

RED HAT SINGLE SIGN-ON

Application Performance Management

SSO 둘러보기

KHAN
[a p m]
[s b w]

SSO란 무엇인가?



SSO란 무엇인가?



SSO 도입의 필요성



SSO 도입의 기대효과

- 사용자 편의성
 - 한 번의 사용자 인증을 통한 여러 서비스 자원 사용으로 편의성 향상
 - 사용자 계정 정보의 통합을 통한 효율적인 계정 관리 가능
- 운영 및 관리의 효율성
 - 사용자 인증 및 접근 권한의 중앙관리를 통한 일관성 확보
 - 다양한 플랫폼에 대응하는 표준 보안 체계 구축 가능
- 개발의 효율성
 - 통합된 인증 및 권한 모듈을 사용하므로 개발 비즈니스 로직에 집중 가능
 - 중복된 모듈 개발을 방지하여 애플리케이션 품질 향상 및 비용과 시간의 감소 기대

Application Performance Management

Red Hat SSO

KHAN
[a p m]
[g b w]

Keycloak 은 무엇?

- Keycloak : 열쇠+망토=슈퍼키?
- 웹에서 Single Sign On (SSO) 을 구축하기 위한 Java 기반의 인증 소프트웨어
- 2014 년에 버전 1.0.0 출시
 - 최신 버전은 3.4.3 Final (2018 년 1 월 4일 출시)
- Keycloak는 Red Hat JBoss 프로젝트를 통해 오픈 소스 소프트웨어)
 - Apache 2.0 라이선스
 - <http://keycloak.jboss.org>
- "Red Hat JBoss EAP" 서브스크립션에 포함된 제품으로 Keycloak을 기반으로 한 "Red Hat SSO"를 판매



keycloak

Red Hat SSO란?

- Red Hat의 SSO 오픈소스 Keycloak의 상용 버전
- JBOSS EAP 사용시 무료 (JDK 1.8 이상 시스템 필요)
 - 레드햇 홈페이지에서 다운로드 : access.redhat.com/jbossnetwork
- 웹 애플리케이션 및 RESTful 웹 서비스를 위한 SSO 솔루션
- 단순한 보안 관리 구성으로 애플리케이션 및 서비스를 안전하게 보호

