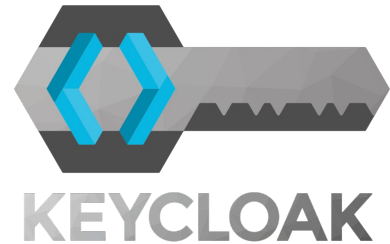


# Keycloak as Big Brother or How to Secure Your Applications?

Ihor Didyk

Software Engineer at GlobalLogic

May, 2022



# Agenda

1

Security Concepts

2

Keycloak Overview

3

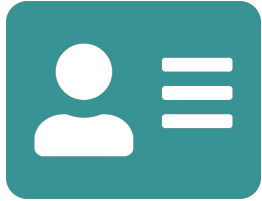
Application Demo

# Disclaimer

Everything described there is true and complete to the best of author's knowledge. All recommendations and inferences are made without guarantee of the part of the author. The author disclaims any liability in connection with the use of this information.

# **Security Concepts**

# IAAA Security Principle



## Identification

Email, username,  
ID number



## Authorization

Access permissions



## Authentication

Password, token,  
signature



## Accountability

logs, user actions,  
traceability of actions

# Implementation of Custom Security Layer

## 1 Authentication for UI

- Manage login/registration forms
- Manage user profiles

## 2 Authentication for Backend

- Store users, passwords
- Check credentials
- API for management tokens

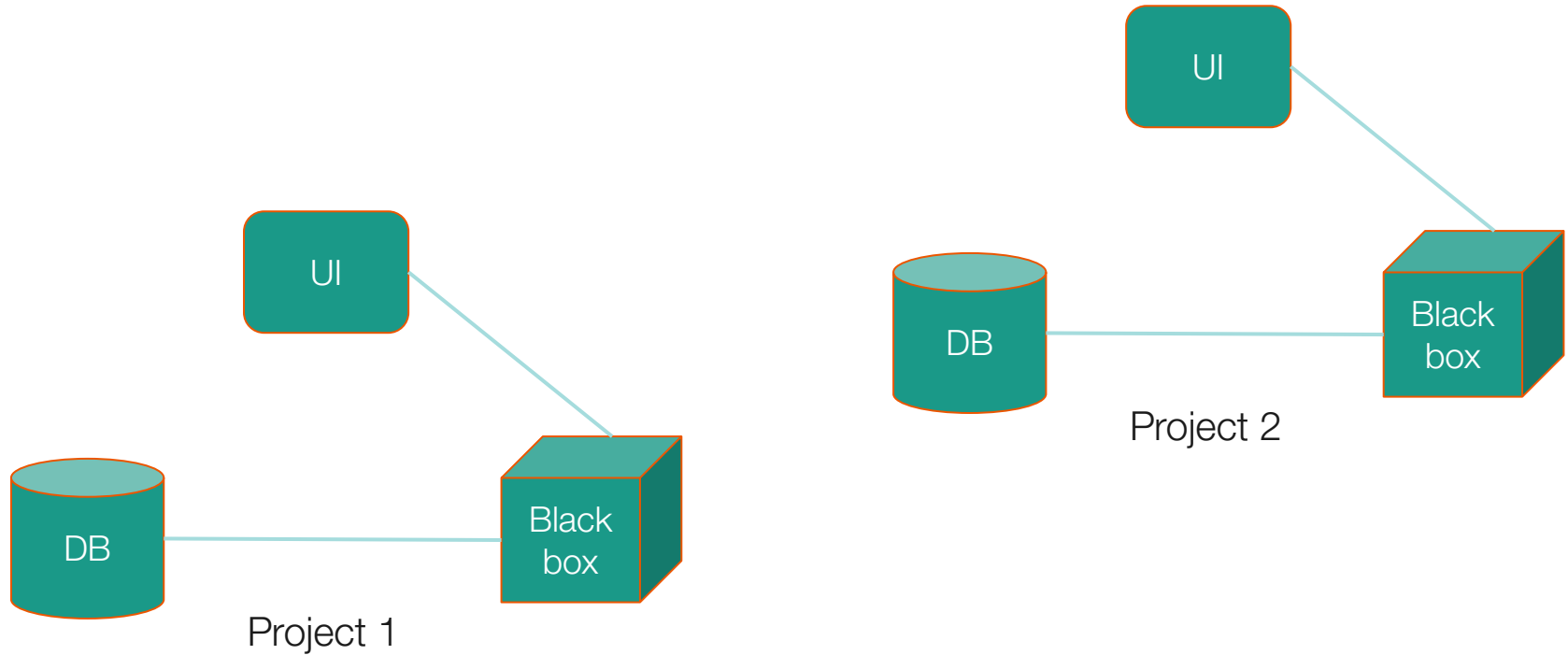
## 3 Put together

- Combine UI and backend together with authentication flows

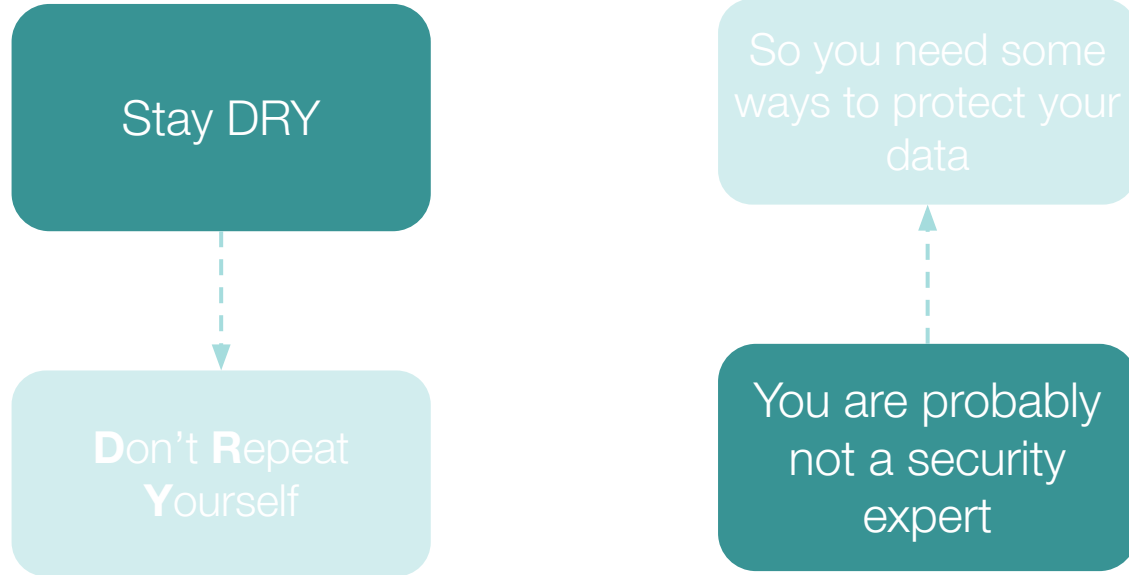
## 4 Project Integration

- Integrate this into the project

# Implementation of Custom Security Layer



# Reasons to Delegate Your Security





# **Keycloak overview:**

Open-source identity and access management.

