

OAuth 2.0 and OpenID Connect and SSO, Oh My!

Security Simplified with IdentityServer4

<http://aaronralls.com>

@cajunAA

What will you learn today?

- An overview of OAuth 2.0 and OpenID Connect protocols.
- How IdentityServer4 can be used to secure your API's, Web, Console/Services and Mobile applications.
- How IdentityServer4 can be used to implement an SSO solution

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

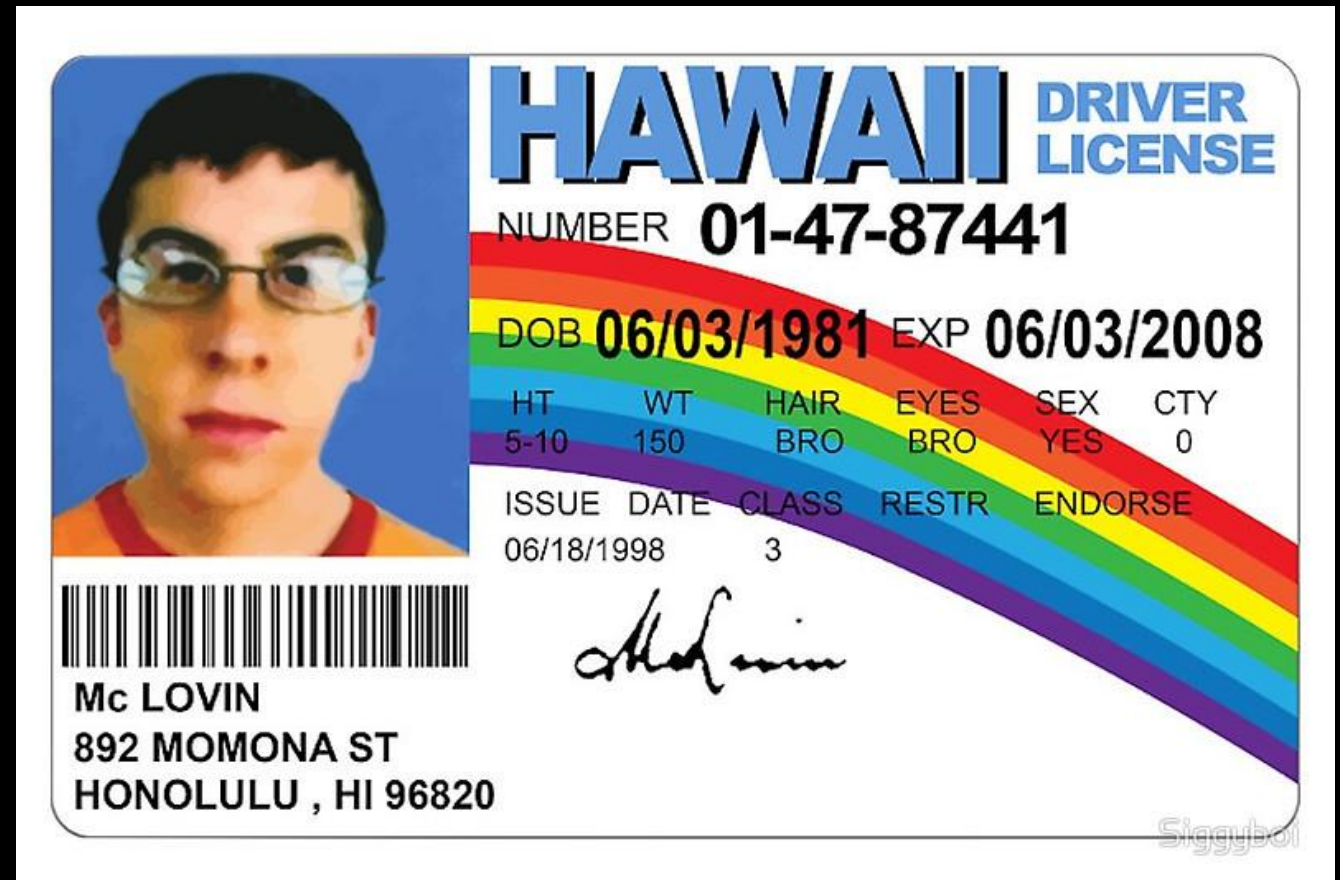
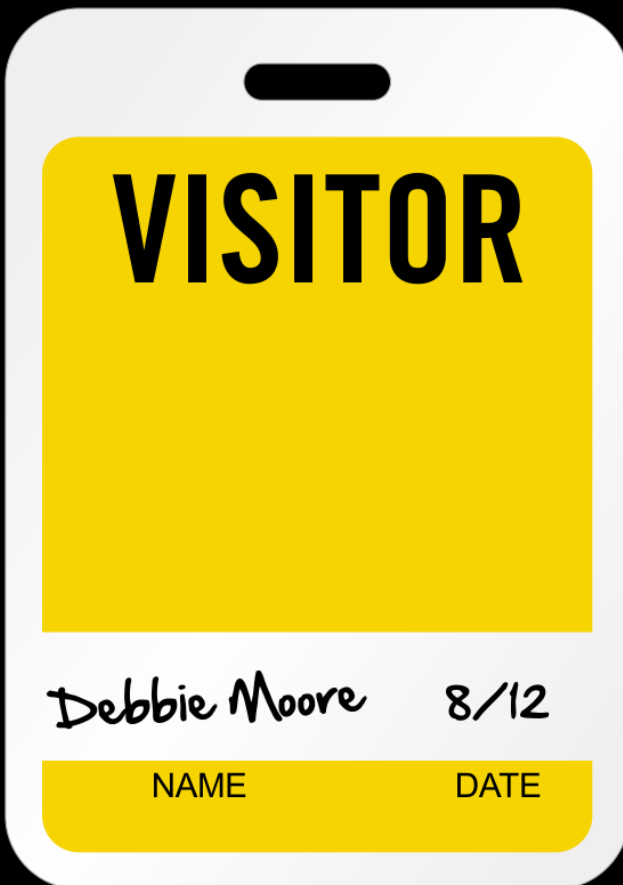
- [JSON Web Token](#)—RFC 7519
- [OAuth Assertions Framework](#)—RFC 7521
- [SAML2 Bearer Assertion](#)—RFC 7522, for integrating with existing identity systems
- [JWT Bearer Assertion](#)—RFC 7523, for integrating with existing identity

