OAuth 2.0 and OpenID Connect and SSO, Oh My!

Security Simplified with IdentityServer4

http://aaronralls.com

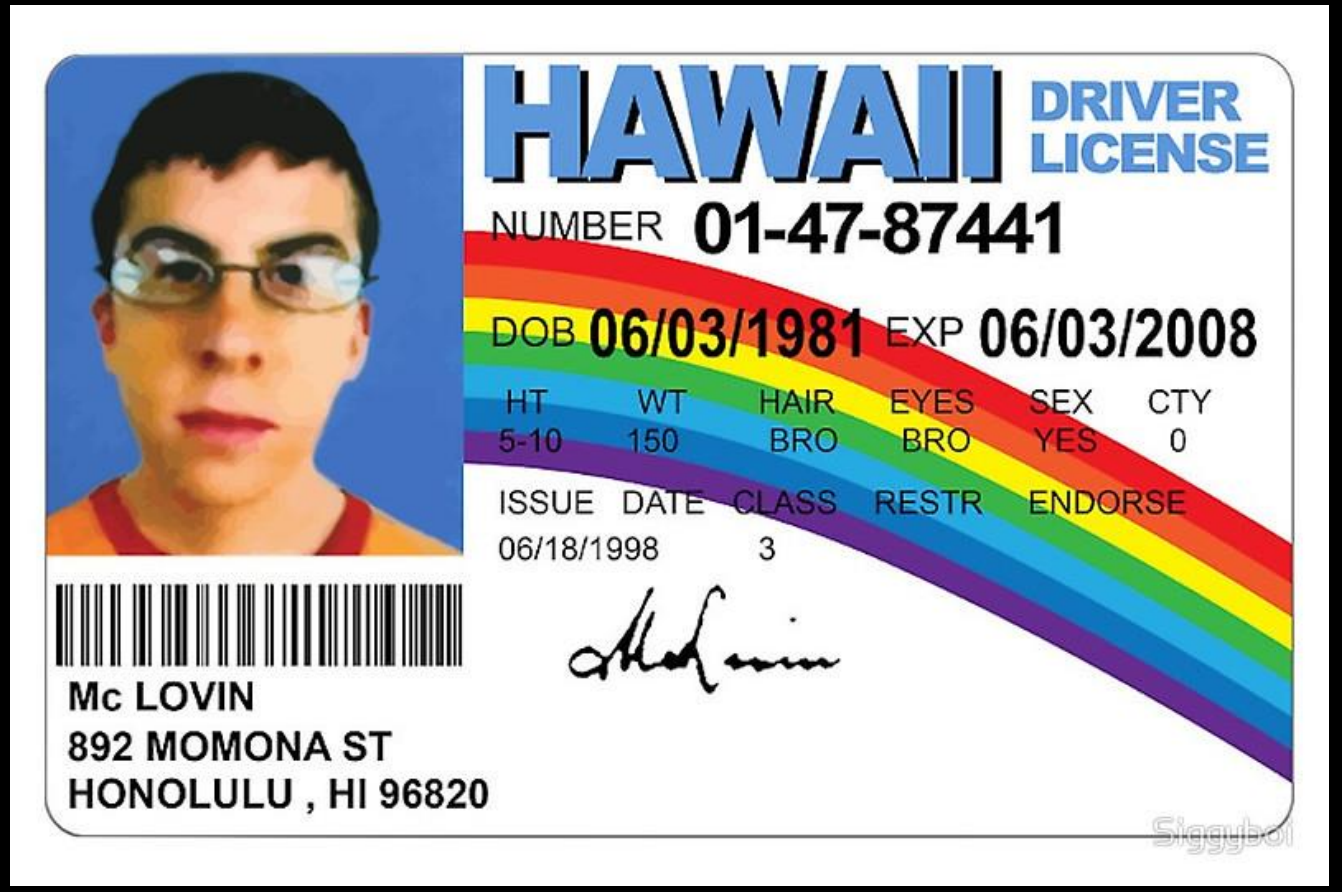
Where to get this presentation and the resources?

