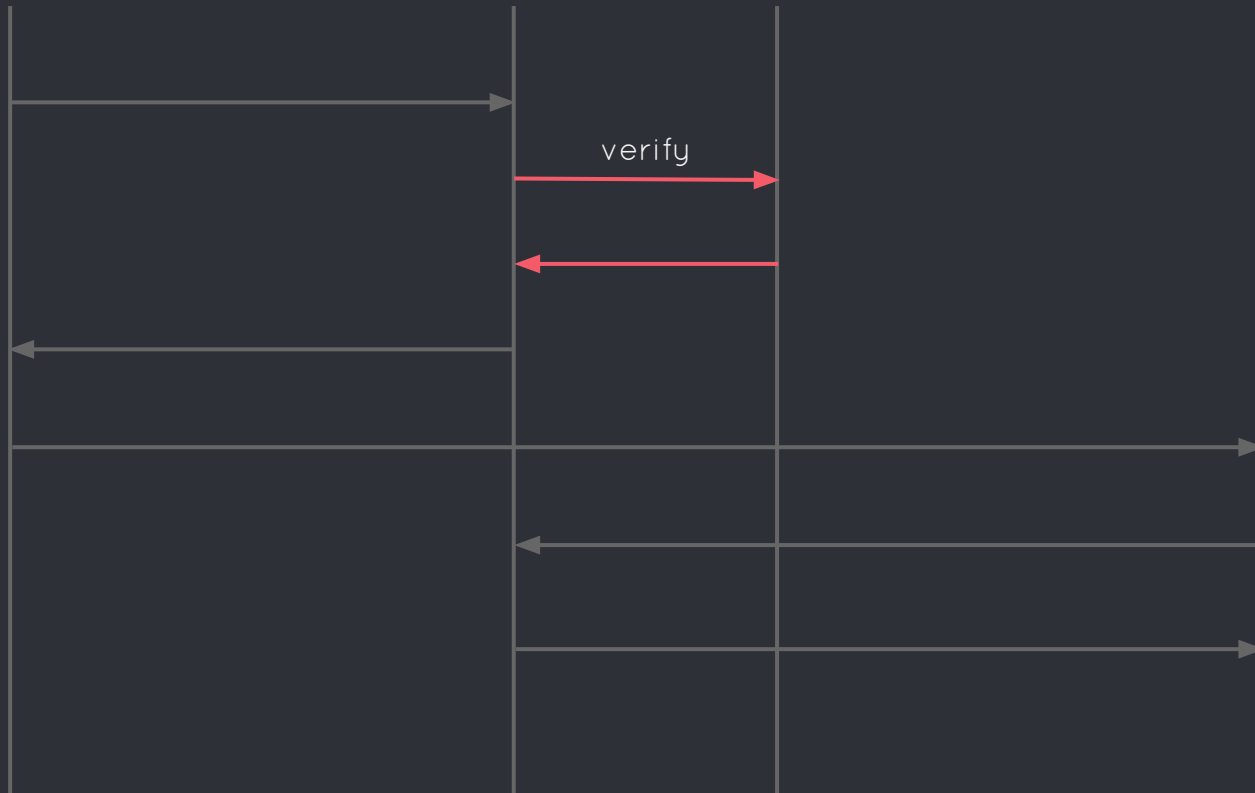
Keystone



Database



Service



AUTHENTICATION WORKFLOW



User



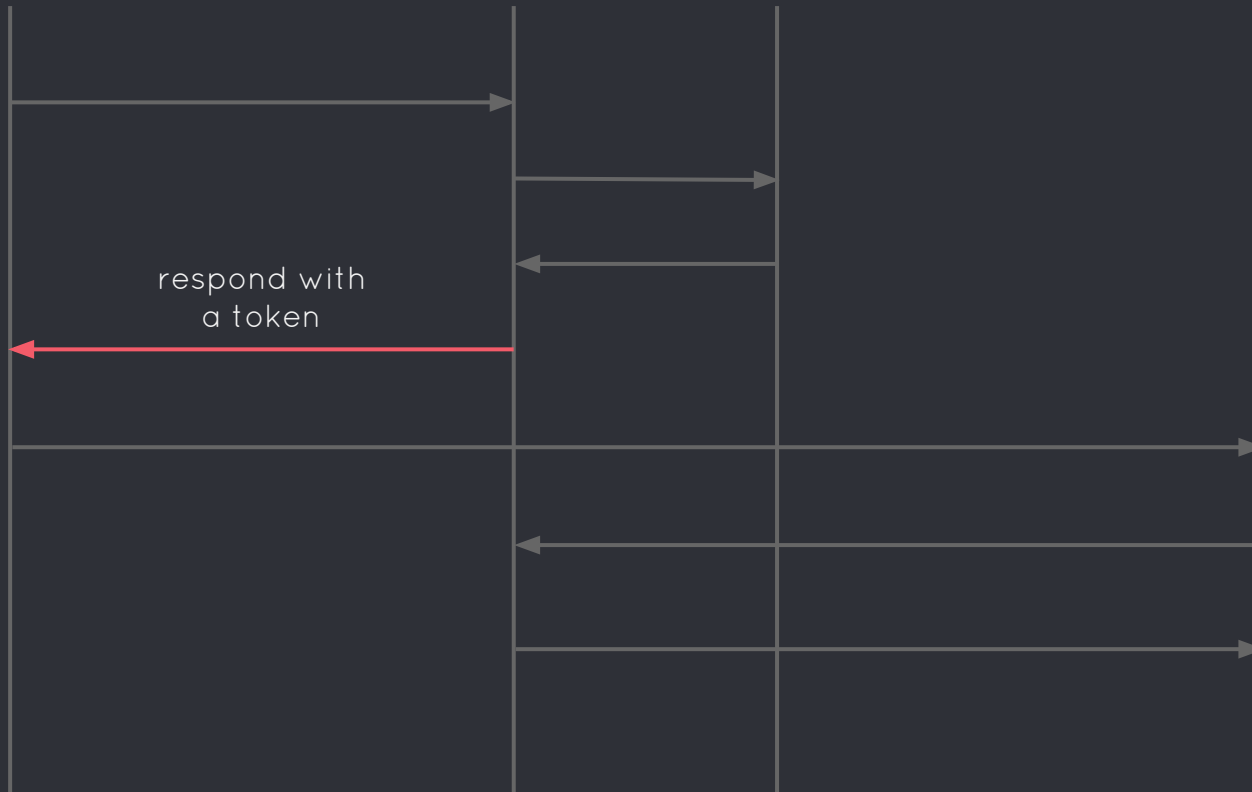
Keystone



Database



Service