OpenID Connect Spec Links

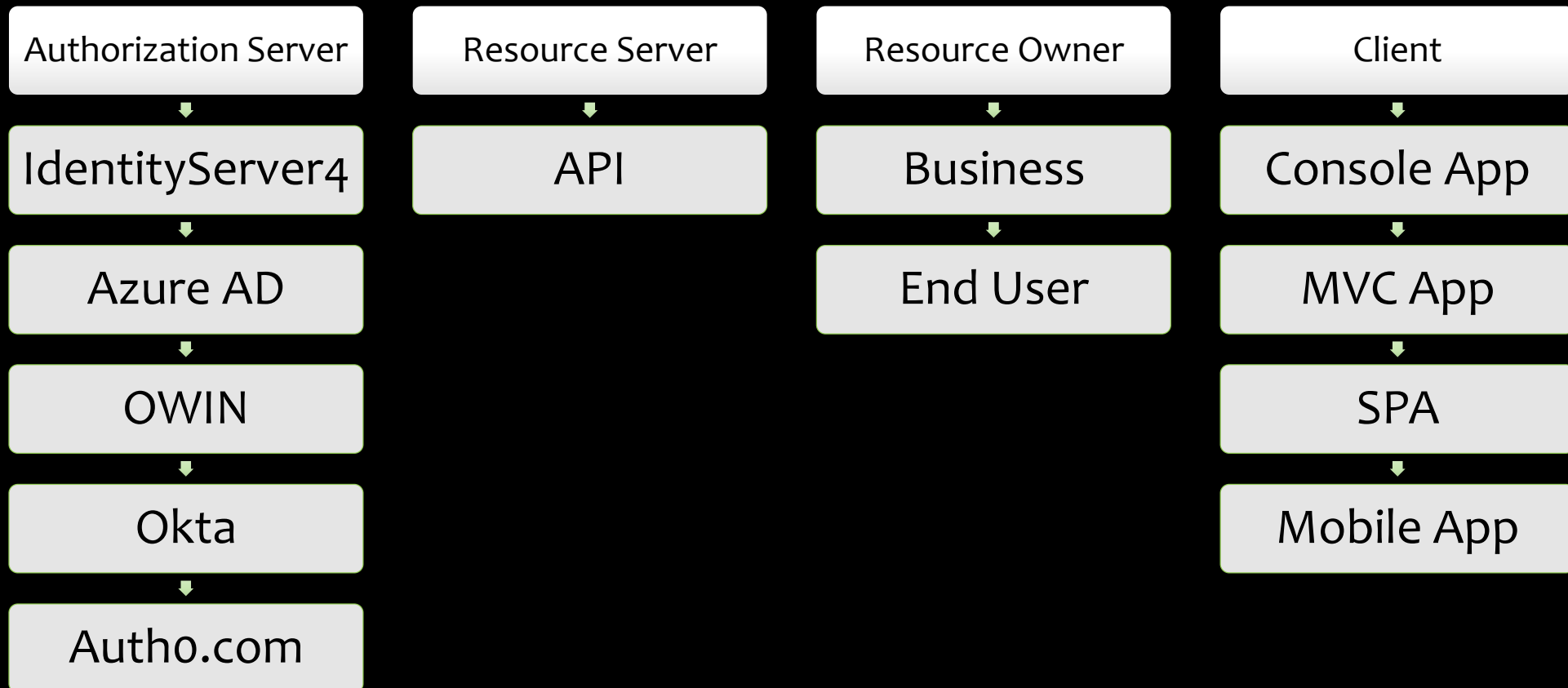
OpenID Connect

- [Core 1.0](#)
- [Discovery](#)

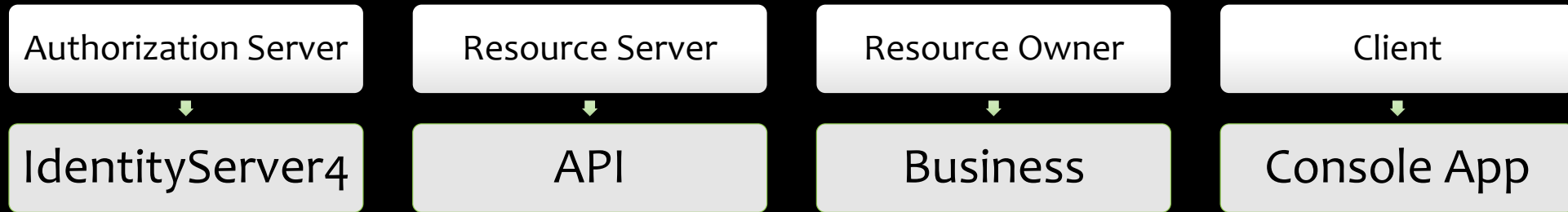
Authorization vs. Authentication



OAuth 2.0 (Authorization)



OAuth 2.0 (Authorization)



OAuth 2.0 Code Flow

Front Channel
(Browser)

Back Channel
(Web Server to Auth Server)