# Features

## Single sign in

Sign in once to multiple applications

## Standard protocols

OpenID Connect, OAuth 2.0, and SAML 2.0

## Centralized management

Available both for admins and users

## Adapters

Secure applications and services

## LDAP and Active Directory

Connect to existing user directories

## Social login

Easily enable social sign in

## Identity brokering

OpenID Connect or SAML 2.0 IdPs

## High performance

Easy, fast, and scalable

## Clustering

Optimize scalability and availability

## Themes

Customize look and feeling

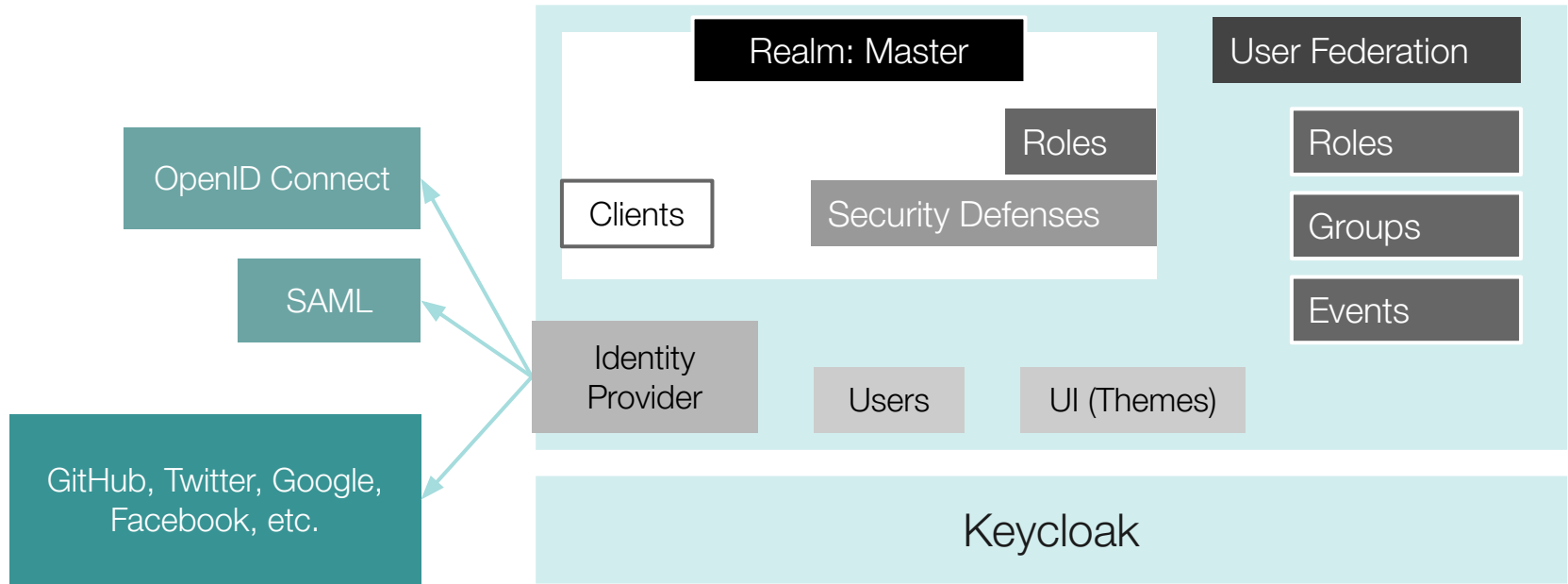
## Extensible

Customize through code

## Password policies

Customize password policies

# Core concepts



# Reasons to Use Keycloak



## Reliable Solution

- Stable release: 18.0.0/April 20, 2022
- Issues board (<https://github.com/keycloak/keycloak/issues>)
- Documentation (<https://www.keycloak.org/documentation.html>)



## Open Source

- Free product
- Various customizations and contributions
- Open community



## Straightforward

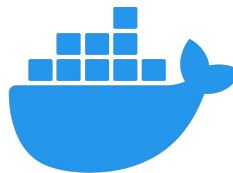
- Not reinventing the wheel
- Shared libraries, keys, certificates, and configurations

# Launch Keycloak



Launch with  
JBoss WildFly

1. Download Keycloak from  
<https://www.keycloak.org/downloads.html>
2. Use the following command:  
`keycloak-x.x.x.Final/bin>./standalone.sh`