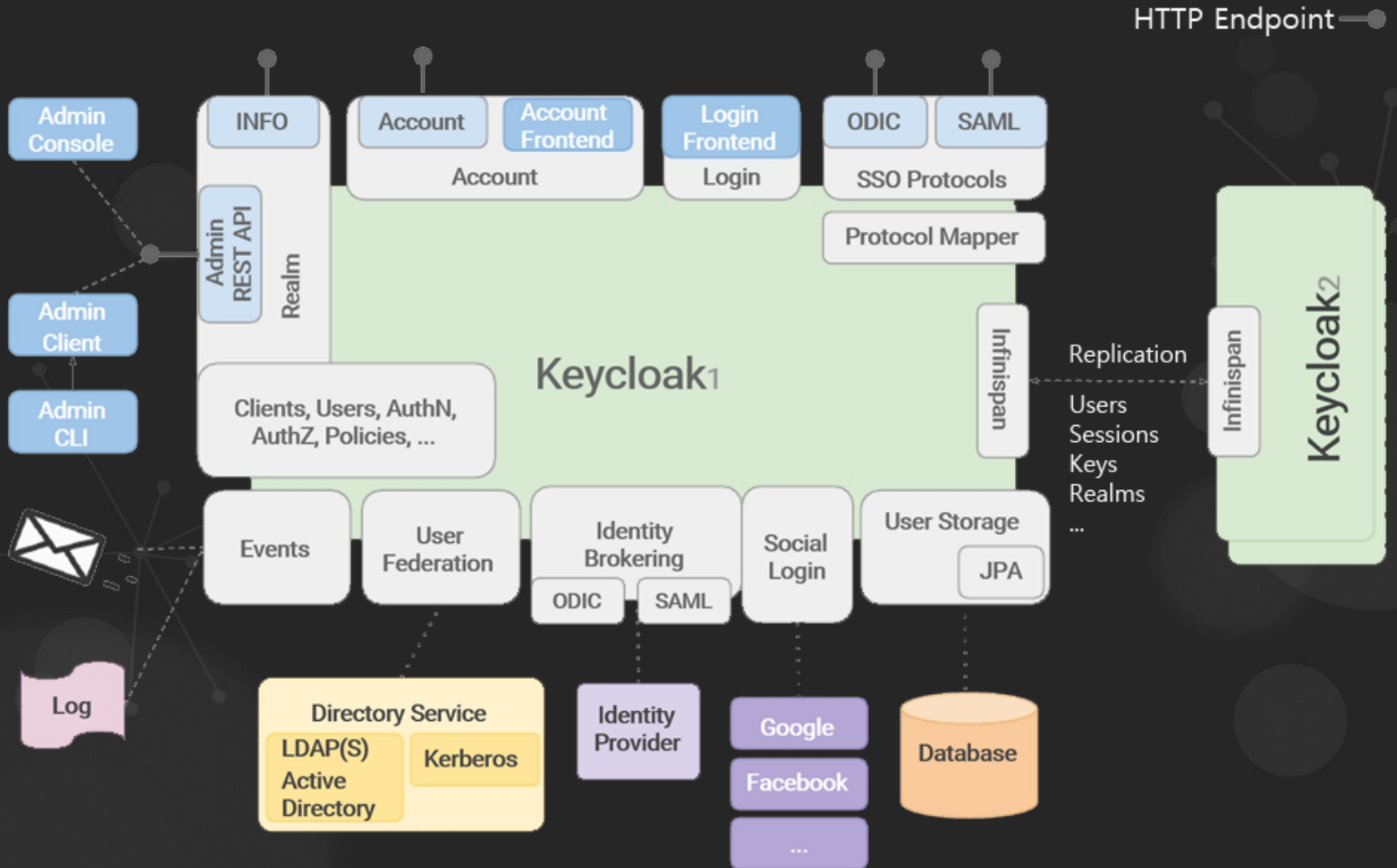


{ REST API }

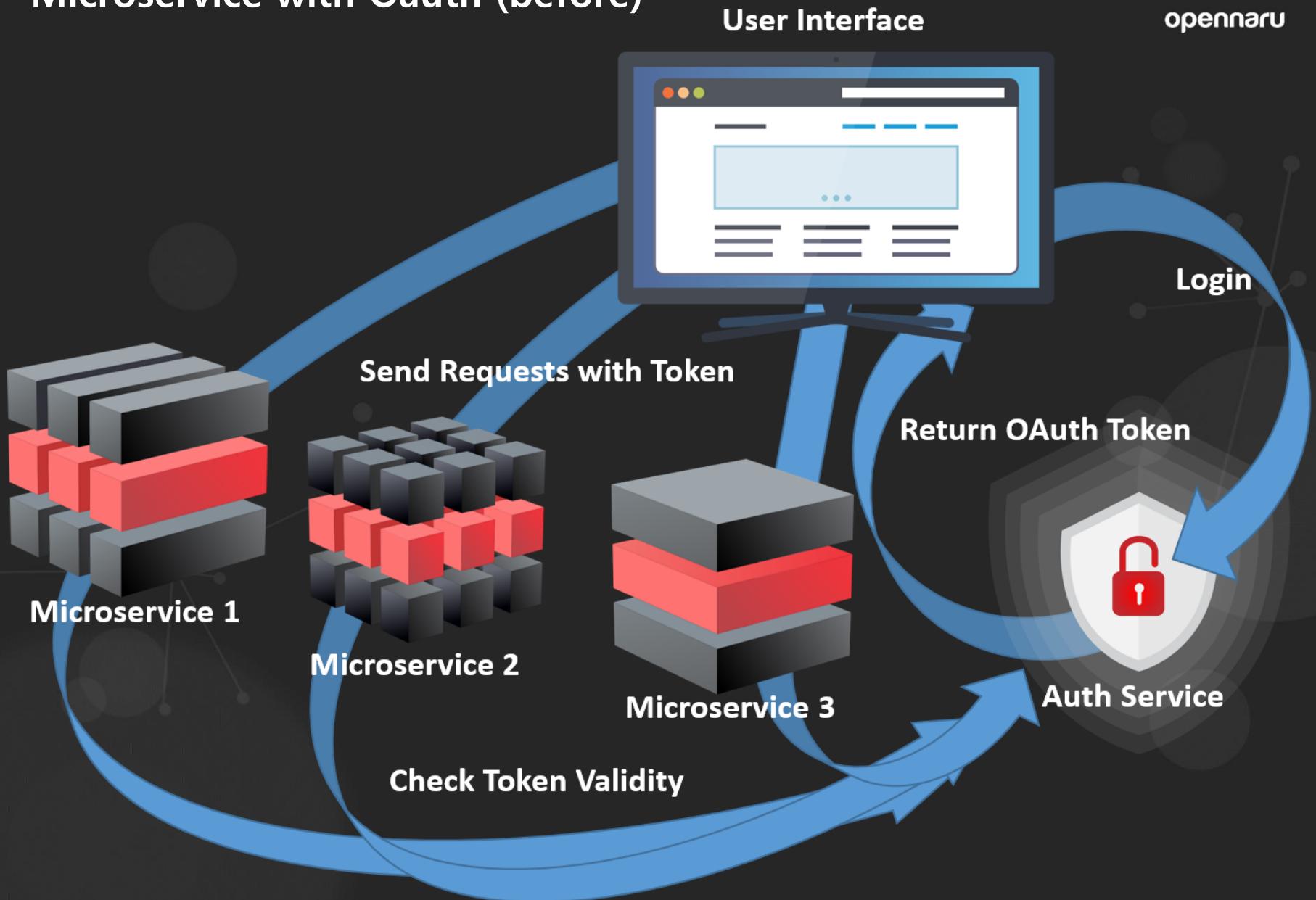
Representational State Transfer API



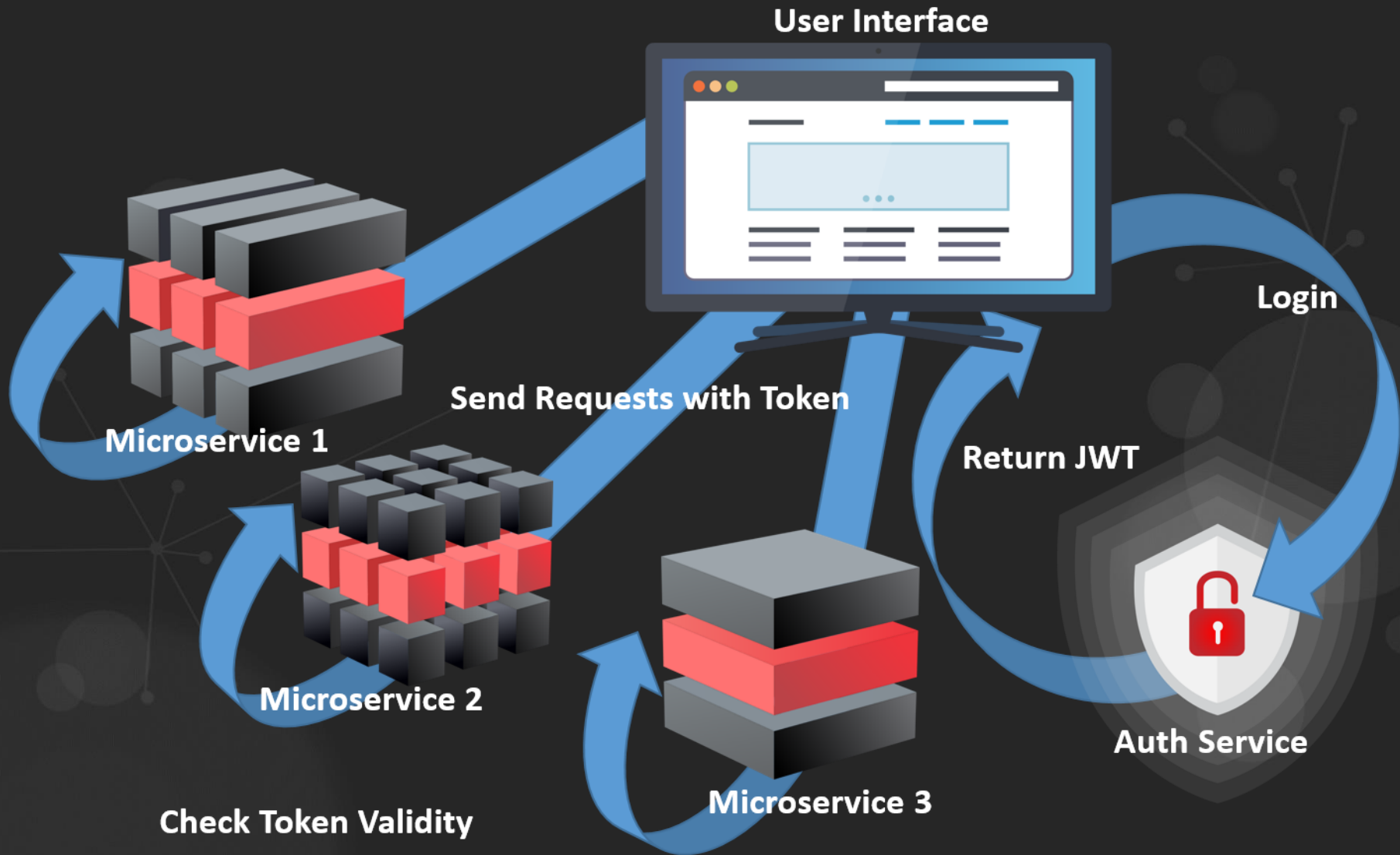
Anatomy of a Keycloak Server



Microservice with Oauth (before)

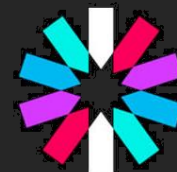


Microservice with JWT (after)



Red Hat SSO의 주요 특징점

- 표준 프로토콜 지원 – OpenID Connect 1.0, OAuth 2.0, SAML 2.0
- 토큰 기반의 보안 - JSON Web Token(JWT) → (“jot”이라고 읽음)
- 사용자 페더레이션 기능 – LDAP, Active Directory 지원
- 중앙 집중화된 웹 관리 콘솔 및 커스터마이징 기능
- Realm(영역) 단위별로 관리 구성



표준 프로토콜 지원

- SAML 2.0 (Security Assertion Markup Language)
 - XML 기반의 인증 프로토콜
 - 복잡하고 무거운 구조
 - 네이티브 애플리케이션, 모바일 환경에 적용하기에는 부적합
- OAuth 2.0 (Open Authorization)
 - API를 사용하여 자원에 접근하기 위한 오픈 표준
 - 다양한 플랫폼 환경에서 권한 부여(Authorization)를 위한 프로토콜
 - 클라이언트에게 제한된 접근을 하도록 권한을 부여하는 일종의 프레임워크
- OpenID Connect 1.0
 - OAuth 2.0 권한 부여 프로토콜을 기반으로 이를 확장한 프로토콜
 - JSON/REST 기반의 상호 운용 가능한 인증(Authentication) 프로토콜
 - 모바일 환경까지 고려한 설계로 다양한 플랫폼에 적용 가능

JSON Web Token(JWT)

- 경량의 데이터 통신에 적합한 JSON 데이터 구조
- Base64 알고리즘으로 인코딩
- Header, Payload, Signature의 3부분으로 구성
 - Header : 사용한 알고리즘과 토큰 타입 정보
 - Payload : 사용자 계정 관련 정보
 - Signature : 보안을 위한 디지털 서명



JSON Web Token

Rathes Sachchithananthan - <https://rathes.de/blog/de/json-web-token>

JSON Web Token(JWT)



Encoded

PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0Ij0wMDAwMDA7.TjVA950rM7E2cBab3
0RMHrHDcEfxfjoYZgeFONfH7HgQ