OAuth 2.0 Implicit Flow

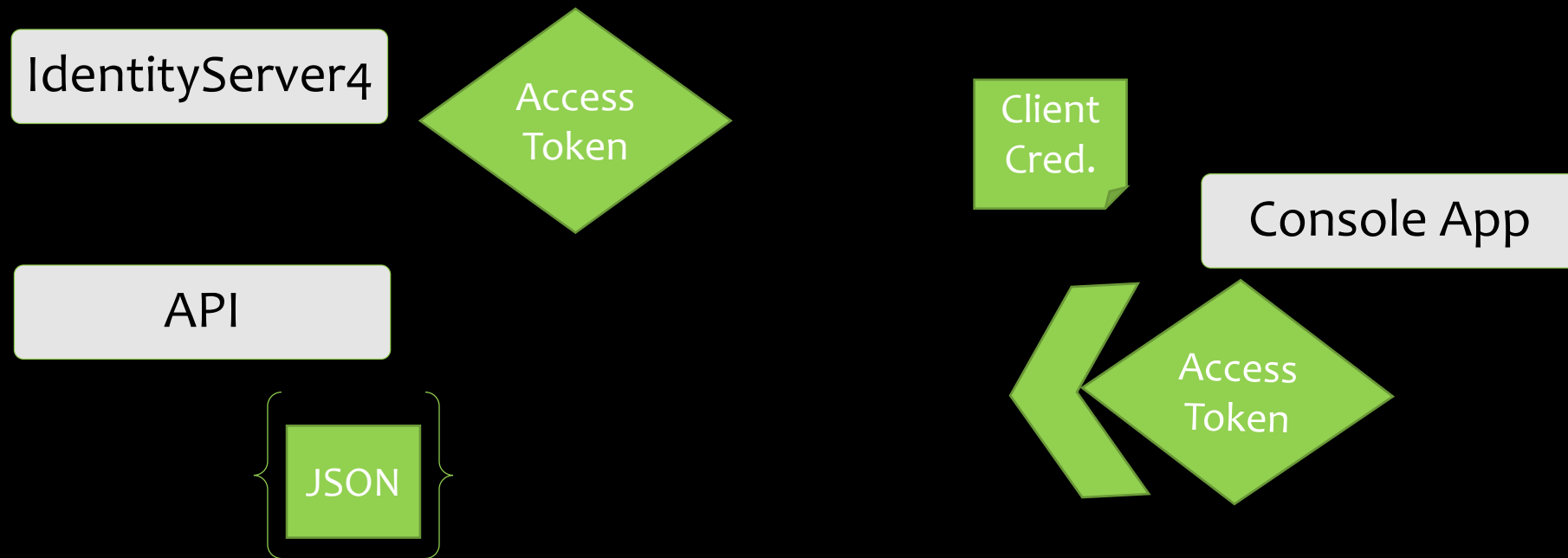
Front Channel
(Browser - SPA)

OAuth 2.0 Access Tokens

Reference

Self contained – JWT
- [JWT.IO](https://jwt.io)

OAuth 2.0 Authorization Grant Type: Client Credentials



DEMO 1

Client Credentials
Console App/Windows Service
accessing a secured API

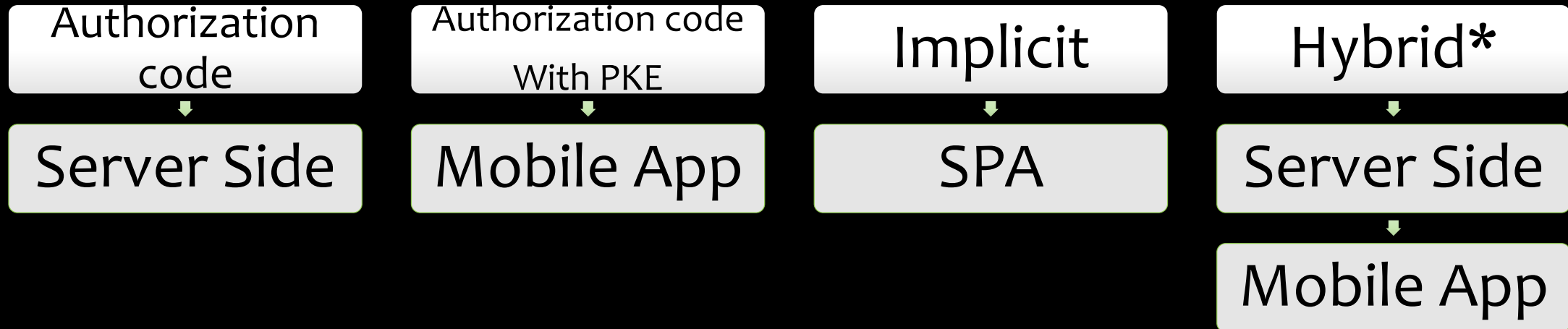
OAuth 2.0 Authorization Grant Types cont..