AUTHENTICATION WORKFLOW



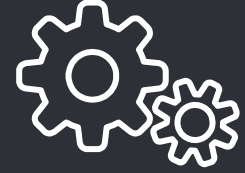
User



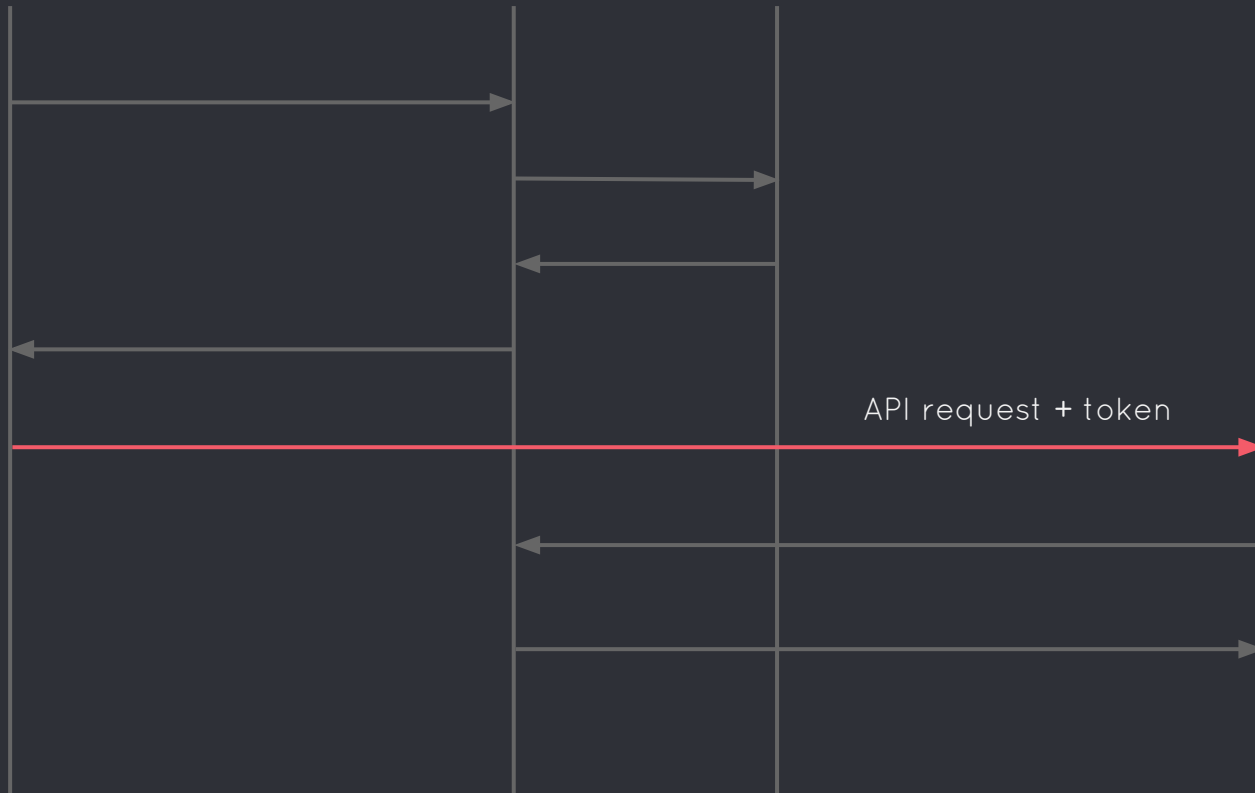
Keystone



Database



Service



AUTHENTICATION WORKFLOW



