ATLANTA | CODE | CAMP

Authentication Using OpenID Connect and OAuth2

@ATLCODECAMP

HTTPS://ATLANTACODECAMP.COM/2016

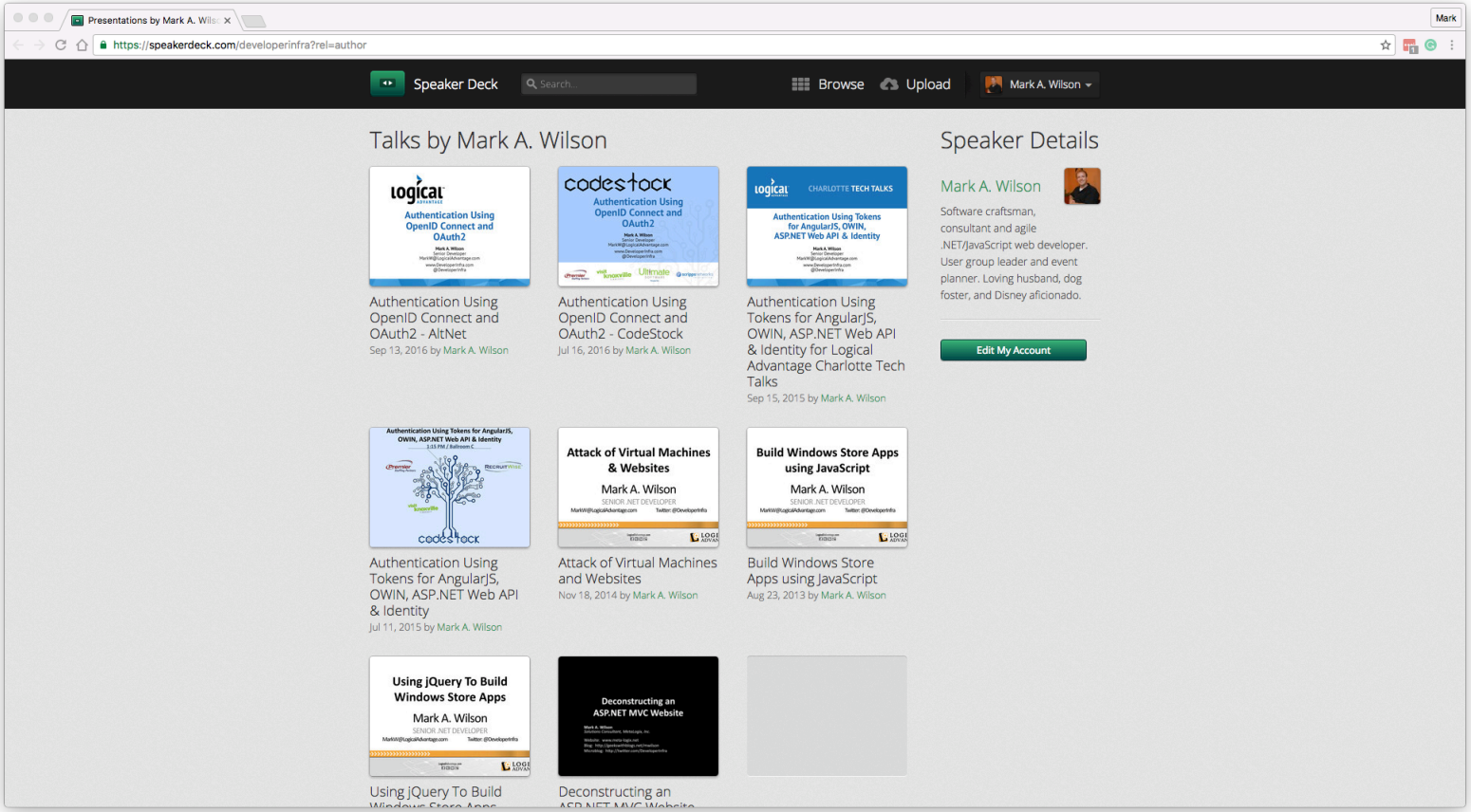
Mark A. Wilson

www.developerinfra.com

@DeveloperInfra

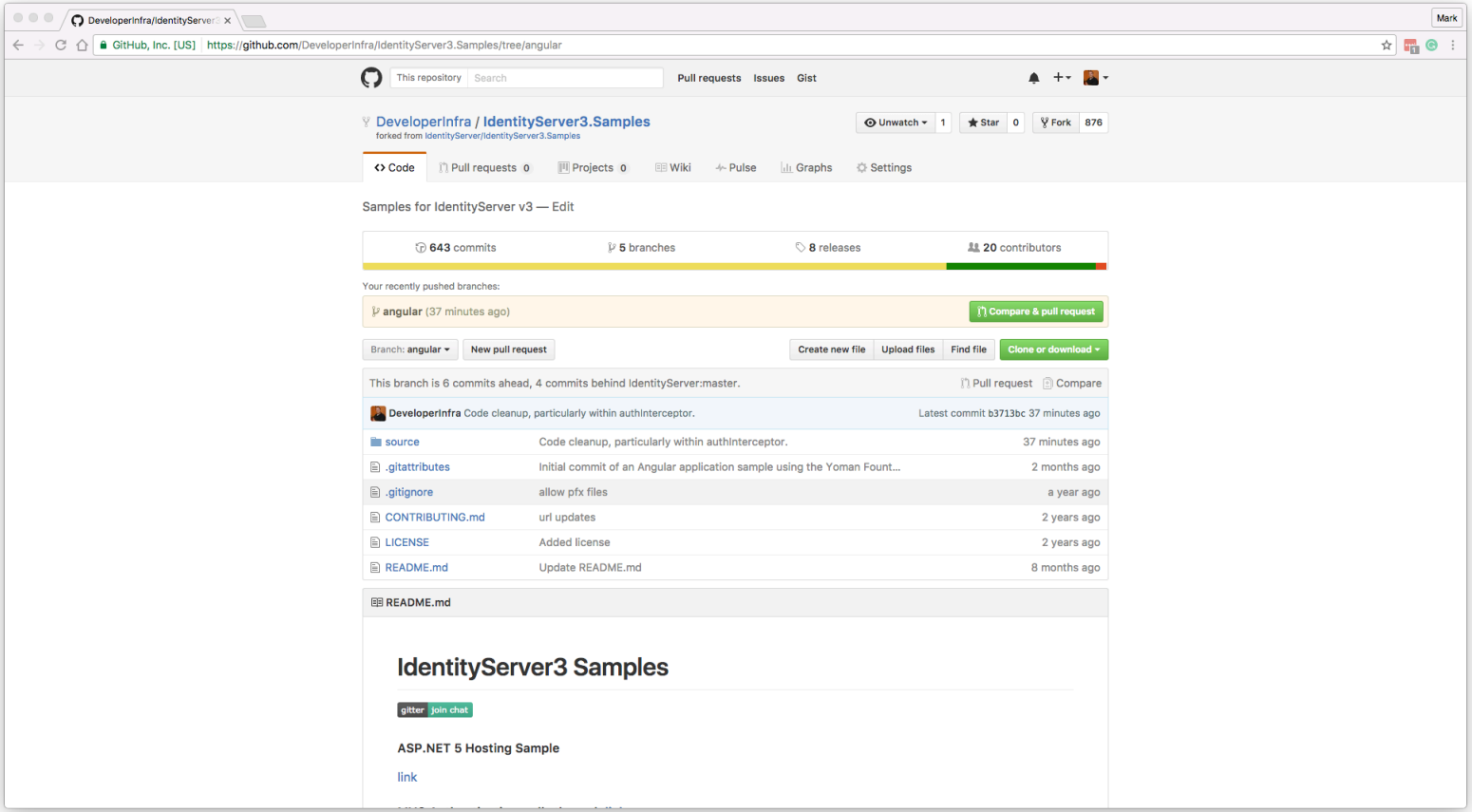
Software craftsman, consultant and agile .NET/JavaScript web developer. User group leader and event planner. Loving husband, dog foster, and Disney aficionado.

Slide Deck



- https://speakerdeck.com/developerinfra

Source Code



- https://github.com/DeveloperInfra/IdentityServer3.Samples/tree/angular

Logical Advantage

www.logicaladvantage.com

Our mission is to partner with our clients to provide strategies and solutions that maximize the ROI of Enterprise Asset Intelligence and Human Capital Development.