Decoded

EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

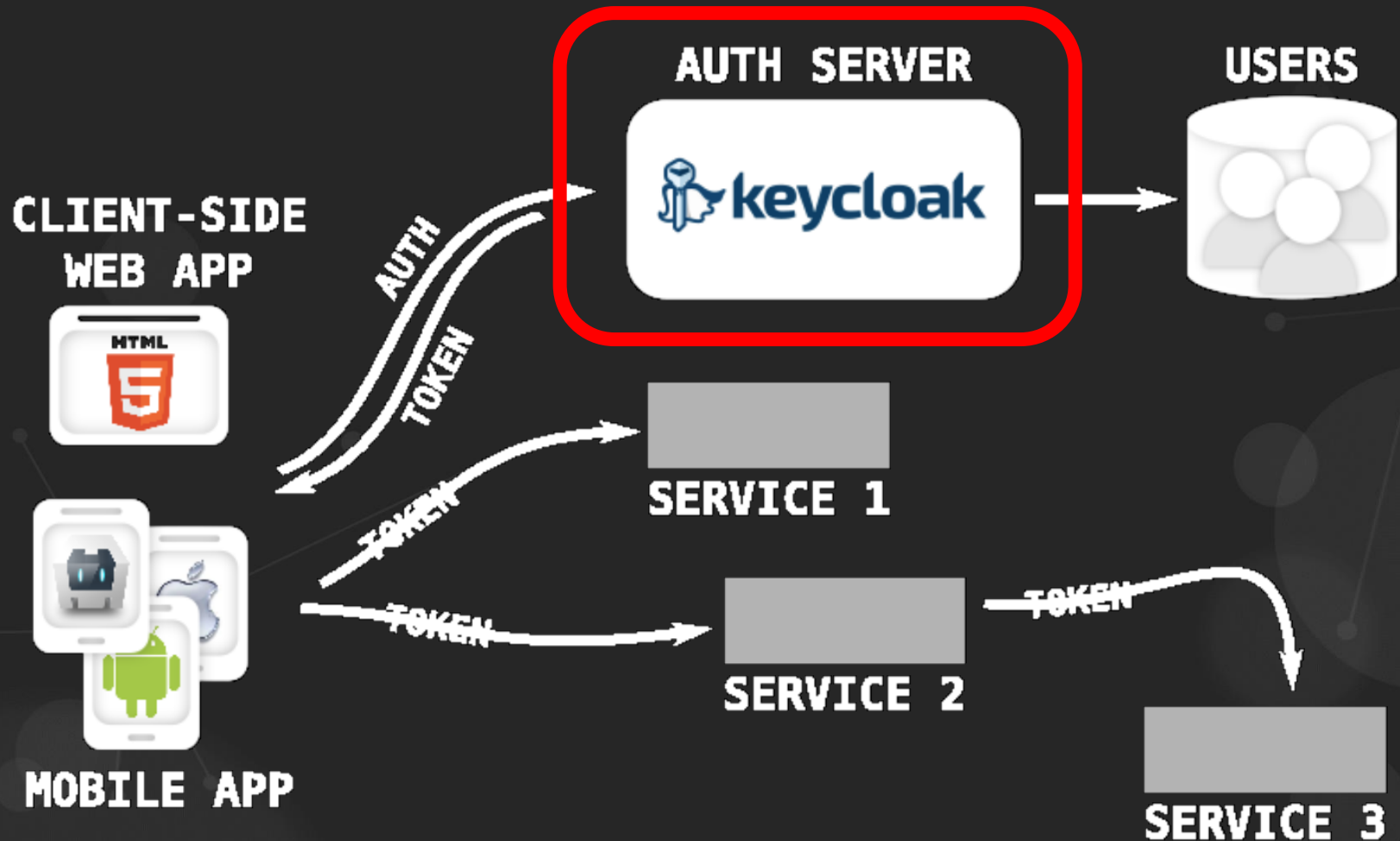
```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

VERIFY SIGNATURE

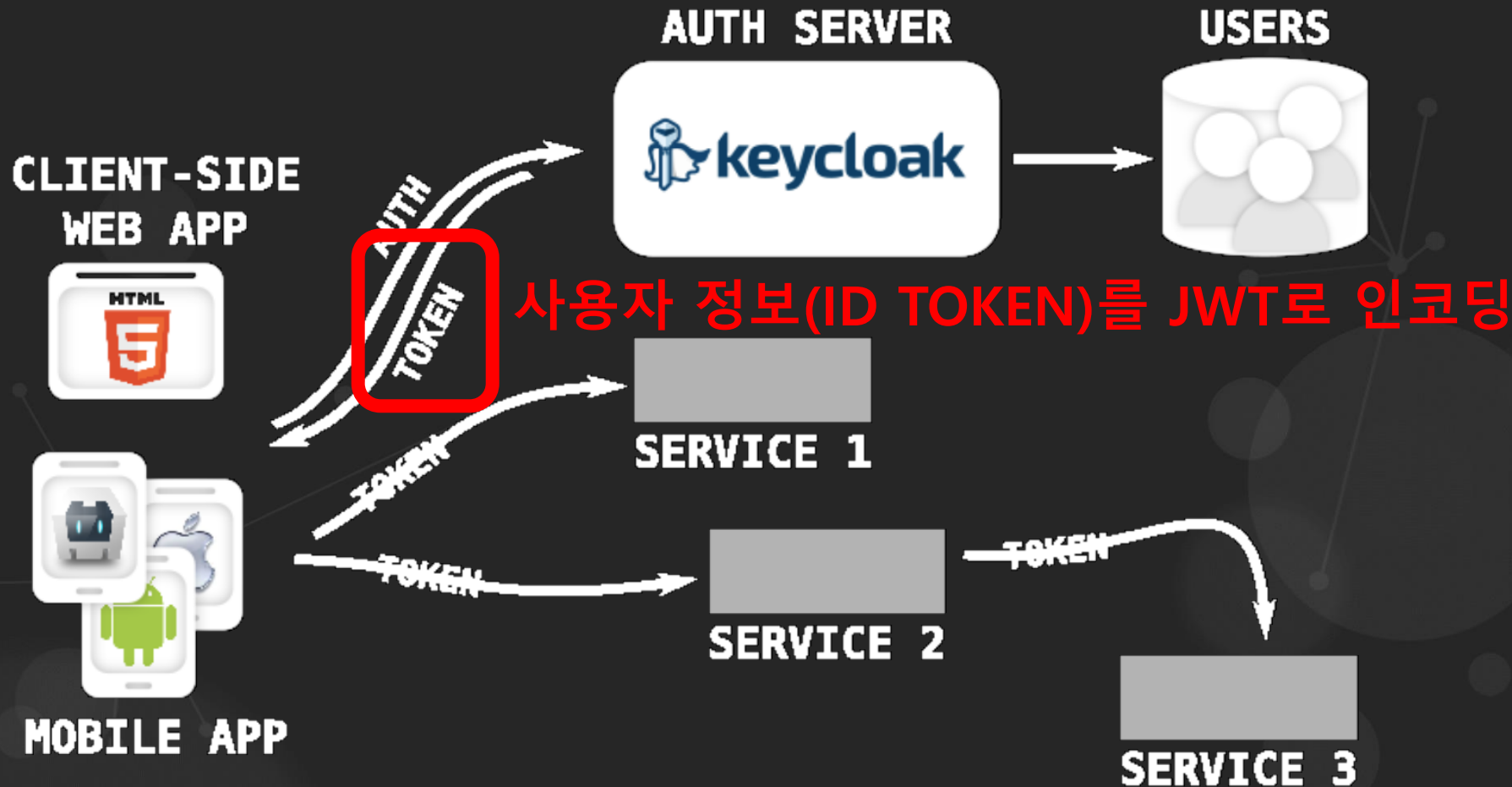
```
HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    secret
) # secret base64 encoded
```

✔ Signature Verified

JWT - <https://jwt.io/>



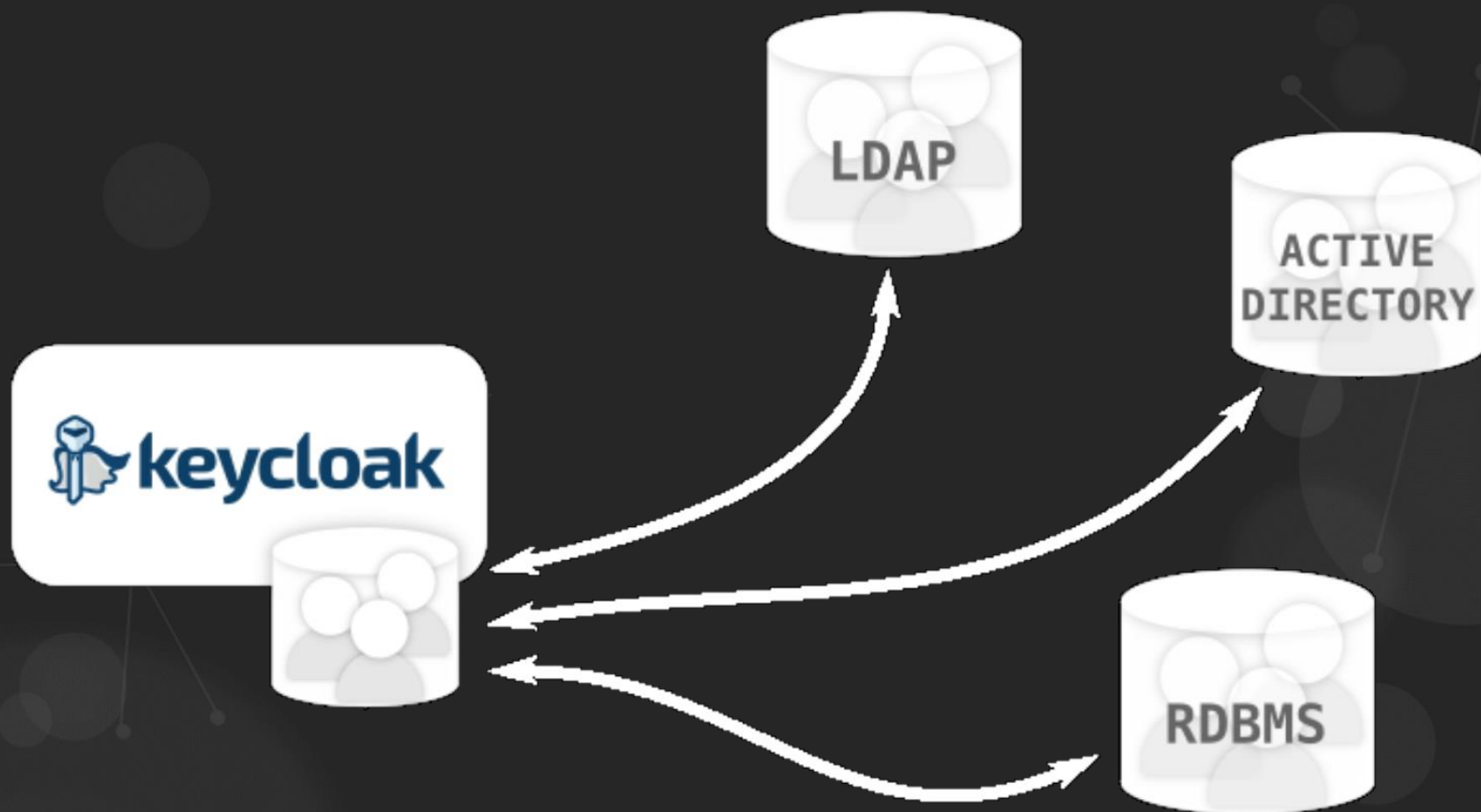
Red Hat SSO 인증 구조



Red Hat SSO 인증 구조

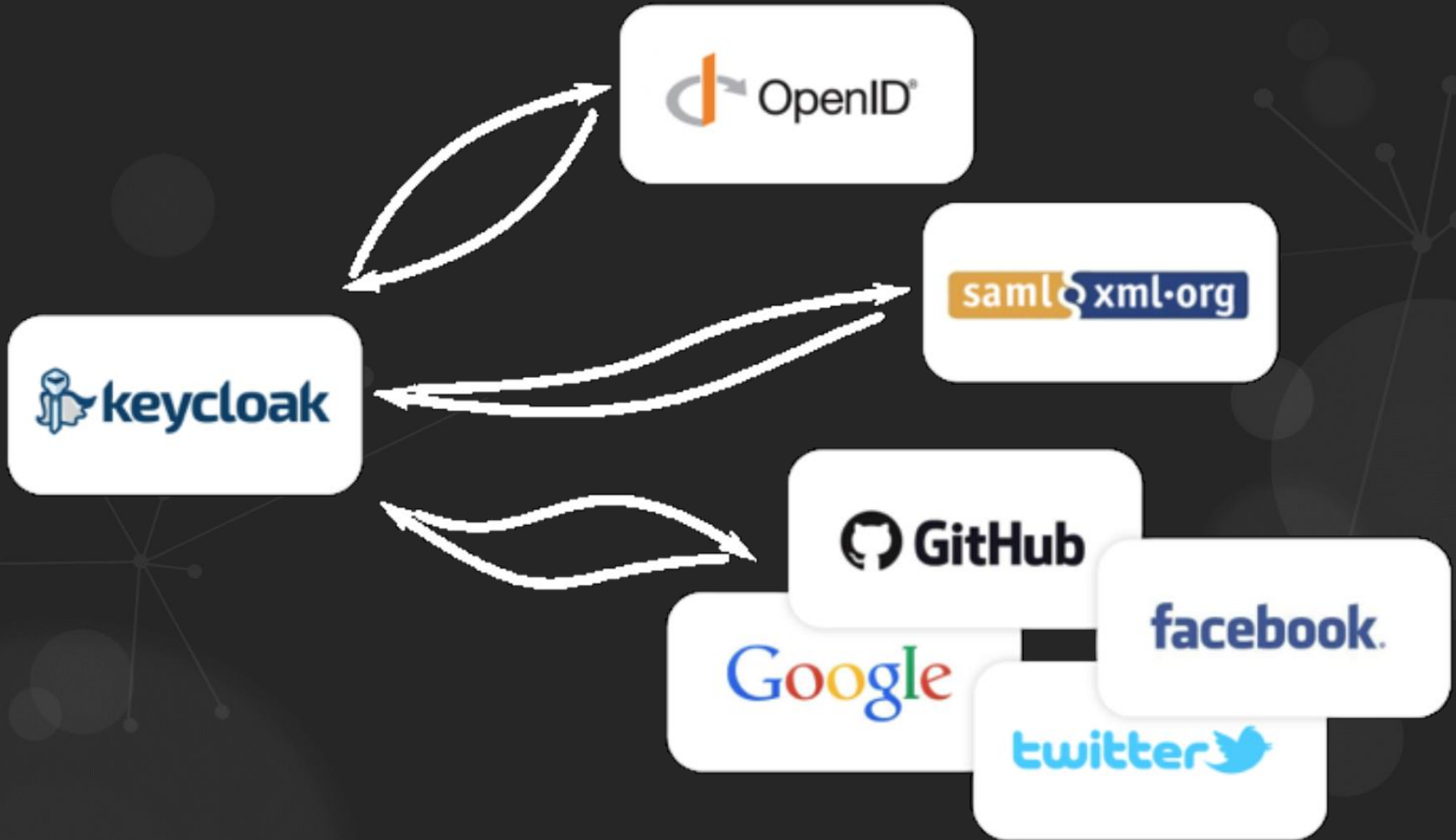


사용자 페더레이션 기능



Keycloak blog - <http://blog.keycloak.org/2015/03/customizing-keycloak.html>

아이디 브로커링



Keycloak blog - <http://blog.keycloak.org/2015/03/customizing-keycloak.html>

RED HAT SINGLE SIGN-ON

Admin

Master

Configure

Realm Settings

Clients

