Security Simplified with IdentityServer4

http://aaronralls.com
@cajunAA

https://bit.ly/bsidesok-idsvr4

What will you learn today?

- Difference between Authentication & Authorization
- 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.
- When to use IdentityServer4

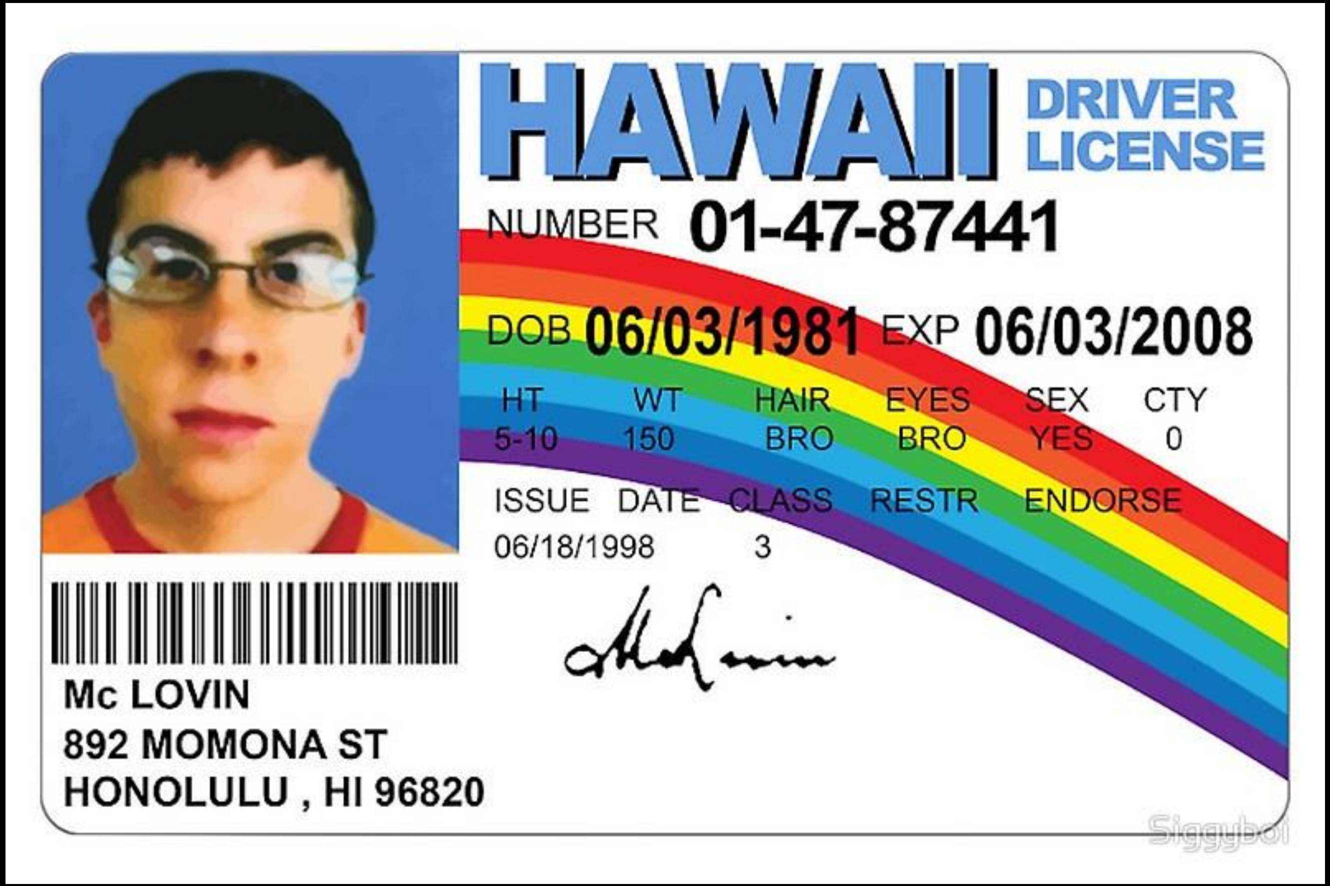
bit.ly/bsidesok-idsvr4

Authorization vs. Authentication

VISITOR

Debbie Moore 8/12

NAME DATE



HAWAII DRIVER LICENSE

NUMBER 01-47-87441

DOB 06/03/1981 EXP 06/03/2008

HT	WT	HAIR	EYES	SEX	CTY
5-10	150	BRO	BRO	YES	0

ISSUE DATE	CLASS	RESTR	ENDORSE
06/18/1998	3		

Mc LOVIN
892 MOMONA ST