- IdentityServer4 Demos 1 & 2
- IdentityServer4 Demo 3
- OIDC JavaScript client
- OpenID Connect Implementations
- iOS OAuth 2.0 & OpenID Connect example
- Xamarin example
- OAuth 2.0 --rfc6749
- OpenID Connect

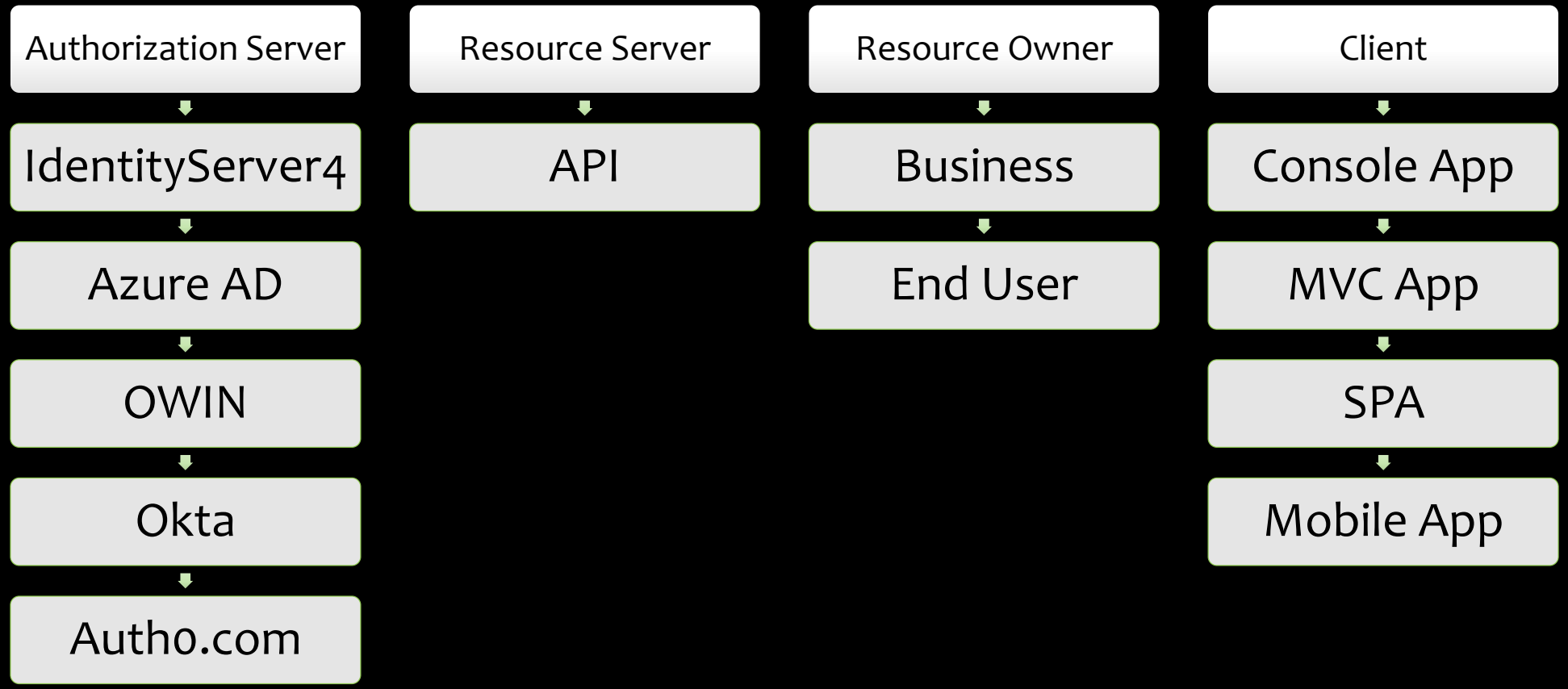
What will you learn today?