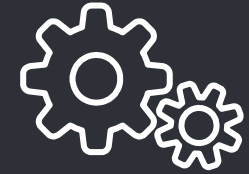
User



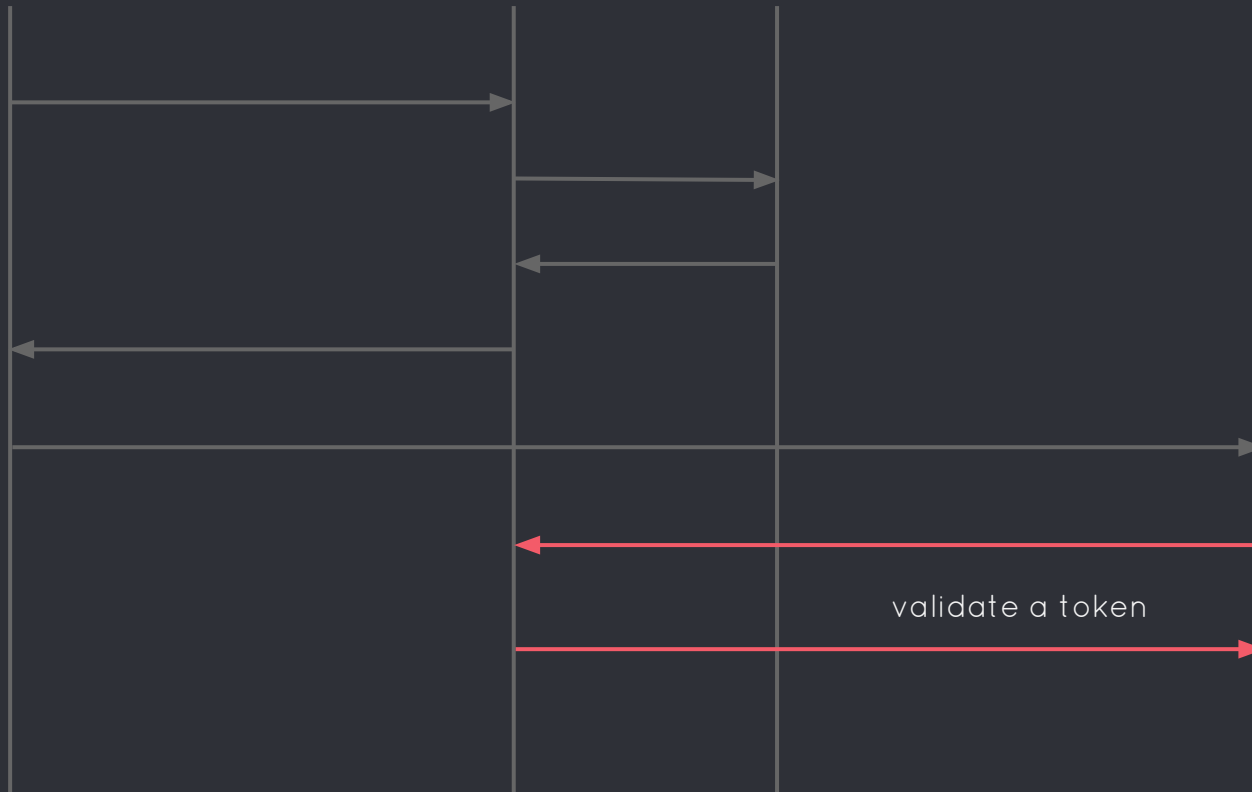
Keystone



Database



Service



AUTHENTICATION WORKFLOW



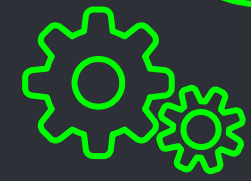
User



Keystone