Authorization Code
(with or without PKCE)

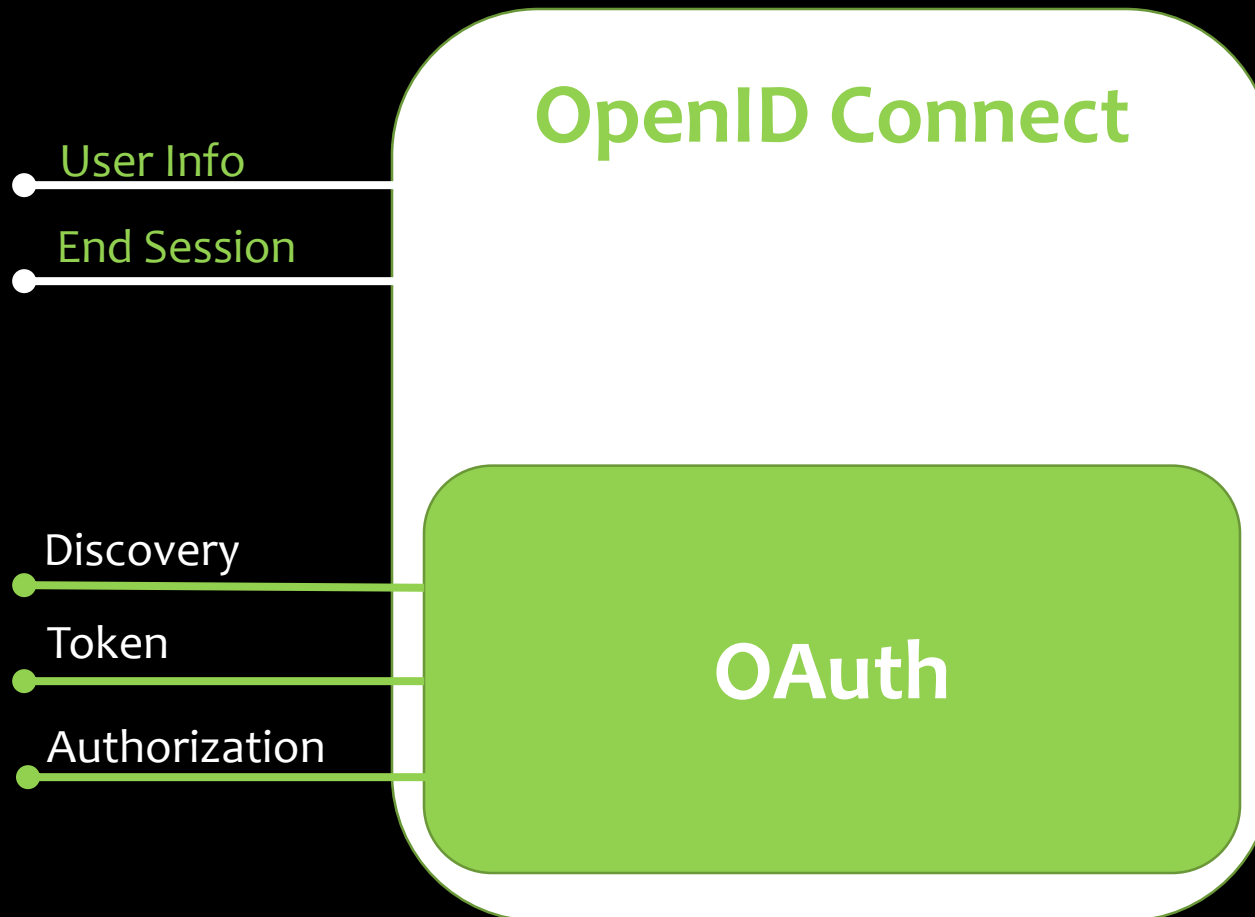
Implicit

Resource Owner Password Credentials

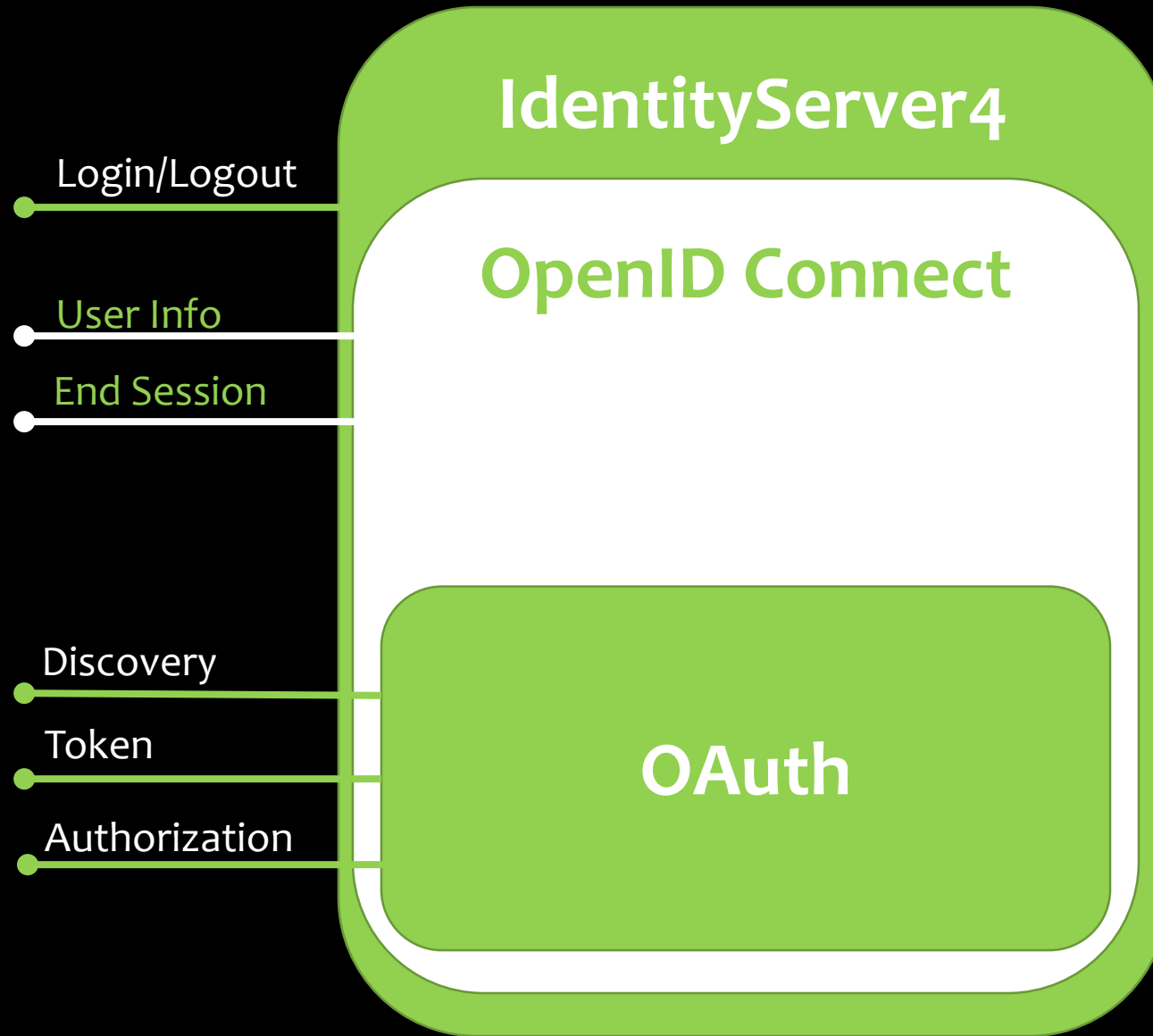
OpenID Connect: Authentication Flows



Authentication & Authorization



Authentication



DEMO 2

MVC Web Application Authentication &
Authorization

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](#)
- <https://github.com/IdentityServer/IdentityServer4/tree/master/samples/Quickstarts>
- <https://www.scottbrady91.com/Identity-Server/Encrypting-Identity-Tokens-in-IdentityServer4>

Helpful links

SPA Web Application Authentication & Authorization

<https://docs.microsoft.com/en-us/aspnet/core/security/authentication/identity-api-authorization?view=aspnetcore-3.0>

Q & A

Twitter :: @cajunAA

Instagram :: double_a_ralls

Stackoverflow :: aaronR

Email :: aaron.ralls@gmail.com

Blog :: <https://arkeytek.com>

[Facebook.com/aaron.ralls.9](https://facebook.com/aaron.ralls.9)

<http://aaronralls.com>

[Github.com/aaronRalls](https://github.com/aaronRalls)

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](#)