Platinum Sponsors

Gold Sponsors

Silver Sponsors

SWAG Sponsors

Surveys and Prizes

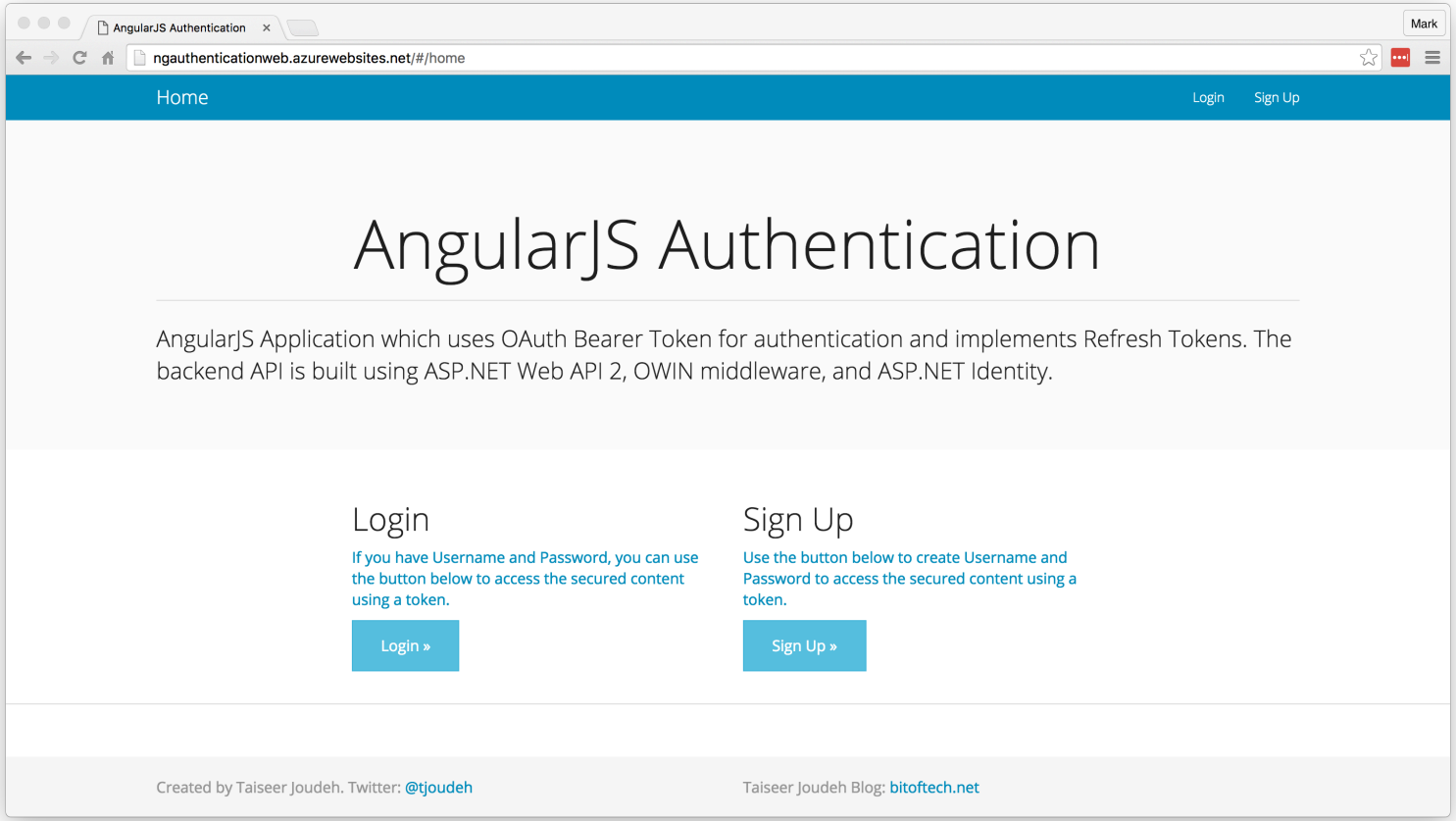
Please complete the session and event surveys!

- ✓ 1 ticket per session survey
- ✓ 1 ticket for the event survey
- ✓ 1 ticket for completing the booth game

Drawing for prizes begins at 5pm in Q202

Authentication Using Tokens for AngularJS, OWIN, ASP.NET Web API & Identity

AngularJS Authentication Demo



- http://bitoftech.net/2014/06/01/token-based-authentication-asp-net-web-api-2-owin-asp-net-identity/

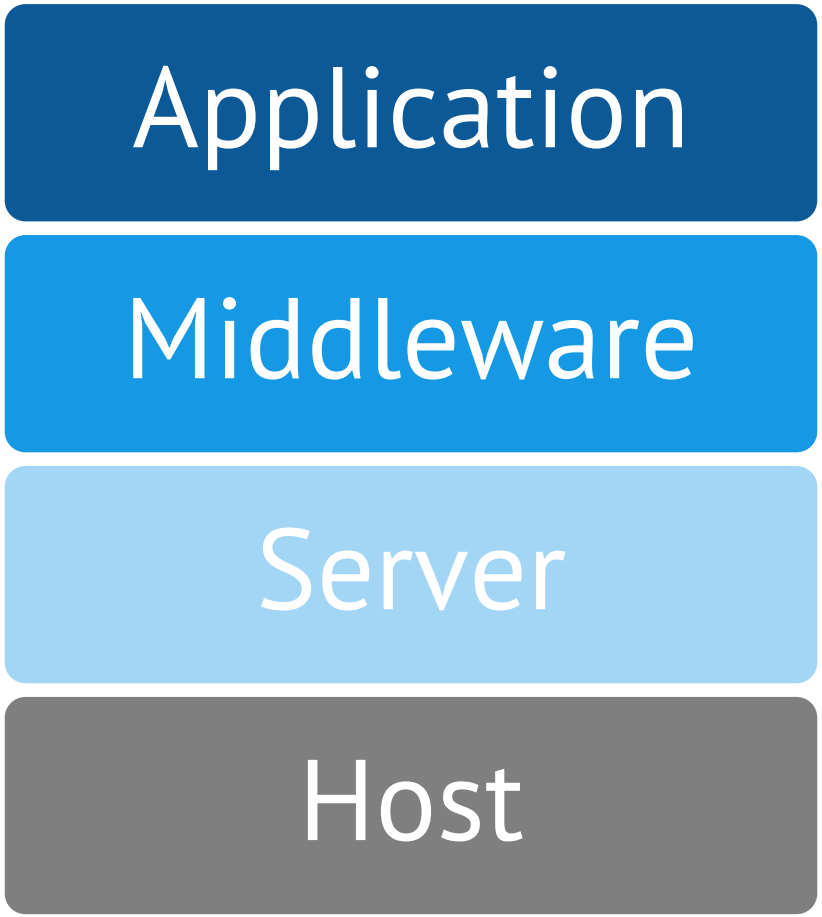
Open Web Interface for .NET

- A *specification*, not a framework
- A standard for an interface between .NET web applications and web servers
- Decouple the application from the [IIS] server
- Encourage development of simple and lightweight modules
- Project Katana is OWIN implementations for Microsoft servers and frameworks

- https://en.wikipedia.org/wiki/Open_Web_Interface_for_.NET

Project Katana

- A set of OWIN components built by Microsoft
- Enables ASP.NET applications to be flexible, portable, lightweight, and provide better performance
- Host – An executable process
- Server – Opens network sockets
- Middleware – Pipeline of OWIN components
- Application – Your code



- http://www.asp.net/aspnet/overview/owin-and-katana/an-overview-of-project-katana

OAuth 2.0

- Authorization framework
- Began in November 2006 when Blaine Cook was developing the Twitter OpenID implementation
- OAuth 1.0 – April 2010
- OAuth 2.0 – October 2012
- Allows *access tokens* be issued to third-party clients/websites
- Not without its critics and controversy