Client Templates

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

Master

General

Login

Keys

Email

Themes

Cache

Tokens

Client Registration

Security Defenses

* Name

master

Display name

rh-sso

HTML Display name

Red Hat[®] Single Sign On

Enabled

ON

Endpoints

OpenID Endpoint Configuration

Save

Cancel

커스터마이징 기능

MOBILE AUTHENTICATOR SETUP



 You need to set up Mobile Authenticator

1. Install one of the following applications on your mobile device
 - FreeOTP
 - Google Authenticator
2. Open the application and scan the barcode



[Unable to scan?](#)

3. Enter the one-time code provided by the application

[Submit](#)

HELLO-WORLD-AUTHZ

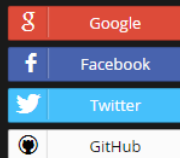
Username or email

Password

☐ Remember me
[Forgot Password?](#)

[Log in](#)

New user? [Register](#)



REALM



SERVICE(=CLIENT)

SERVICE(=CLIENT)

SERVICE(=CLIENT)

Realm 관리 방식

Hello-world-authz ▾

Configure



Realm Settings



Clients



Client



Templates



Roles

 Groups

 Users

 Sessions

 Events

 Import

Hello-world-

General

Login

Tokens

Client Registration

Security Defenses

* Name

Display name

HTML Display
name

Realm 관리 방식



RED HAT SINGLE SIGN-ON

Admin

Hello-world-authz

Configure

Realm Settings

Clients

Client

Templates

Manage

Groups

Users

Sessions

Events

Import

Export

Users

Lookup

Search...

Q

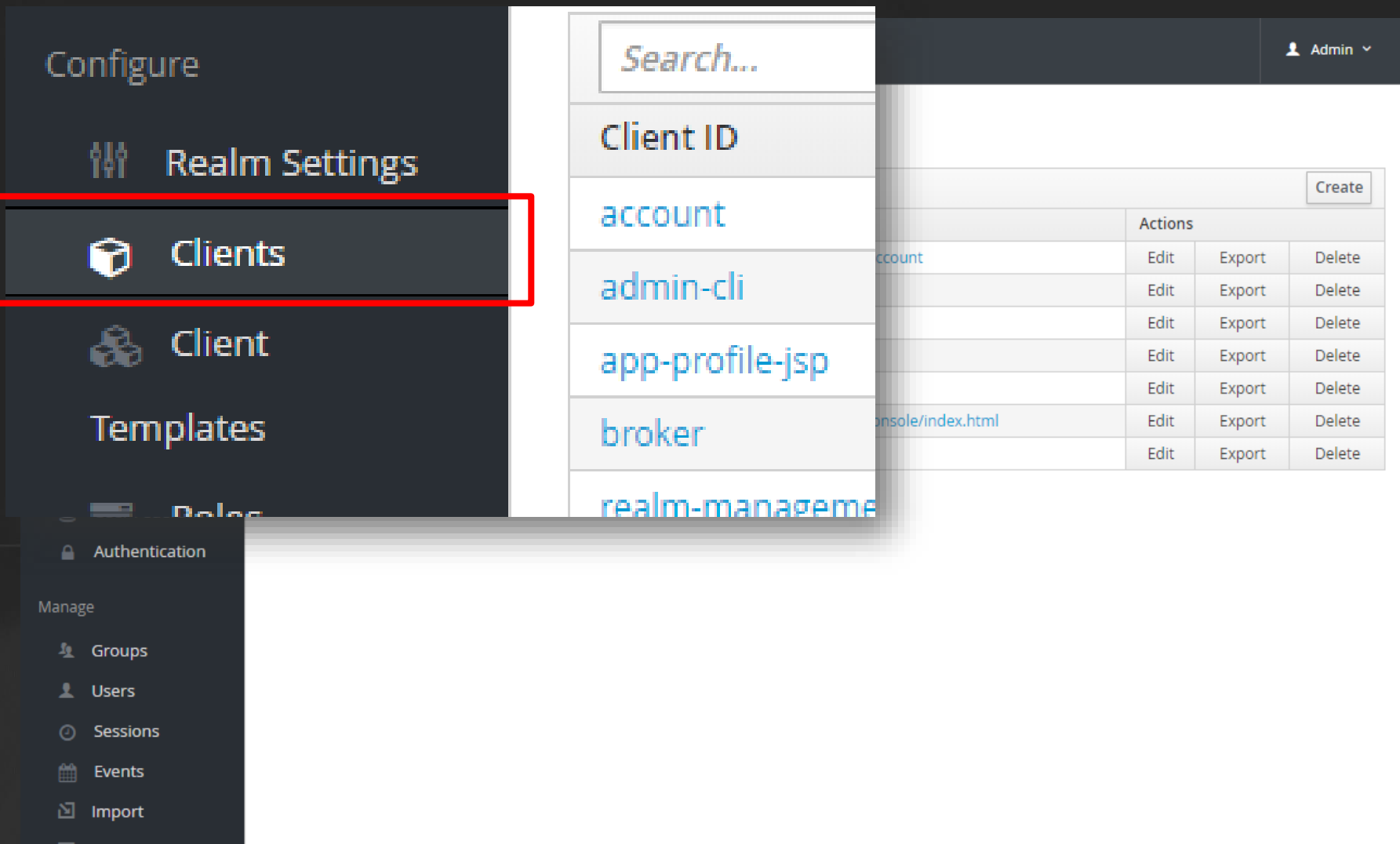
View all users

Unlock users

Add user

ID	Username	Email	Last Name	First Name	Actions		