- The principals of OAuth 2.0 and OpenID Connect protocols.
- How IdentityServer4 can be used to implement the OAuth 2.0 and OpenID Connect protocols to secure your API's, Web and Mobile applications.
- How IdentityServer4 can be used to implement a SSO

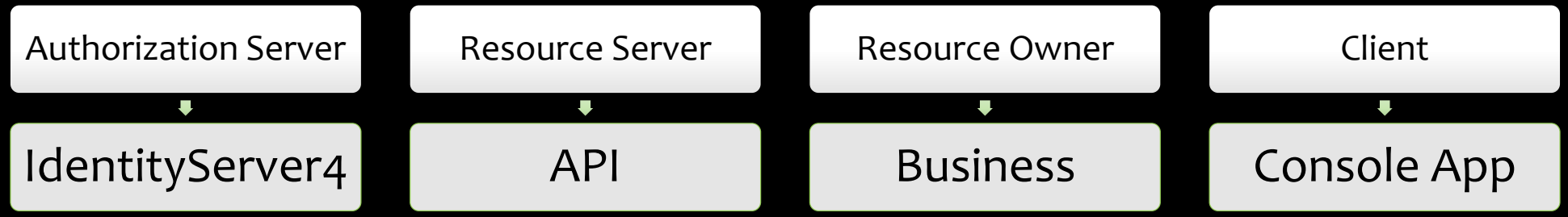
Authorization vs. Authentication



OAuth 2.0 (Authorization)



OAuth 2.0 (Authorization)



OAuth 2.0

Front Channel (Browser)