Database



Service



AUTHENTICATION WORKFLOW



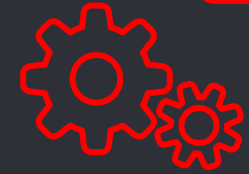
User



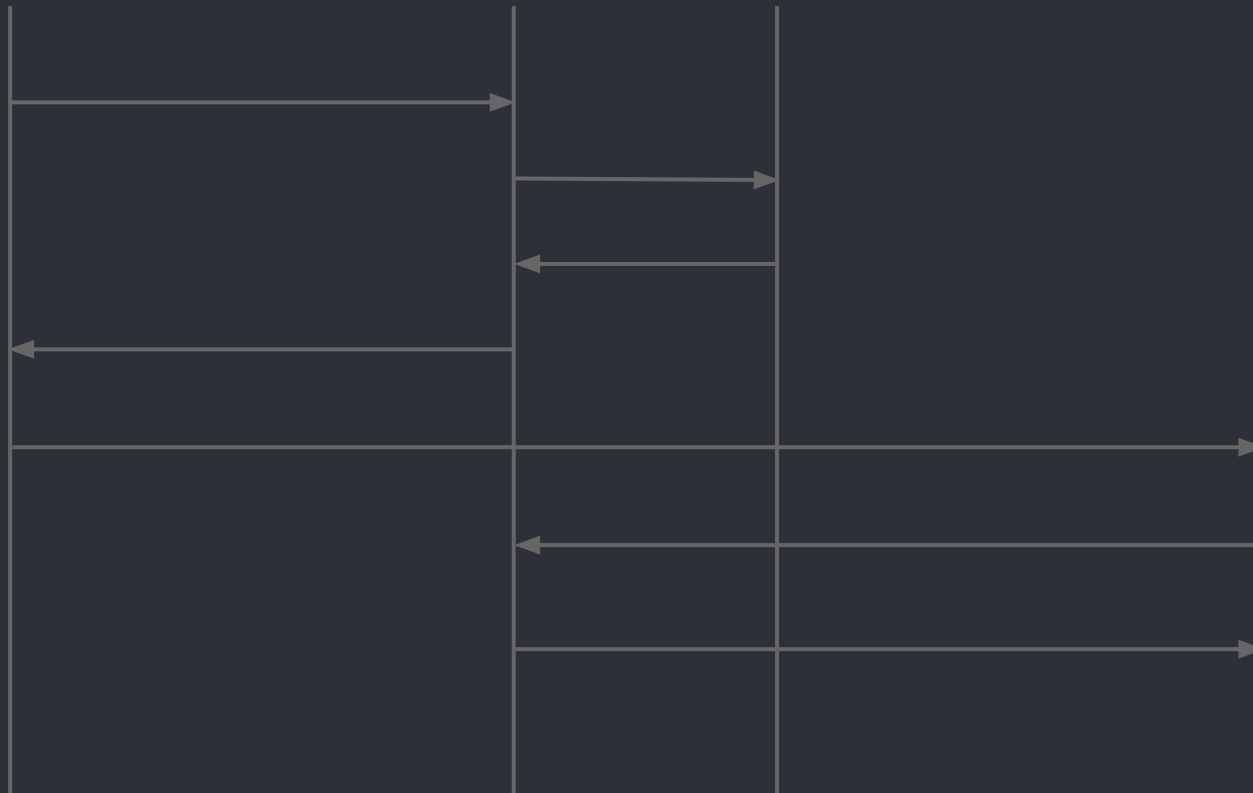
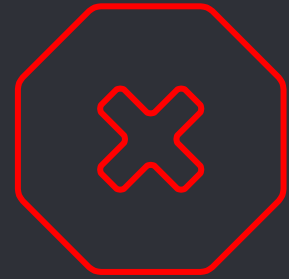
Keystone