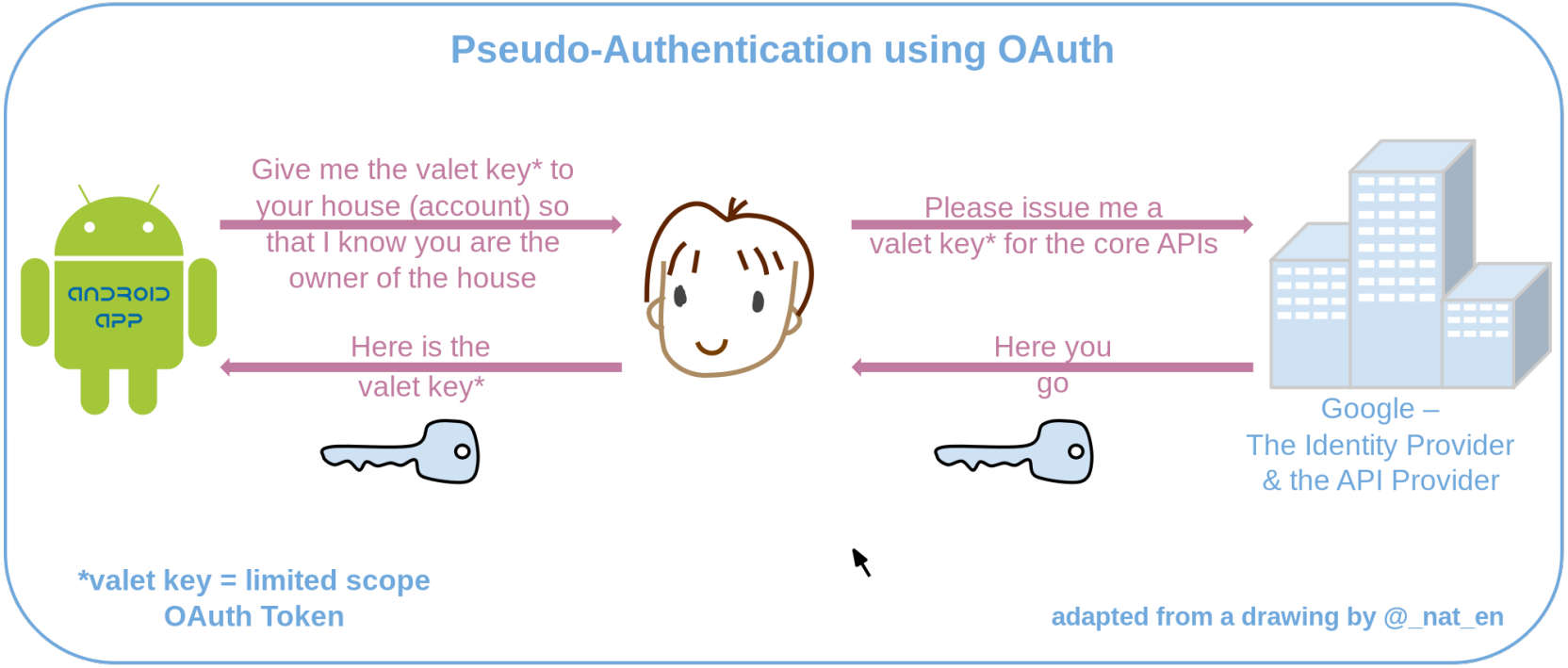
- https://en.wikipedia.org/wiki/OAuth

OAuth 2.0

- Does not support signature, encryption, channel binding, or client verification.
- Relies completely on Transport Layer Security (TLS) / Secure Sockets Layer (SSL).
- “Covert Redirect” involving the redirect_uri.
- Phishing site attacks.
- Eran Hammer resigned as lead author in July 2012.
- “OAuth 2.0 is not an authentication protocol.”

- https://en.wikipedia.org/wiki/OAuth

Pseudo-Authentication using OAuth



- https://en.wikipedia.org/wiki/OAuth

Project Katana

”**vNext is the successor to Katana** (which is why they look so similar). Katana was the beginning of the break away from System.Web and to more modular components for the web stack.”

– David Fowler
ASP.NET Core Architect

- http://forums.asp.net/t/2004299.aspx?Katana%20VS%20vNext

Is it worth it?

Pros

- Authentication & authorization abstracted into a "component" using standard protocol (OAuth2)
- Eliminated the cookie and Cross-Site Request Forgery (CSRF) problems for SPAs
- Encrypted and signed tokens (using shared machine key)
- SSL by default
- Resource owner flow very easy.

Cons

- Exponentially complex
- Adding refresh tokens required implementing persistence
- Implicit flow (native or JS apps) lacked login/consent view engine
- Lacking in validation
- The ASP.NET team decided to discontinue Project Katana to focus on consuming tokens
- "Note: This outline should not be intended to be used for creating a secure production app."

- https://leastprivilege.com/2014/03/24/the-web-api-v2-oauth2-authorization-server-middlewareis-it-worth-it/