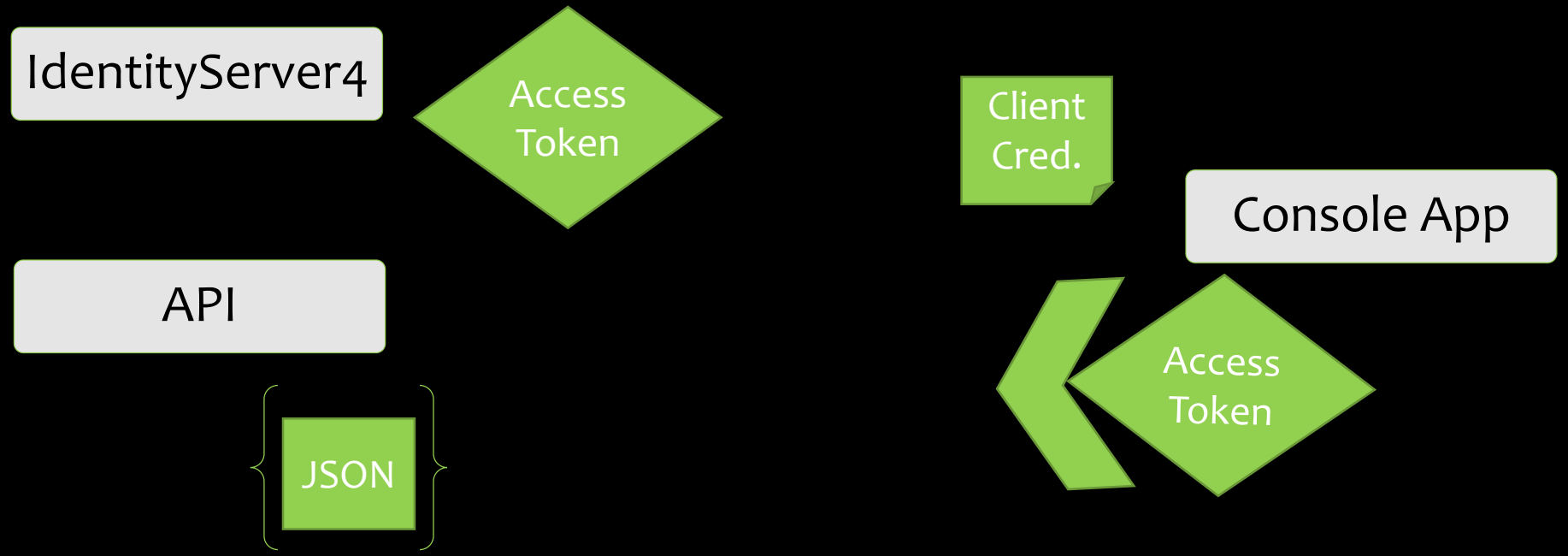
Back Channel

OAuth 2.0 Access Tokens

Reference

Self contained - JWT

OAuth 2.0 Authorization Grant Type: Client Credentials



DEMO 1

Client Credentials
Console App/Windows Service
accessing a secured API

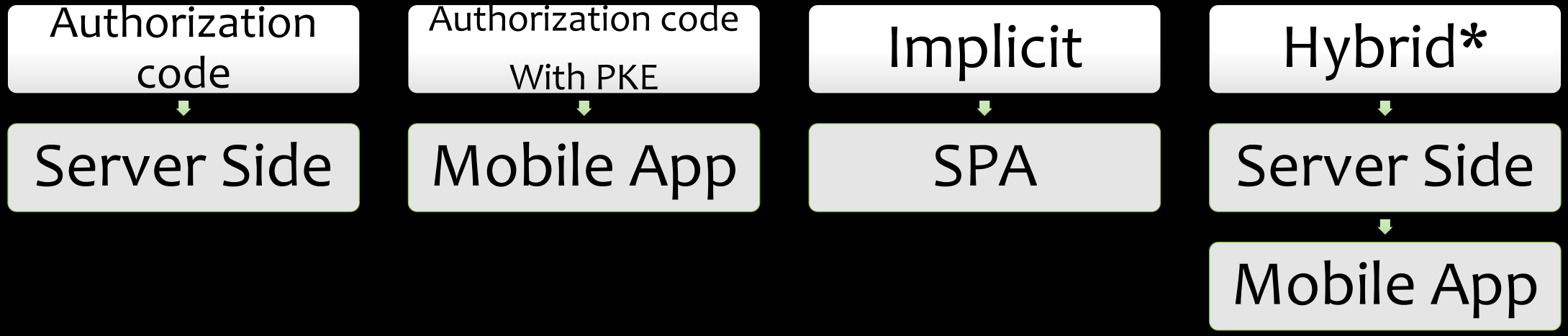
OAuth 2.0 Authorization Grant Types cont..

Authorization Code (PKCE)