Database



Service





4

FEDERATION IN KEYSTONE

SINGLE SIGN-ON

Sign Up **Log In**

First Name Last Name

Email

Username

Password

Create An Account

Or connect with

Facebook Google GitHub



SINGLE SIGN-ON

Sign Up **Log In**

First Name Last Name

Email

Username

Password

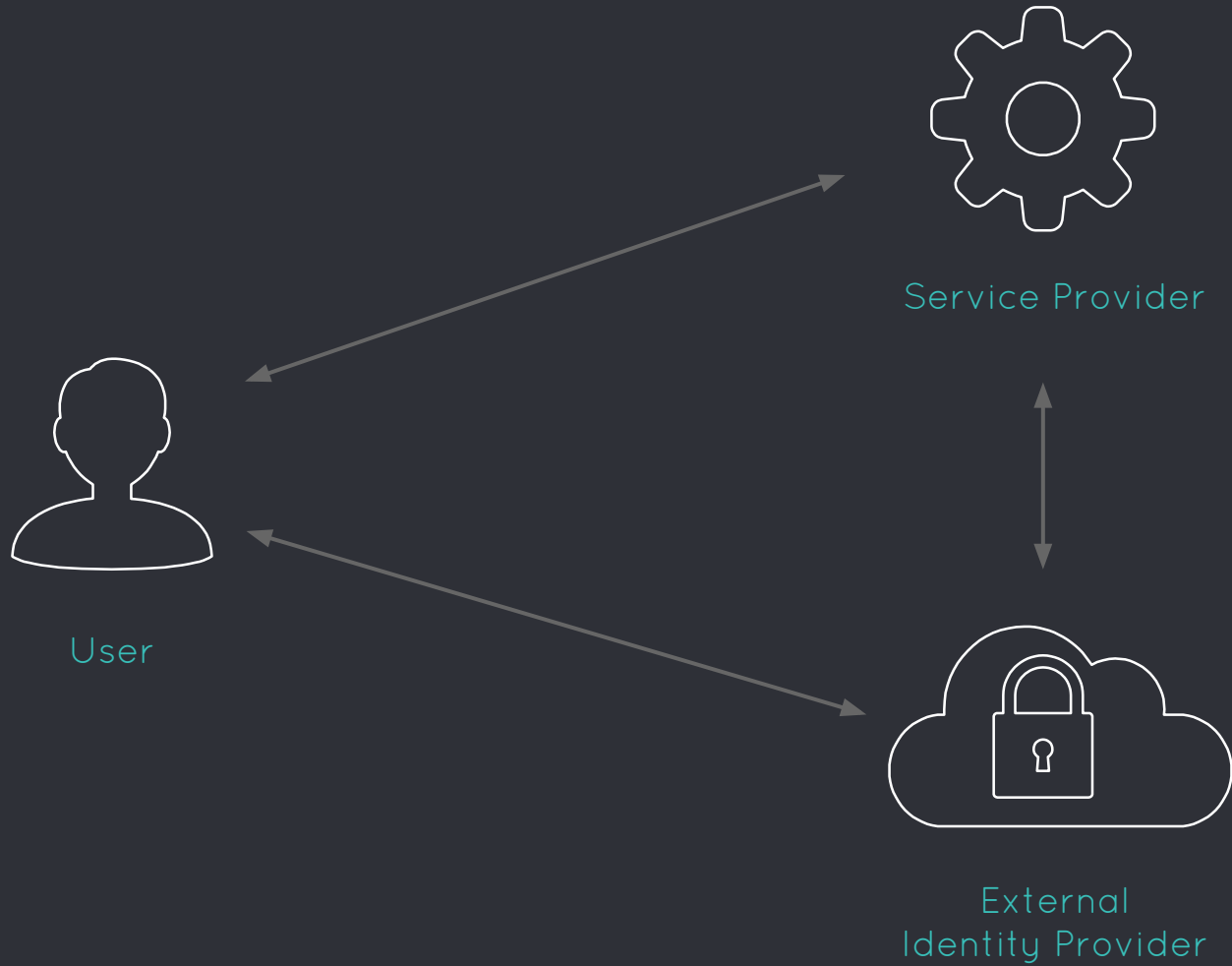
Create An Account