Modern Applications

This happened…

No SOAP

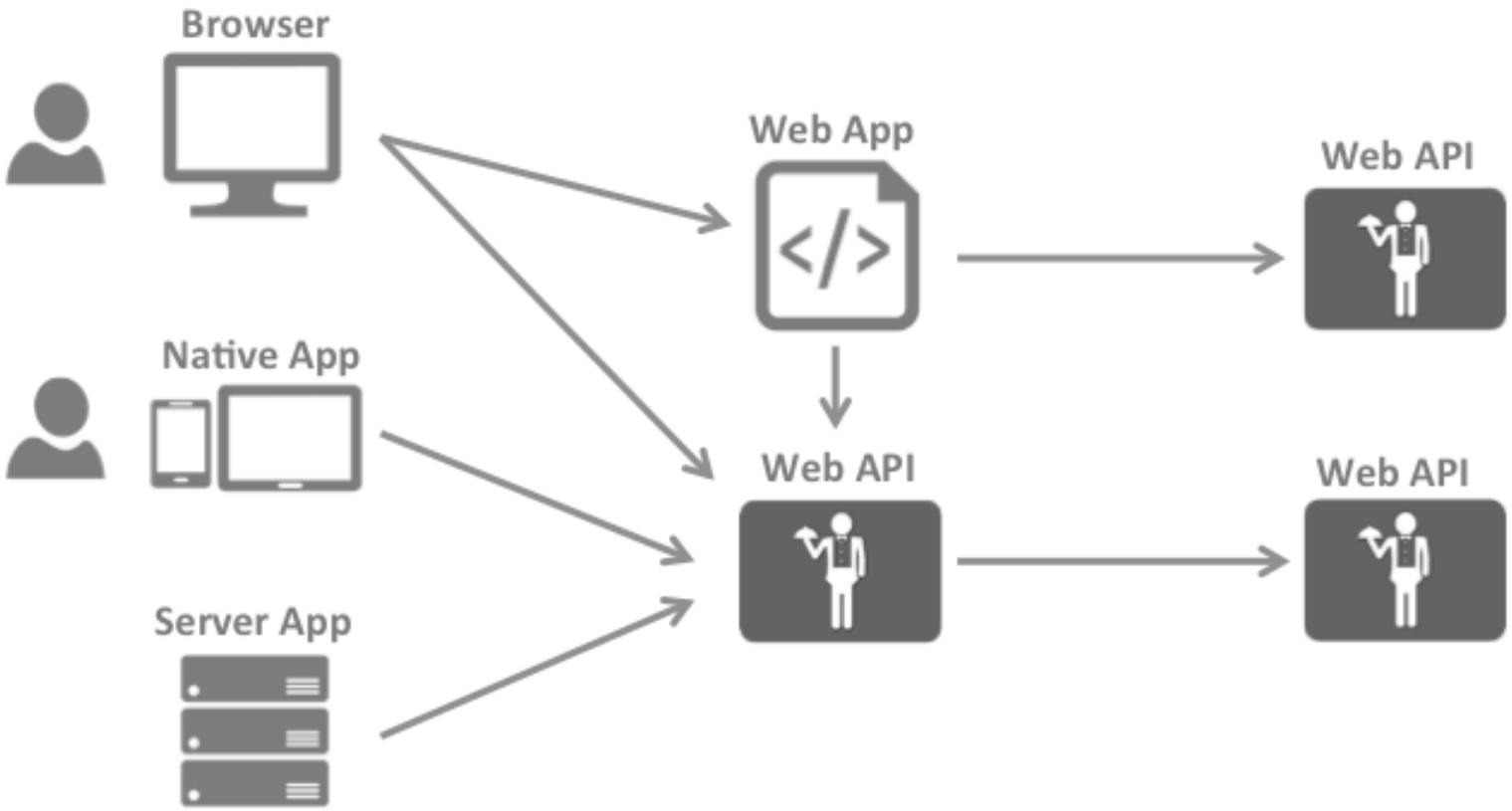
No SAML

No WS*

No Windows

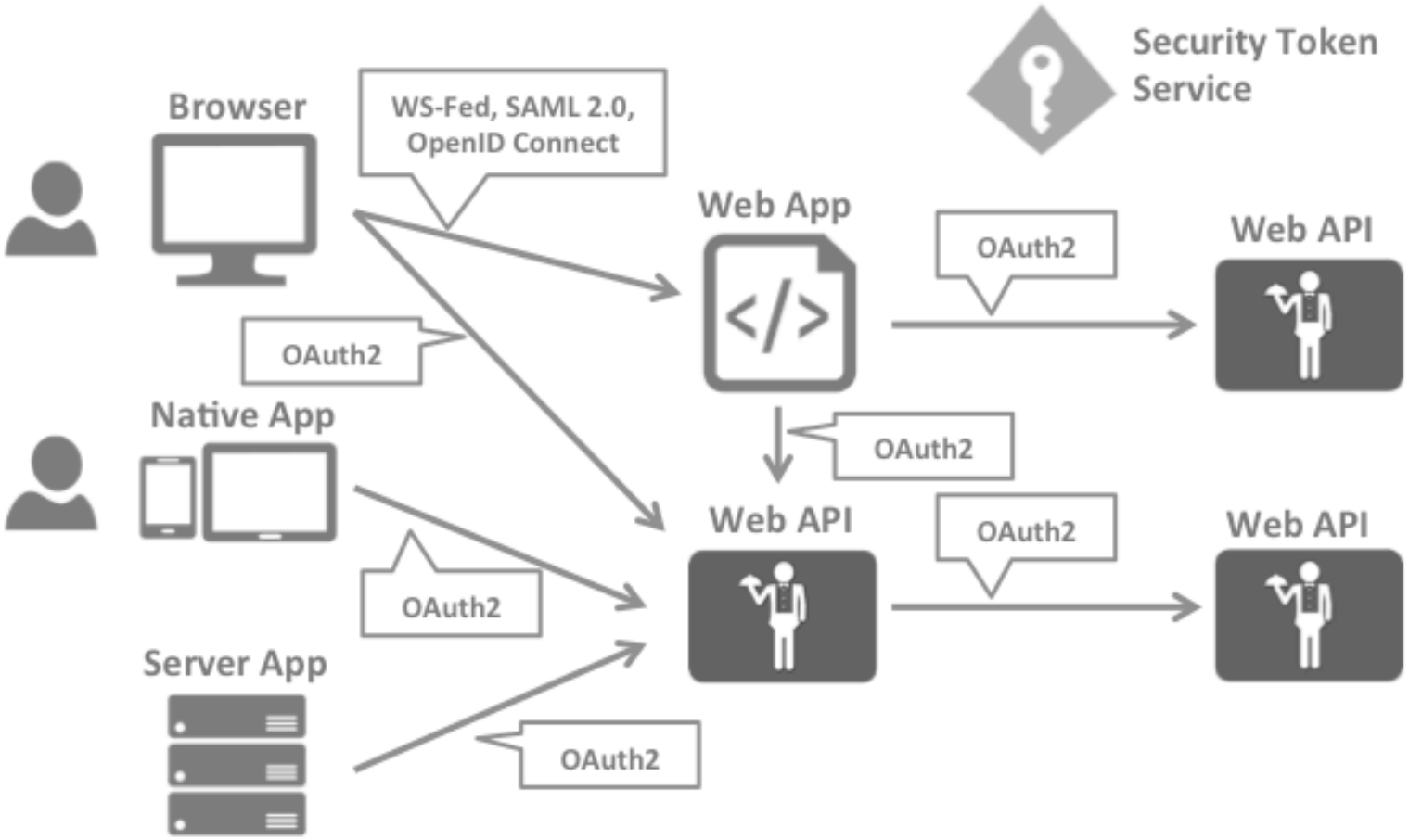
No Enterprise

The Big Picture



- https://identityserver.github.io/Documentation/docsv2/overview/bigPicture.html

Security Protocols



- https://identityserver.github.io/Documentation/docsv2/overview/bigPicture.html

Security Concerns

Authentication

Identity of the current user

API Access

Application identity and/or delegating the user's identity

- https://identityserver.github.io/Documentation/docsv2/overview/bigPicture.html

Security Assertion Markup Language

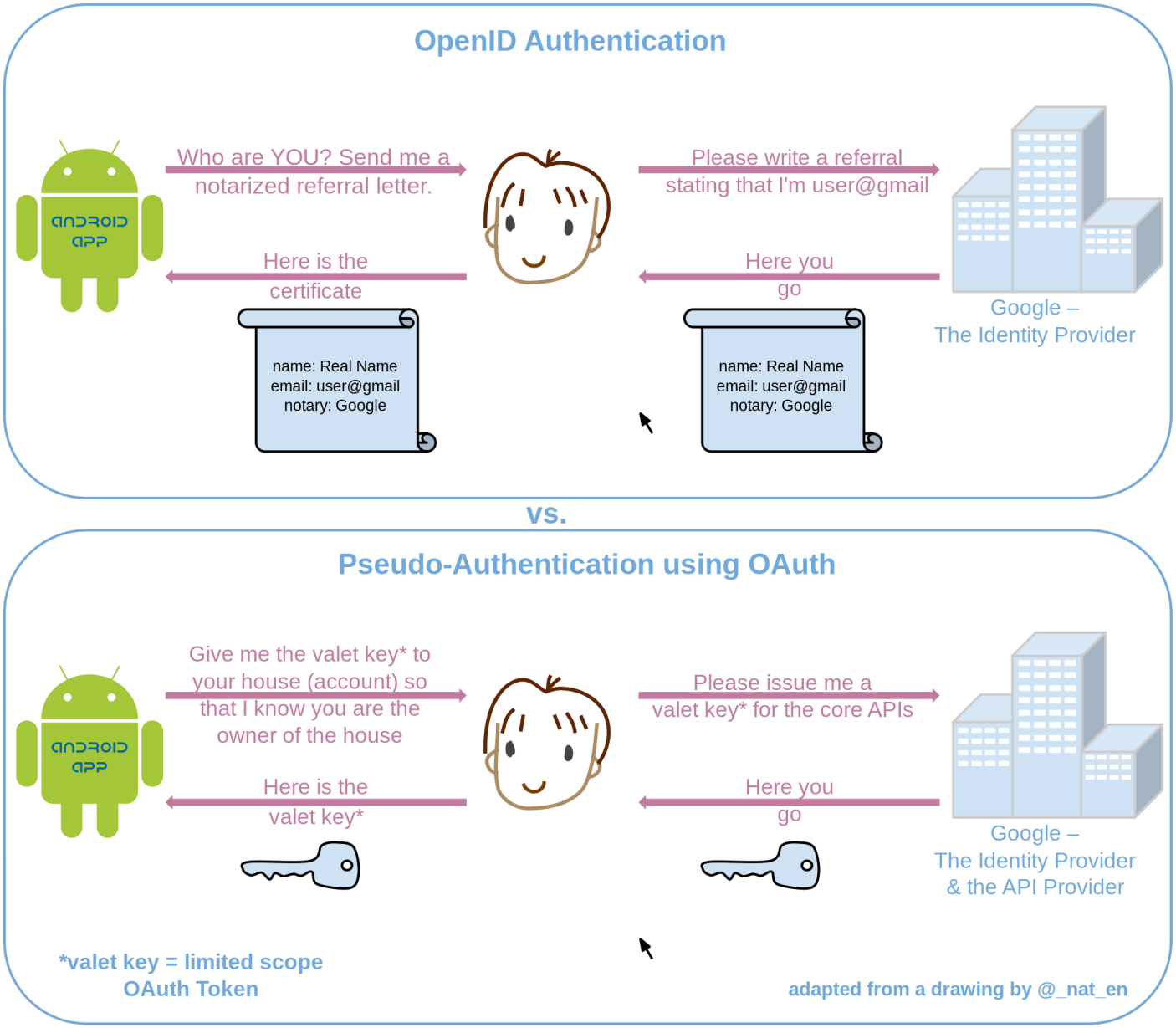
- Most popular & widely deployed
- SAML 1.0 – November 2002
- SAML 1.1 – September 2003
- SAML 2.0 – March 2005
- Browser single sign-on (SSO)
- Problematic beyond intranet
- XML-based
- “Enterprisey” and “not trivial”

- https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

OpenID Connect

- Newest but generally considered to be the future
- OpenID – May 2005
- OpenID 2.0 – December 2007
- OIDC [3.0] – February 2014
- Designed to be more usable by native and mobile applications
- RESTful HTTP API using JSON
- Authentication layer on top of the OAuth 2.0 authorization framework
- Uses the JSON Web Token (JWT) and JSON Object Signing and Encryption (JOSE) specs