03bb428a-bc9d-4...	test1	ssotest1@test.com	vadar	darth	Edit	Impersonate	Delete
fe070947-8b2e-46...	test2				Edit	Impersonate	Delete

Realm 관리 방식



Configure

Realm Settings

Clients

Client

Templates

Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import

Search...

Client ID

- account
- admin-cli
- app-profile-jsp
- broker
- realm-manageme

Create

	Actions		
account	Edit	Export	Delete
	Edit	Export	Delete
	Edit	Export	Delete
	Edit	Export	Delete
	Edit	Export	Delete
console/index.html	Edit	Export	Delete
	Edit	Export	Delete

Realm 옵션 설정



RED HAT SINGLE SIGN-ON

Admin ▾

Hello-world-authz ▾

Configure

Realm Settings

Clients

Client

Templates

Roles

Identity

Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Hello-world-authz

General

Login

Keys

Email

Themes

Cache

Tokens

Client Registration

Security Defenses

User registration ?

ON

Email as username ?

OFF

Edit username ?

OFF

Forgot password ?

ON

Remember Me ?

ON

Verify email ?

OFF

Login with email ?

ON

Require SSL ?

external requ ▾

Save

Cancel

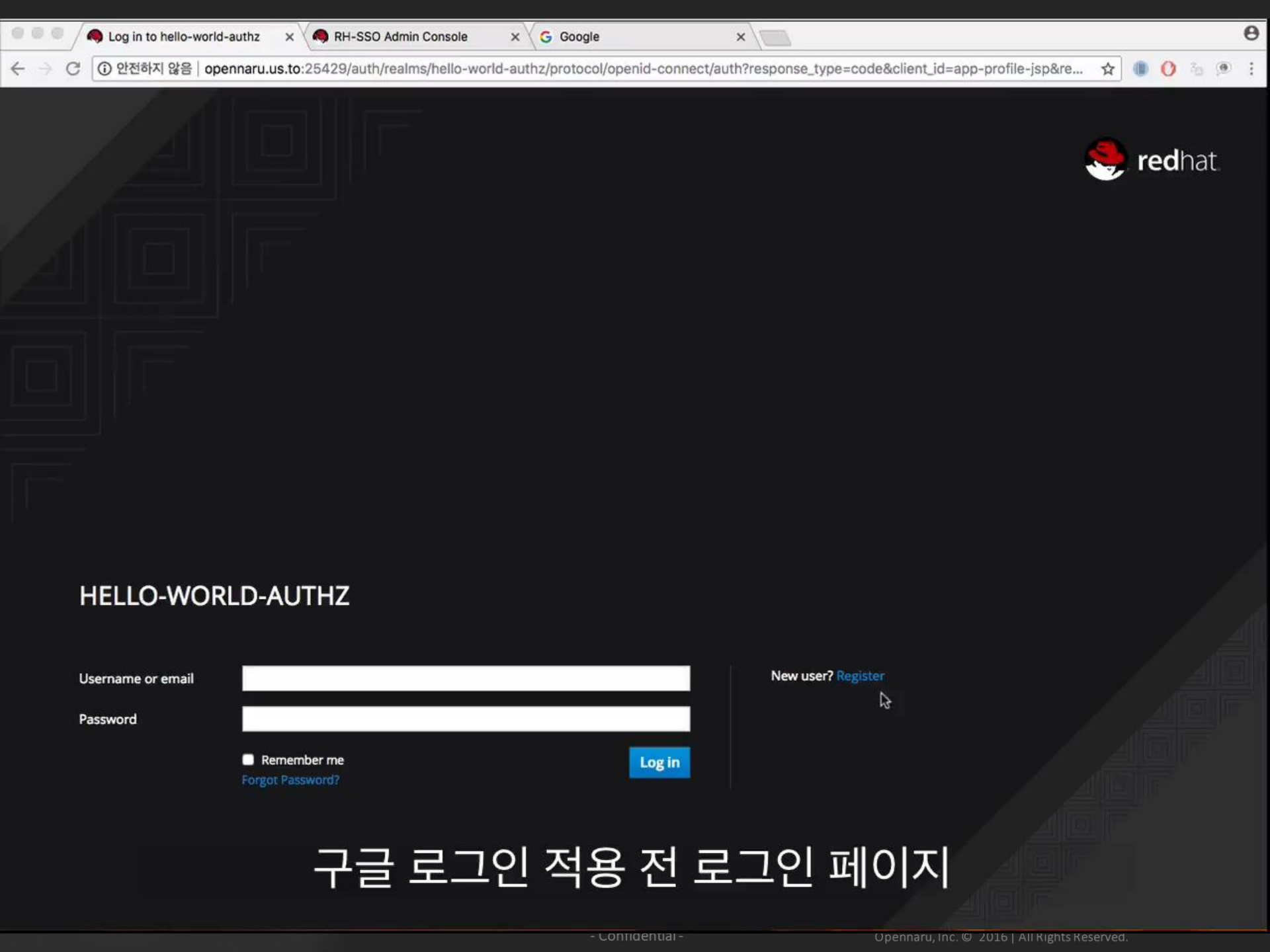
- Confidential -

Opennaru, Inc. © 2016 | All Rights Reserved.

Application Performance Management

RH-SSO DEMO

KHAN
a p m
g b w



HELLO-WORLD-AUTHZ

Username or email

Password

☐ Remember me

[Forgot Password?](#)

Log in

New user? [Register](#)

구글 로그인 적용 전 로그인 페이지

Application Performance Management

감사합니다.

KHAN
[a p m]
[g b w]



제품이나 서비스에 관한 문의

콜 센터 : 02-469-5426 (휴대폰 : 010-2243-3394)

전자 메일 : sales@opennaru.com