Or connect with

Facebook Google GitHub



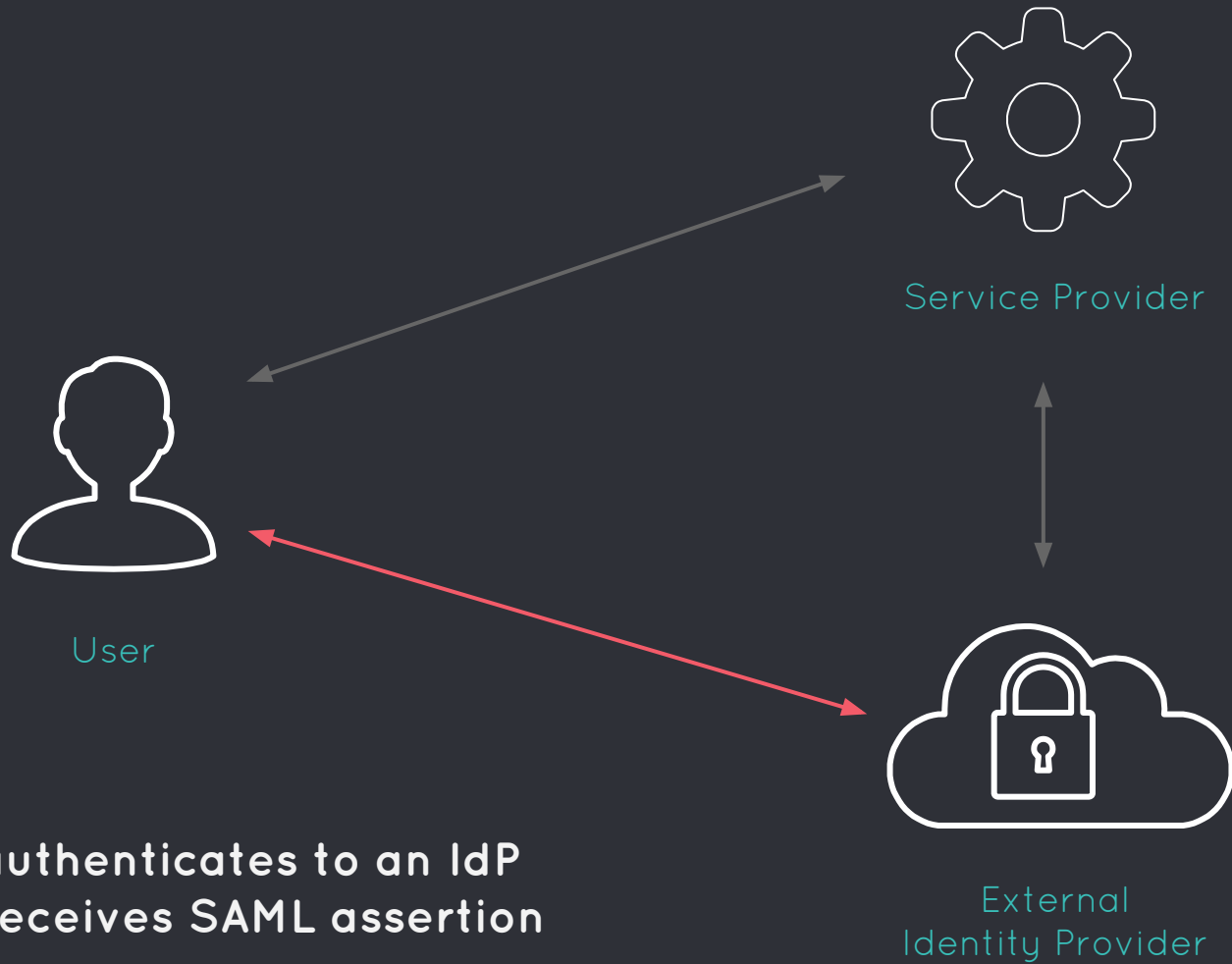
FEDERATION IN KEYSTONE



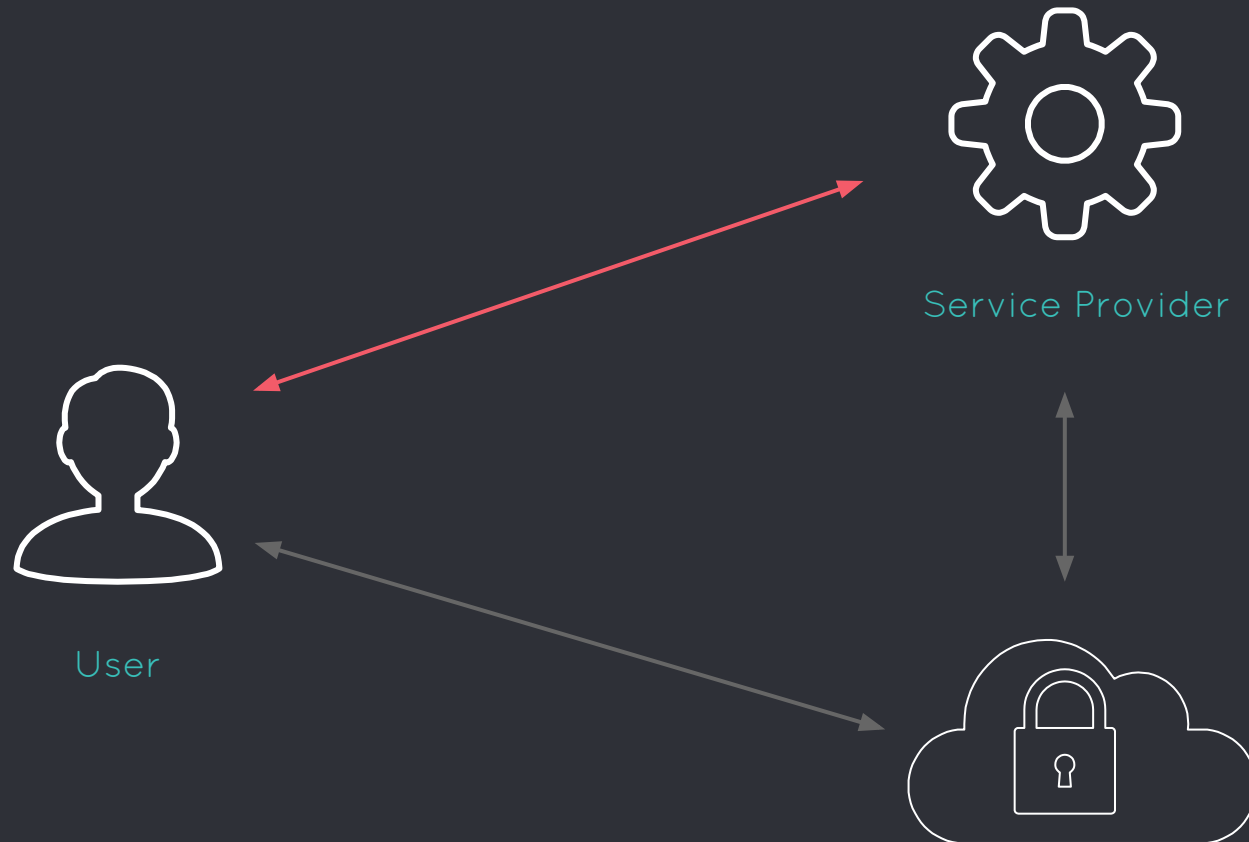
● FEDERATION IN KEYSTONE - ADVANTAGES

- single credential authenticated by a trusted provider
- no need to provision additional identities and centrally store this information
- less identity management