- https://en.wikipedia.org/wiki/OpenID



- https://en.wikipedia.org/wiki/OAuth

Better Together

- https://identityserver.github.io/Documentation/docsv2/overview/bigPicture.html

Authentication Using OpenID Connect and OAuth2

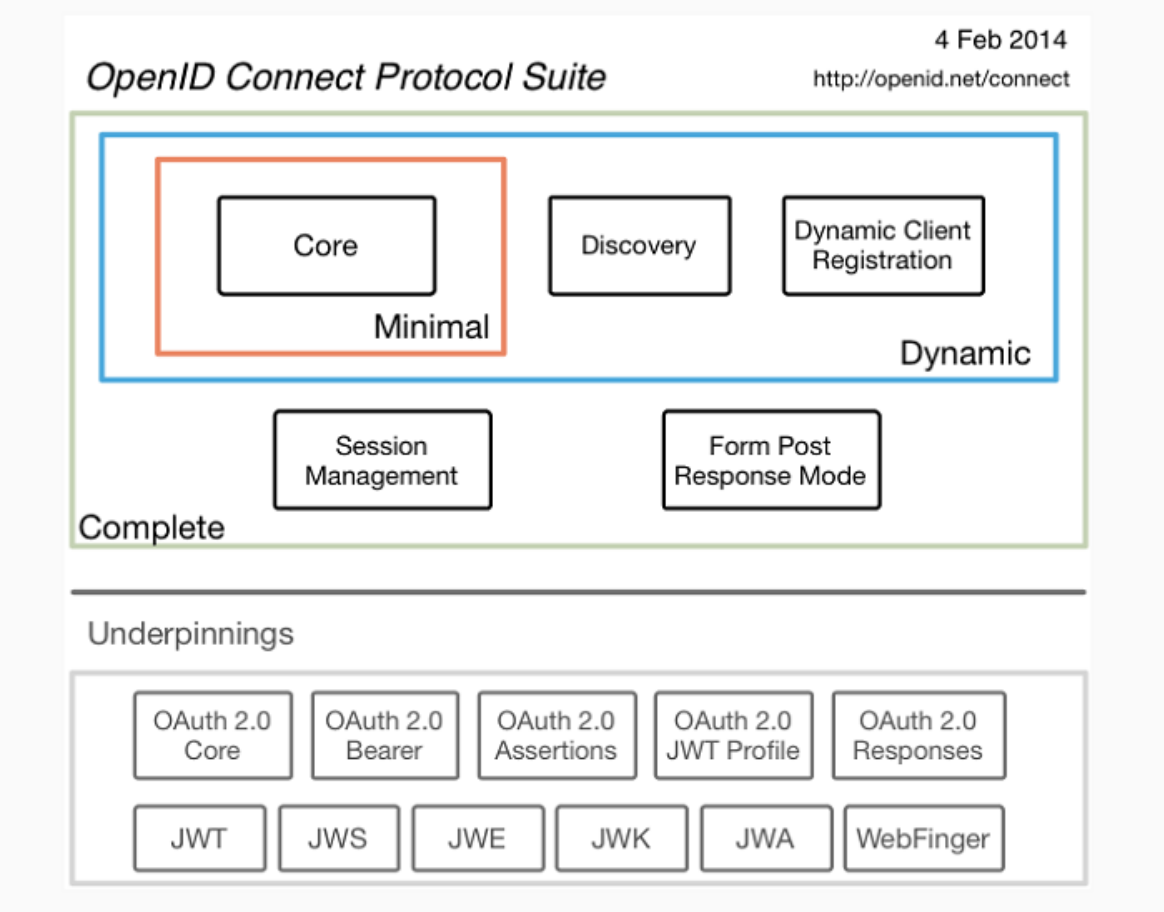
OpenID Connect

"OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol."

- Defines identity tokens
- Defines standard token type
- Defines standard cryptography
- Defines validation procedures
- Defines flows for browser, native, and server-based apps
- Combines authentication with short/long-lived delegated API access

- http://openid.net/connect/

OpenID Connect



- http://openid.net/connect/

OpenID Connect

Authorize Endpoint

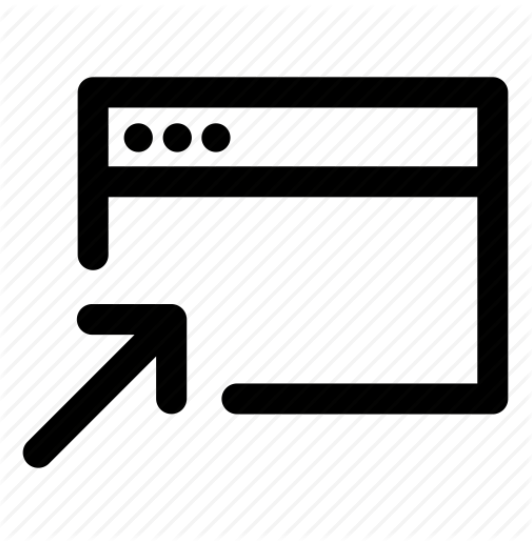
Token Endpoint

UserInfo Endpoint

Flows

Implicit Flow

(Browser-based)



Hybrid Flow

(Native/Mobile)

Client Credentials Flow

(Server-to-Server/IoT)