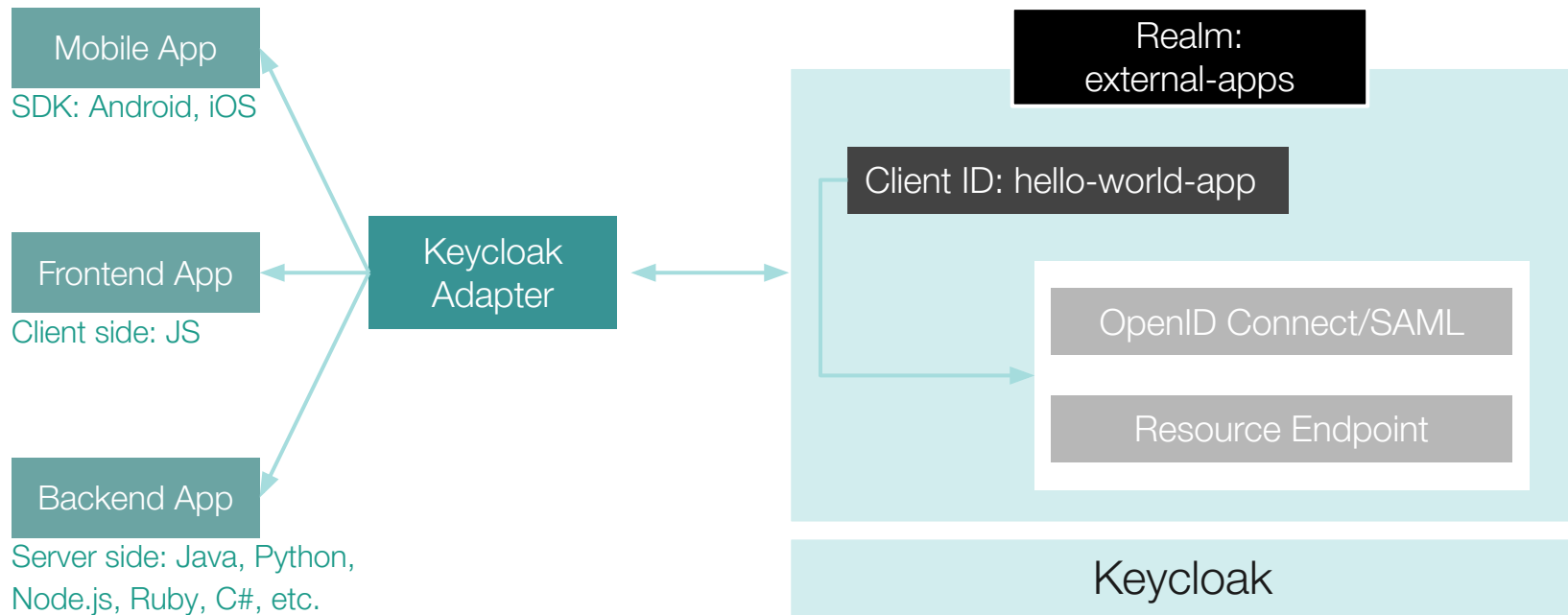


Launch with  
Docker

Use the following commands:

1. `docker pull jboss/keycloak`
2. `docker run --rm -d --name keycloak -p 5555:8080 -e KEYCLOAK_USER=admin -e KEYCLOAK_PASSWORD=admin jboss/keycloak`

# Prepare to Integrate with Keycloak



# Integrate with Keycloak

## 1 Create a realm

- You can use `master` for a dev environment or base it into your business domain (for example, `external-apps` or `internal-apps`).

## 2 Create a client

- Create a client for your application (for example, `hello-world-app`). Client configuration requires the following details:
  - Protocol — SAML or OpenID).
  - Resource endpoint — the application hostname or REST endpoint.
  - Redirect URL — where to redirect the user when authentication is granted.

## 3 Provide a client configuration

- Provide the client configuration to your application as input, for example:
  - The client ID (`hello-world-app`).
  - The realm (`external-apps`).
  - The Keycloak server URL.

# **Application Demo**



**Thank you !**