FEDERATION IN KEYSTONE



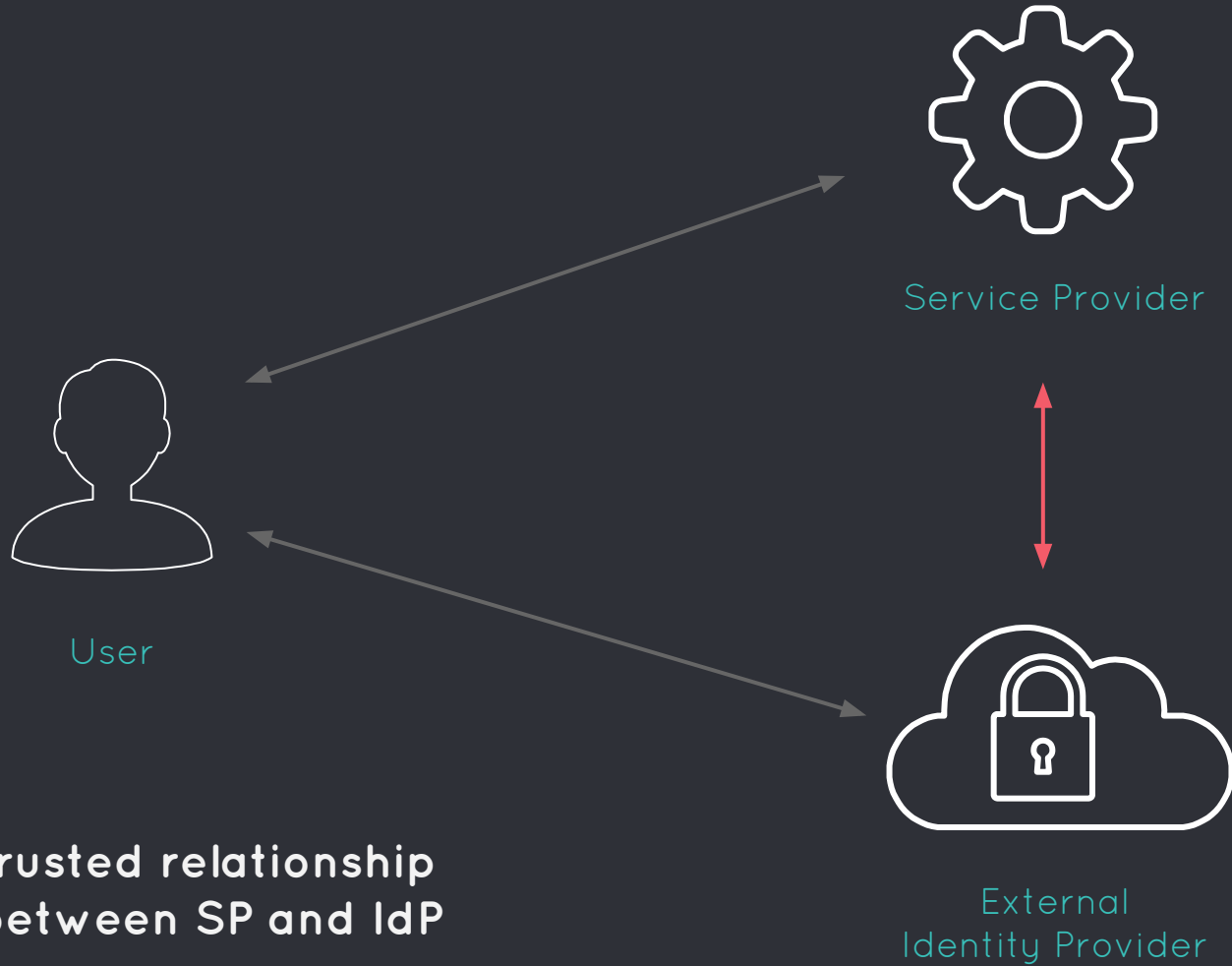
FEDERATION IN KEYSTONE



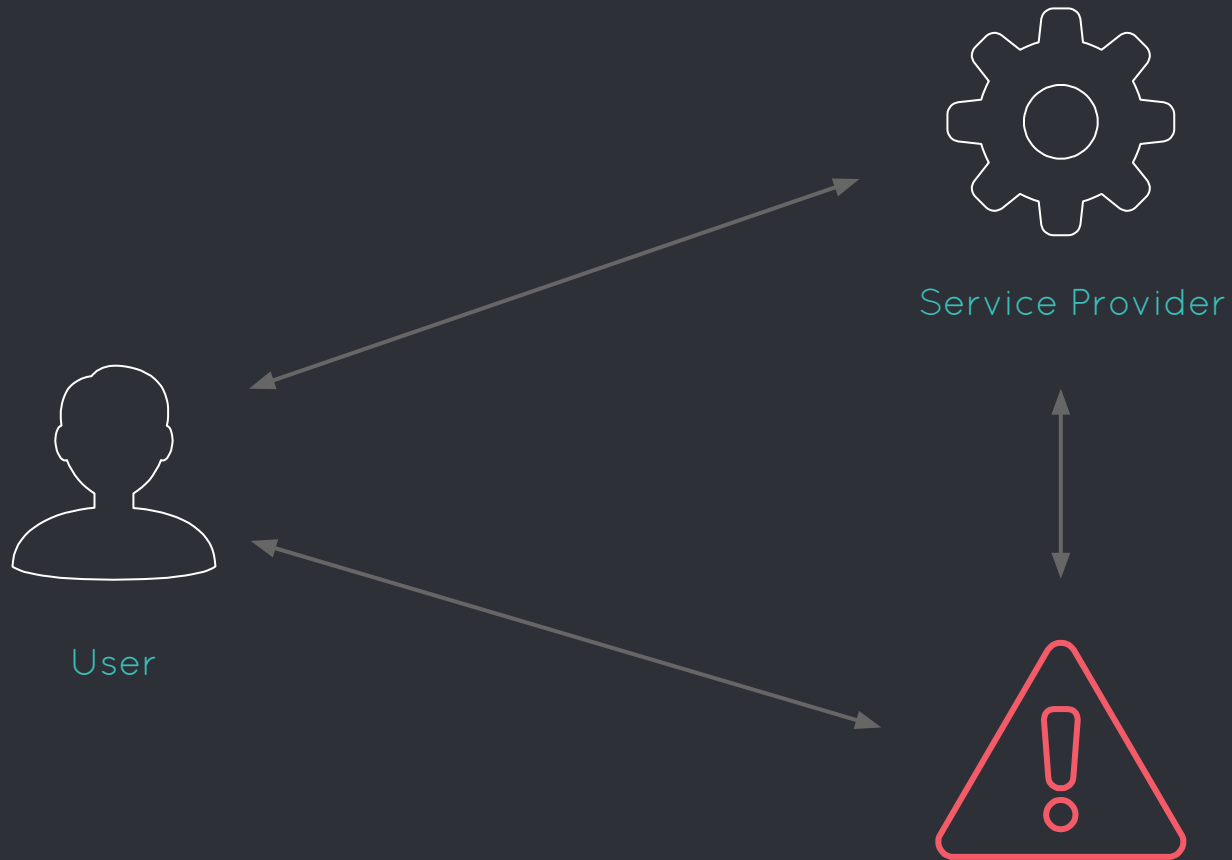
- sends an assertion to a SP
- assertion is mapped to a token
- receives a token for API requests

External
Identity Provider

FEDERATION IN KEYSTONE



FEDERATION IN KEYSTONE



Security of the Openstack Federation is compromised



● RESULTS

- token revocation issue is now solved
 - multiple token types
 - both token invalidation mechanisms
- guide for Keystone developers
 - testing environment
 - code structure
 - testing tools





Thank you for your attention!

pawel.pamula@{cern.ch, gmail.com}