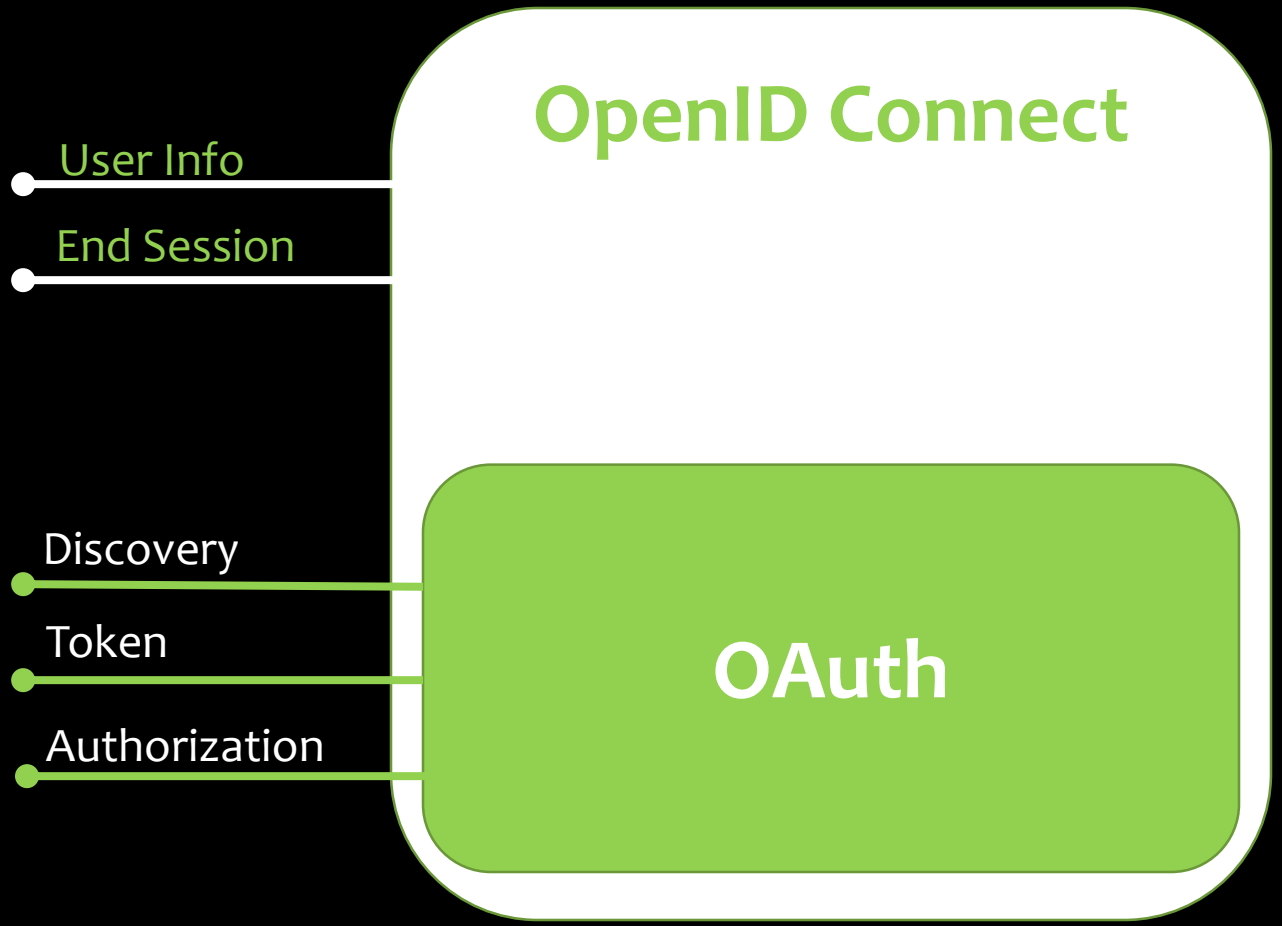
Implicit

Resource Owner Password Credentials

OpenID Connect: Authentication Flows



Authentication & Authorization



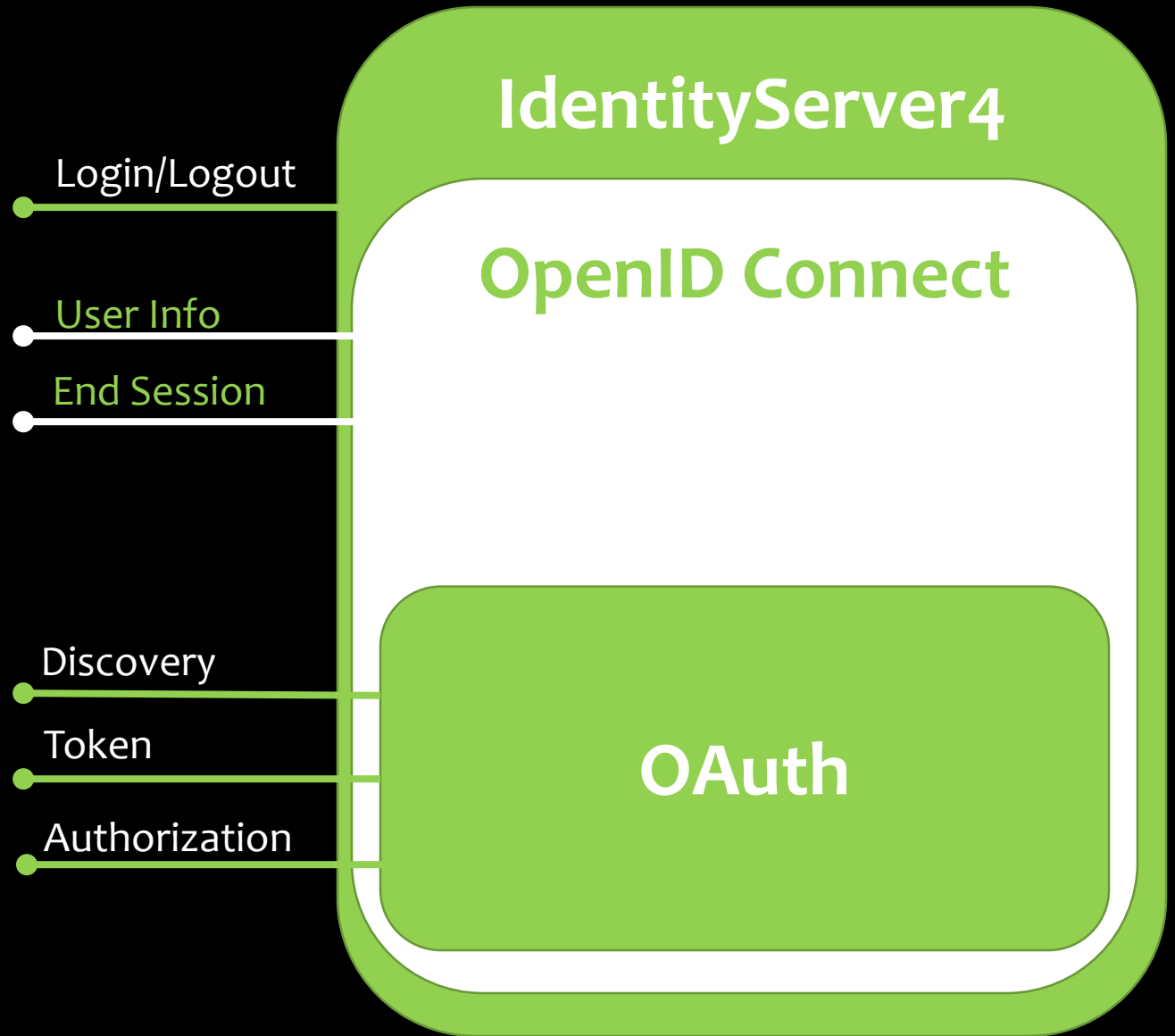
DEMO 2

MVC Web Application Authentication & Authorization

DEMO 3

SPA Web Application Authentication & Authorization

Authentication



OAuth 2.0 Spec Links

OAuth 2.0 Core

- OAuth 2.0 Framework—RFC 6749
- Bearer Token Usage—RFC 6750
- Threat Model and Security Considerations—RFC 6819

OAuth 2.0 Extensions

- JSON Web Token—RFC 7519
- OAuth Assertions Framework—RFC 7521
- SAML2 Bearer Assertion—RFC 7522, for integrating with existing identity systems
- JWT Bearer Assertion—RFC 7523, for integrating with existing identity

OpenID Connect Spec Links

OpenID Connect

- Core 1.0
- Discovery

Helpful links

- OAuth 2.0 Protocol Detailed Walkthrough
- OpenID Connect Flows
- OKTA - SaaS
- Explicit Logout from IdentityServer4
- Using existing DB with IdentityServer4
- Why not use OAuth 2.0 Resource Owner Password Grant Type

Q & A

Twitter :: @cajunAA
Instagram :: double_a_ralls
Stackoverflow :: aaronR
Email :: aaron.ralls@gmail.com
Blog :: https://arkeytek.com

Facebook.com/aaron.ralls.9
http://aaronralls.com
Github.com/aaronRalls