Implicit Flow

GET /authorize

?**client_id**=app1

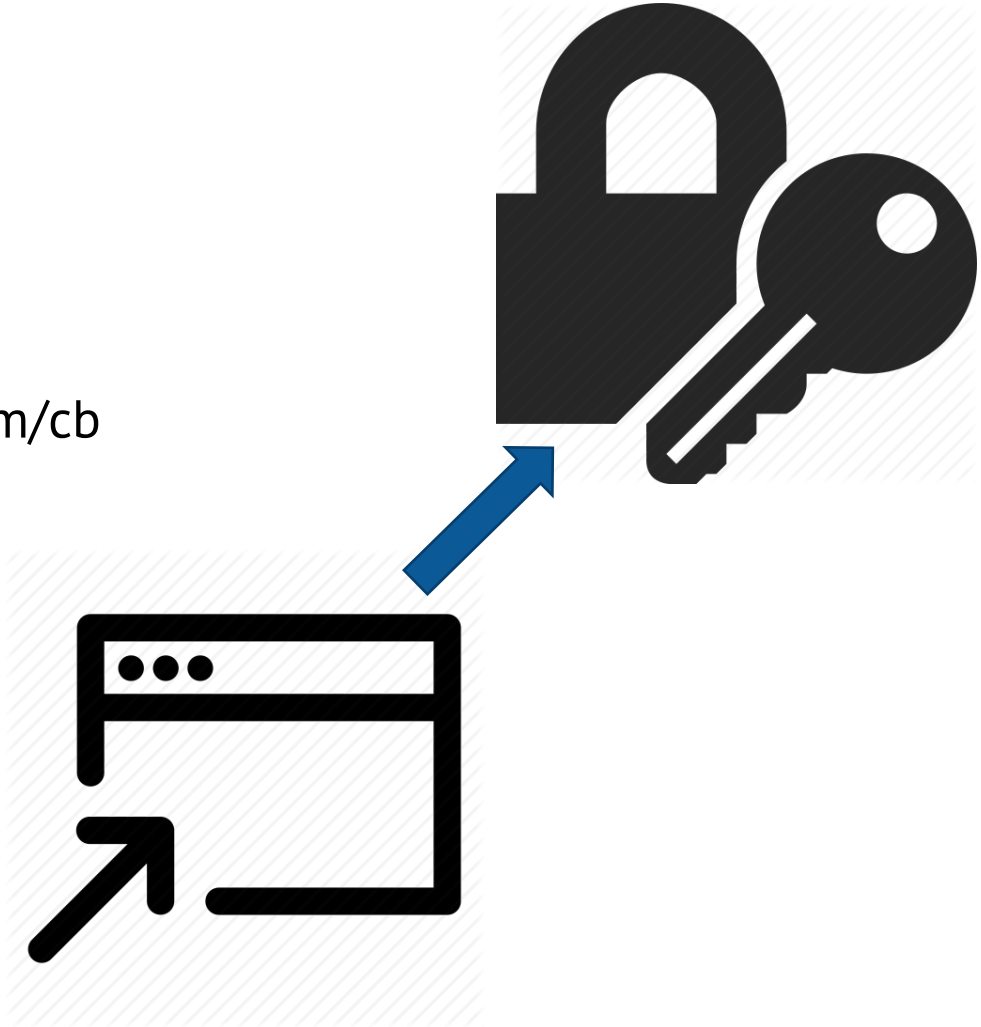
&**redirect_uri**=https://app.com/cb

&**response_type**=id_token

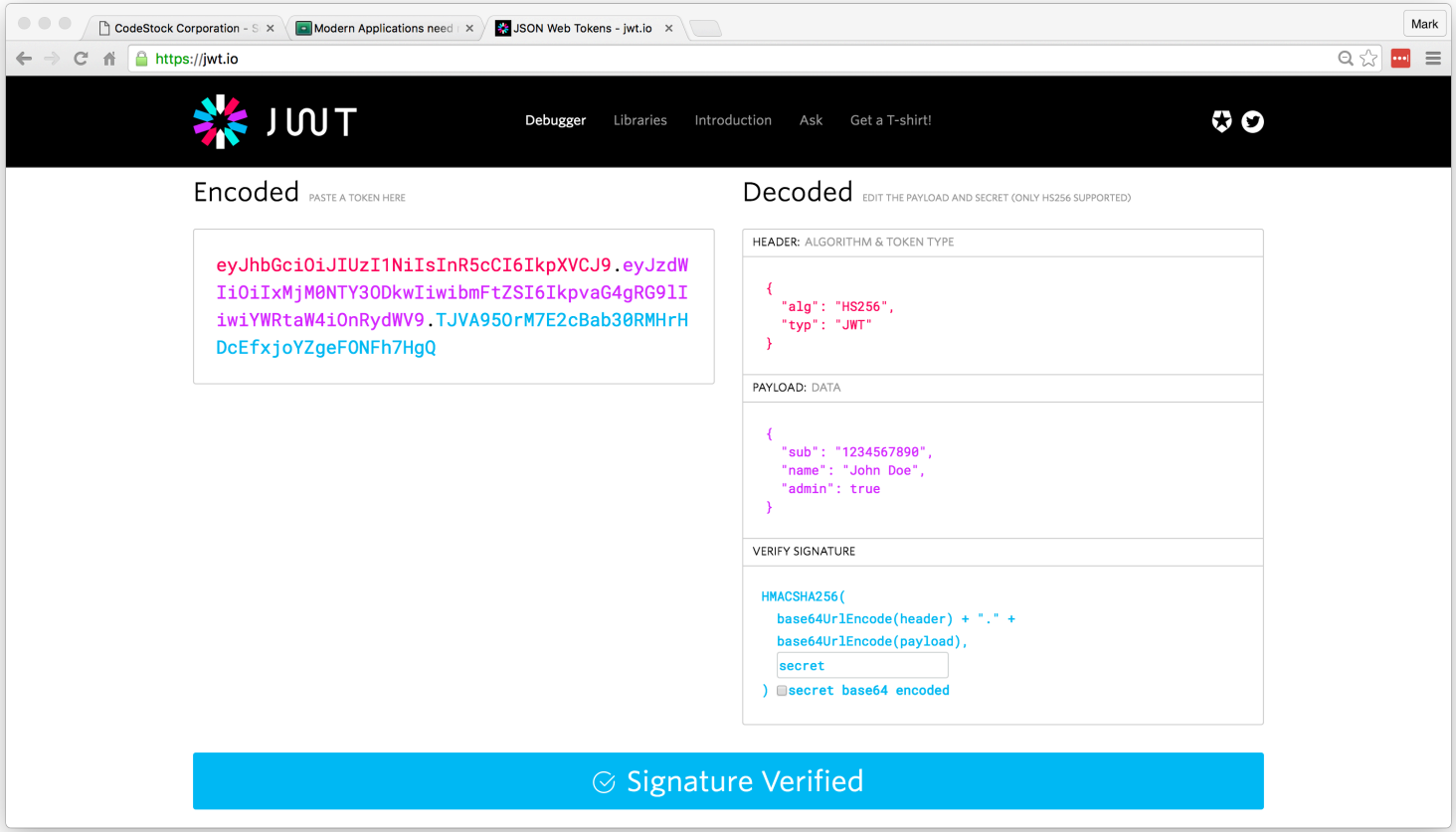
&**response_mode**=form_post

&**nonce**=a1b...x9z

&**scope**=openid email

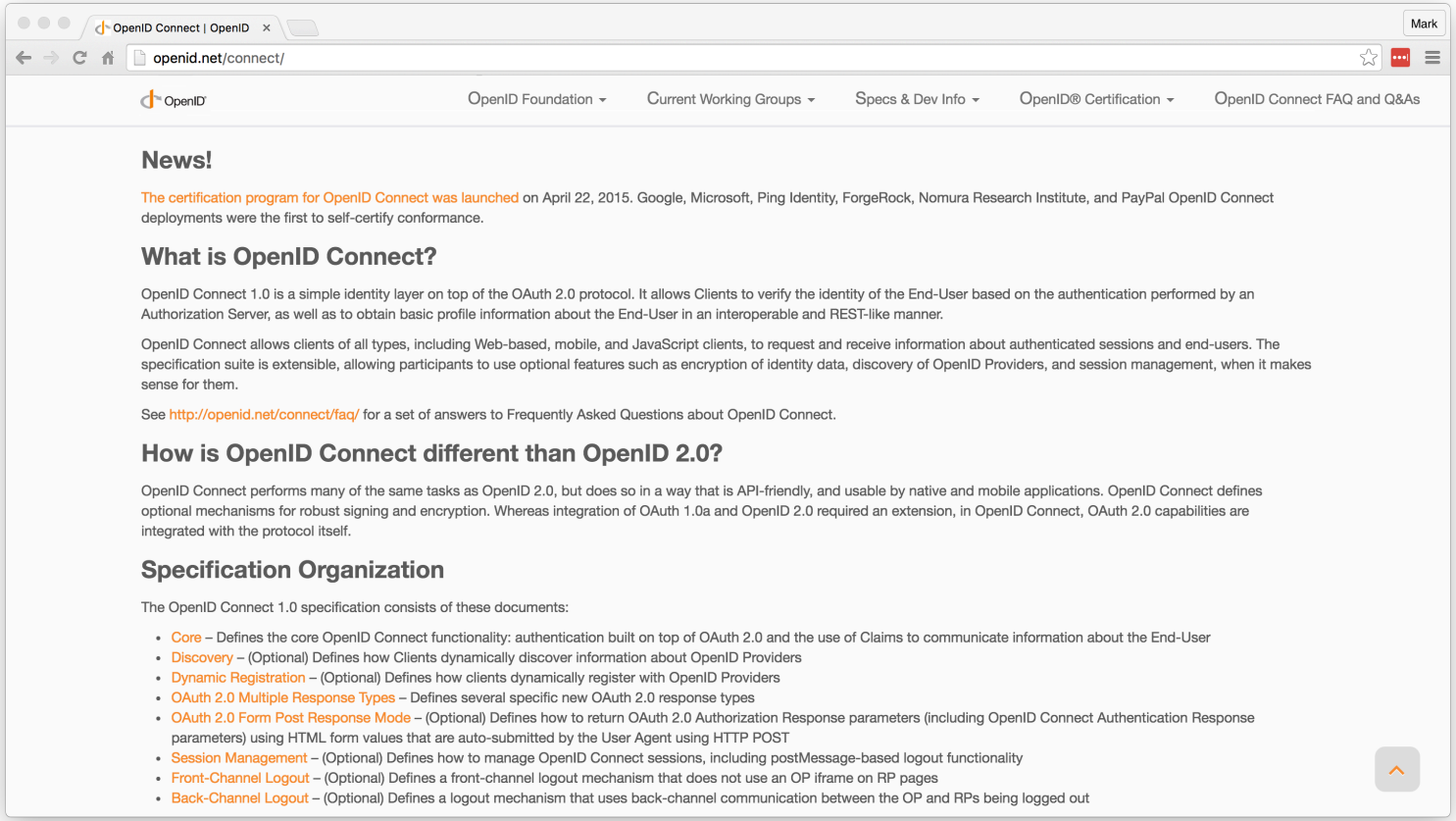


Identity Token



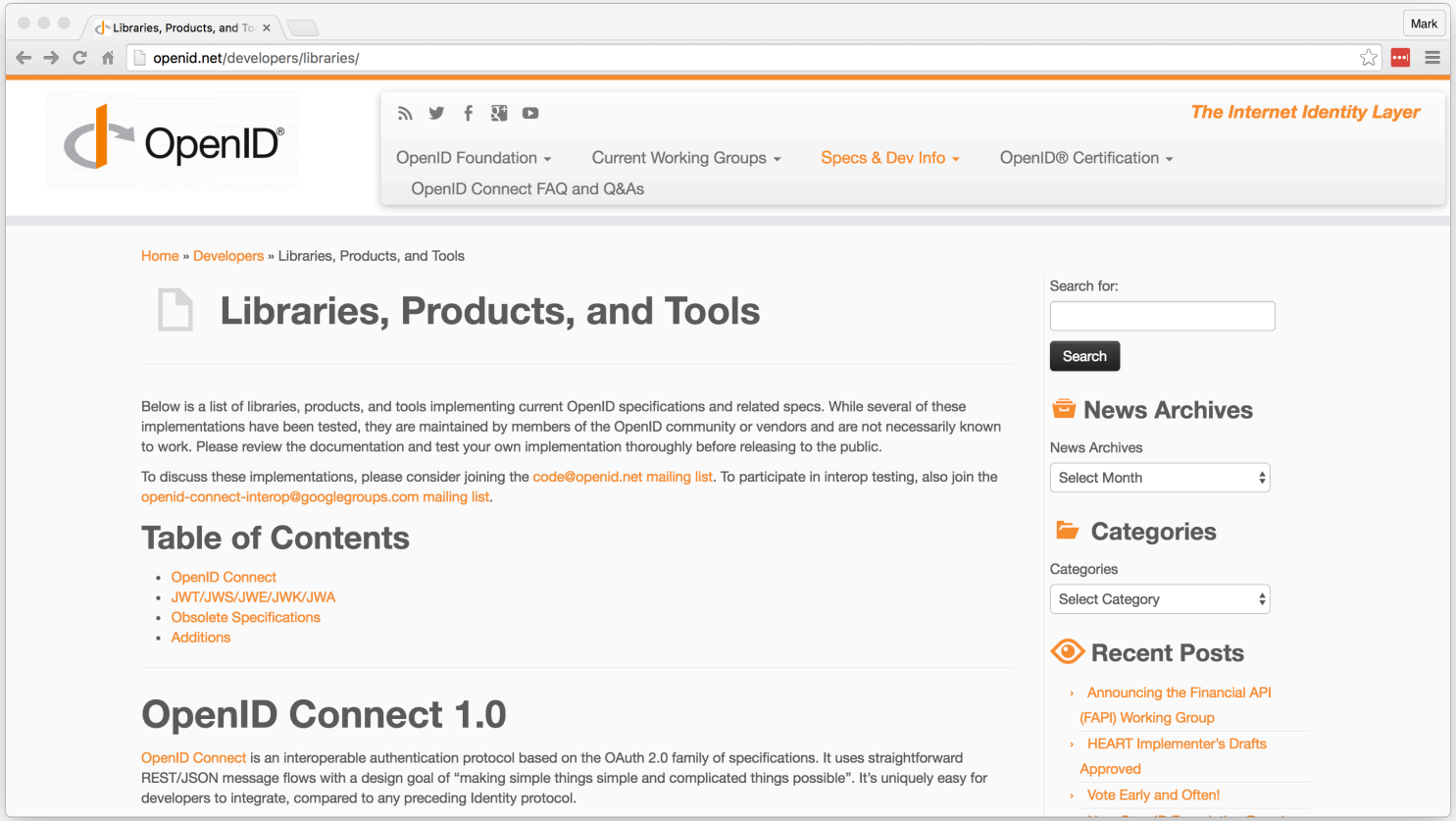
- https://jwt.io/

Getting Started



- http://openid.net/connect/

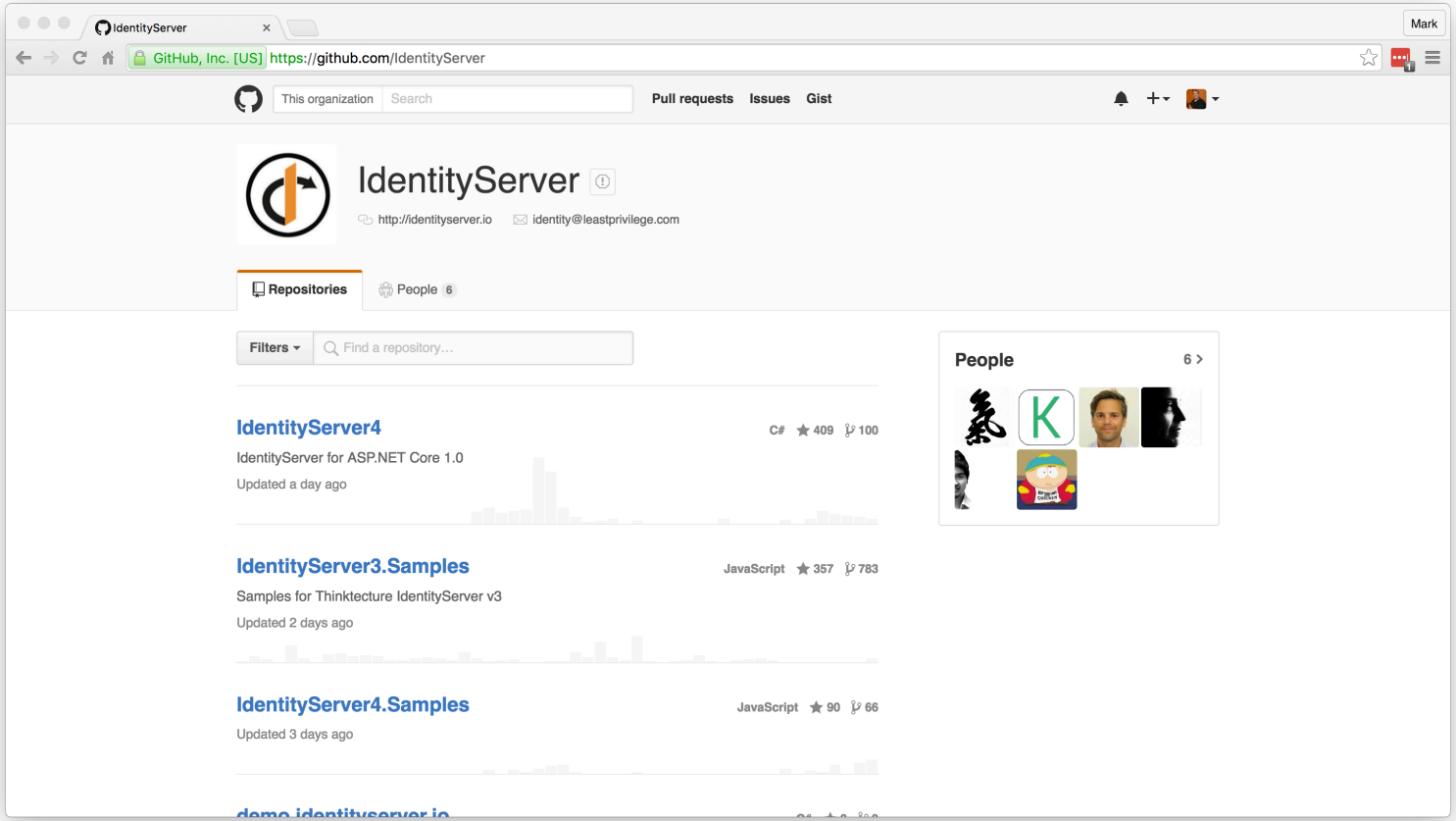
Getting Started



- http://openid.net/developers/libraries/

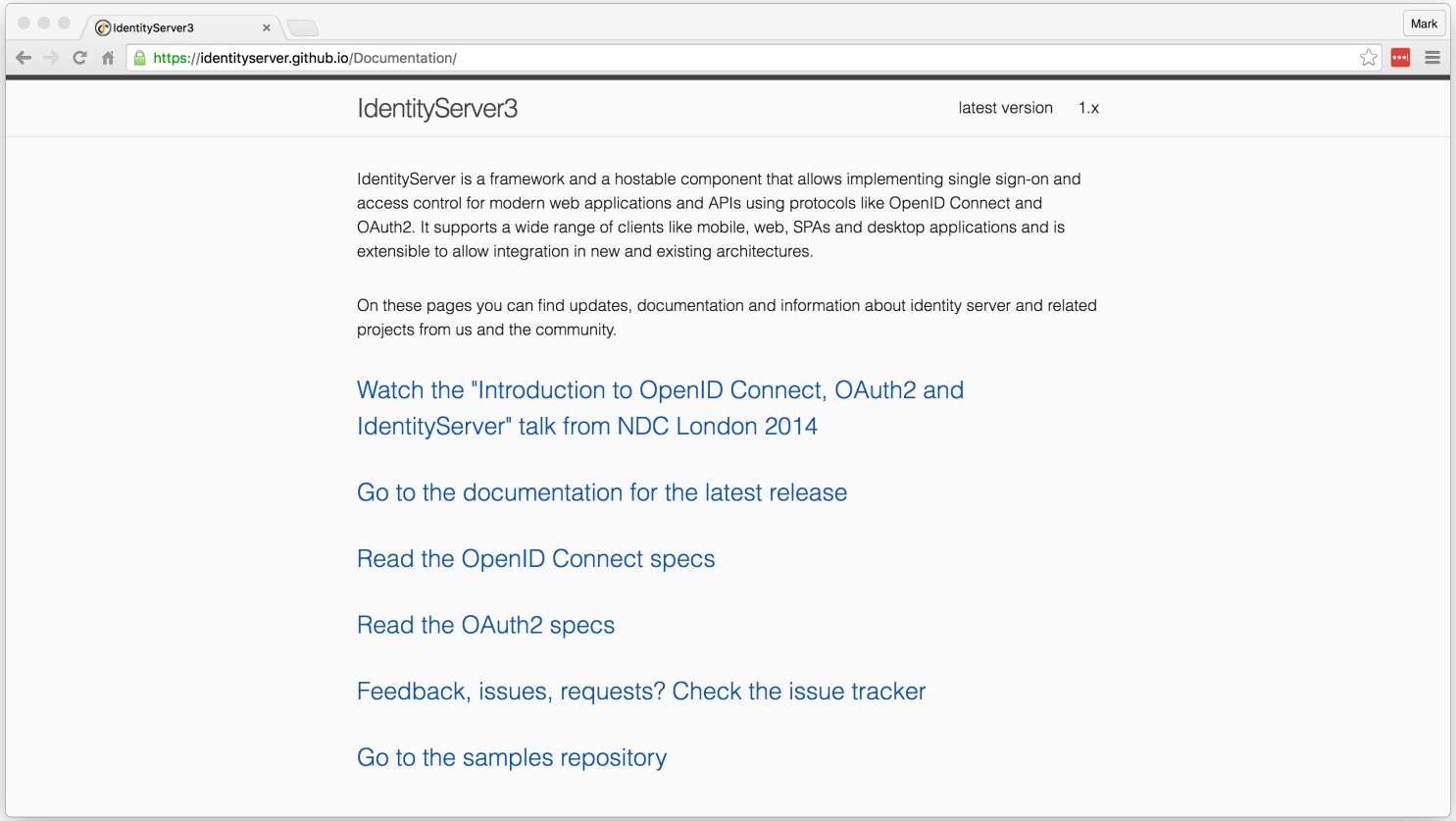
IdentityServer

Getting Started



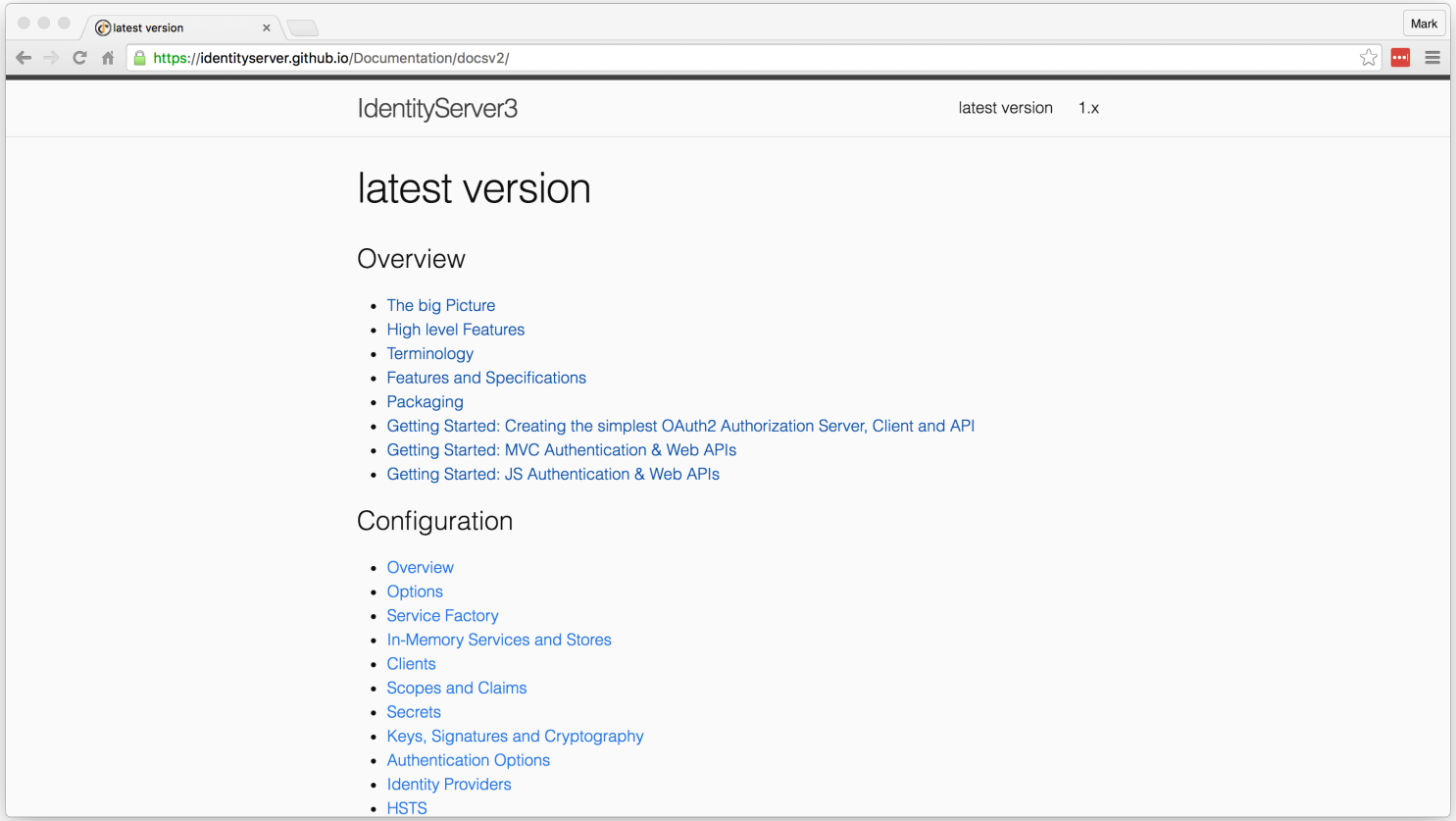
- https://github.com/IdentityServer

Getting Started



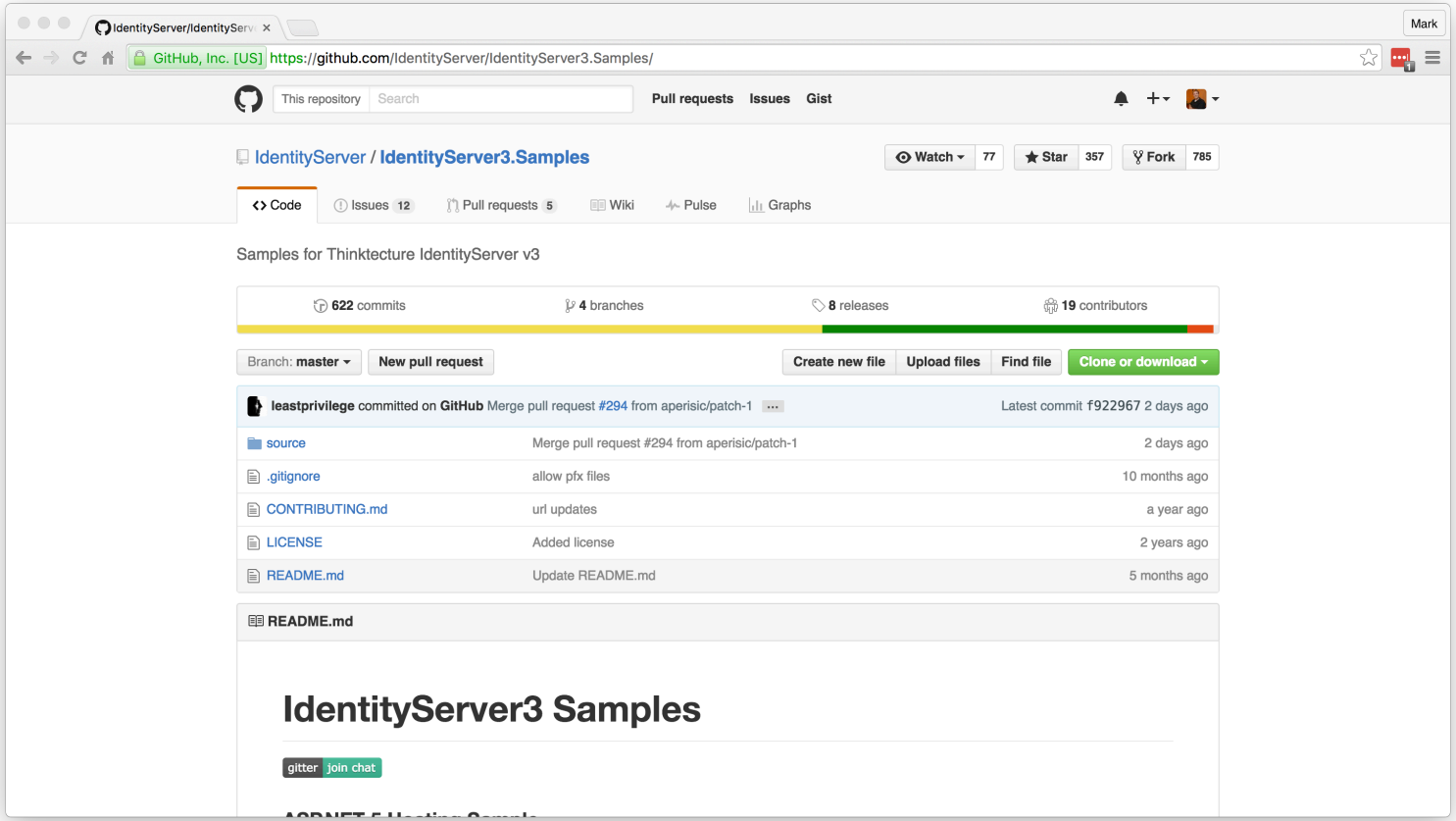
- https://identityserver.github.io/Documentation/

Getting Started



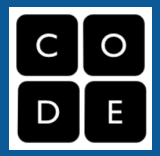
- https://identityserver.github.io/Documentation/docsv2/

Getting Started



- https://github.com/IdentityServer/IdentityServer3.Samples/

IdentityServer



DEMO

Resources

- OpenID Connect: http://openid.net/connect/
- OpenID Connect Libraries: http://openid.net/developers/libraries/

- IdentityServer: https://github.com/IdentityServer
- IdentityServer Samples: https://github.com/IdentityServer/IdentityServer3.Samples/

- OAuth for ASP.NET: http://www.oauthforaspnet.com/
- JSON Web Tokens: https://jwt.io/

Authentication Using OpenID Connect and OAuth2

Mark A. Wilson
Senior Developer
MarkW@LogicalAdvantage.com

www.DeveloperInfra.com
@DeveloperInfra