HONOLULU , HI 96820

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

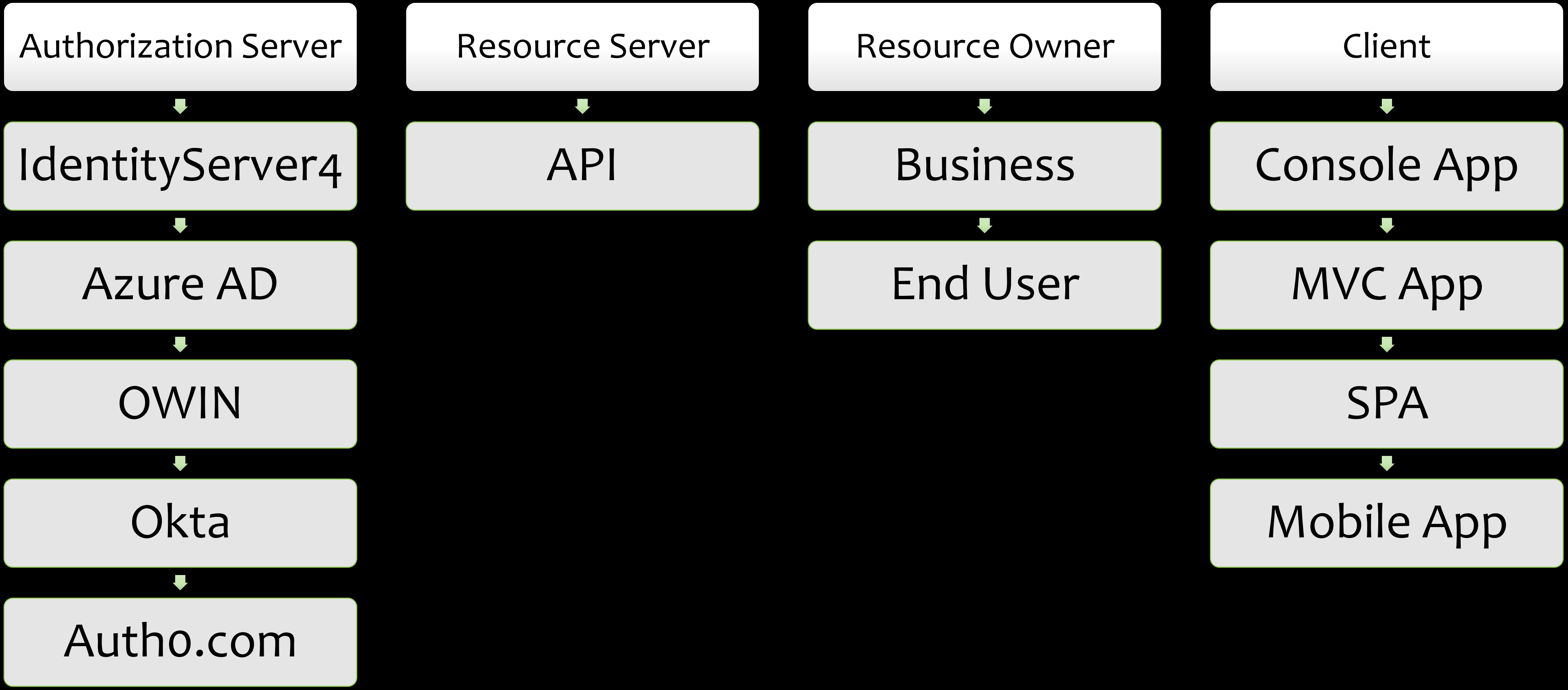
OpenID Connect Spec Links

OpenID Connect

- Core 1.0
- Discovery

bit.ly/bsidesok-idsvr4

OAuth 2.0 (Authorization)



Authorization Server

- IdentityServer4
- Azure AD
- OWIN
- Okta
- Autho.com

Resource Server

- API

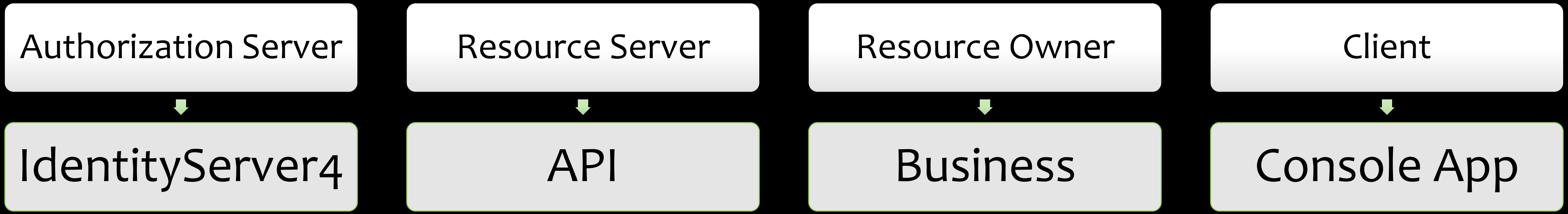
Resource Owner

- Business
- End User

Client

- Console App
- MVC App
- SPA
- Mobile App

OAuth 2.0 (Authorization)



Authorization Server → IdentityServer4

Resource Server → API

Resource Owner → Business

Client → Console App

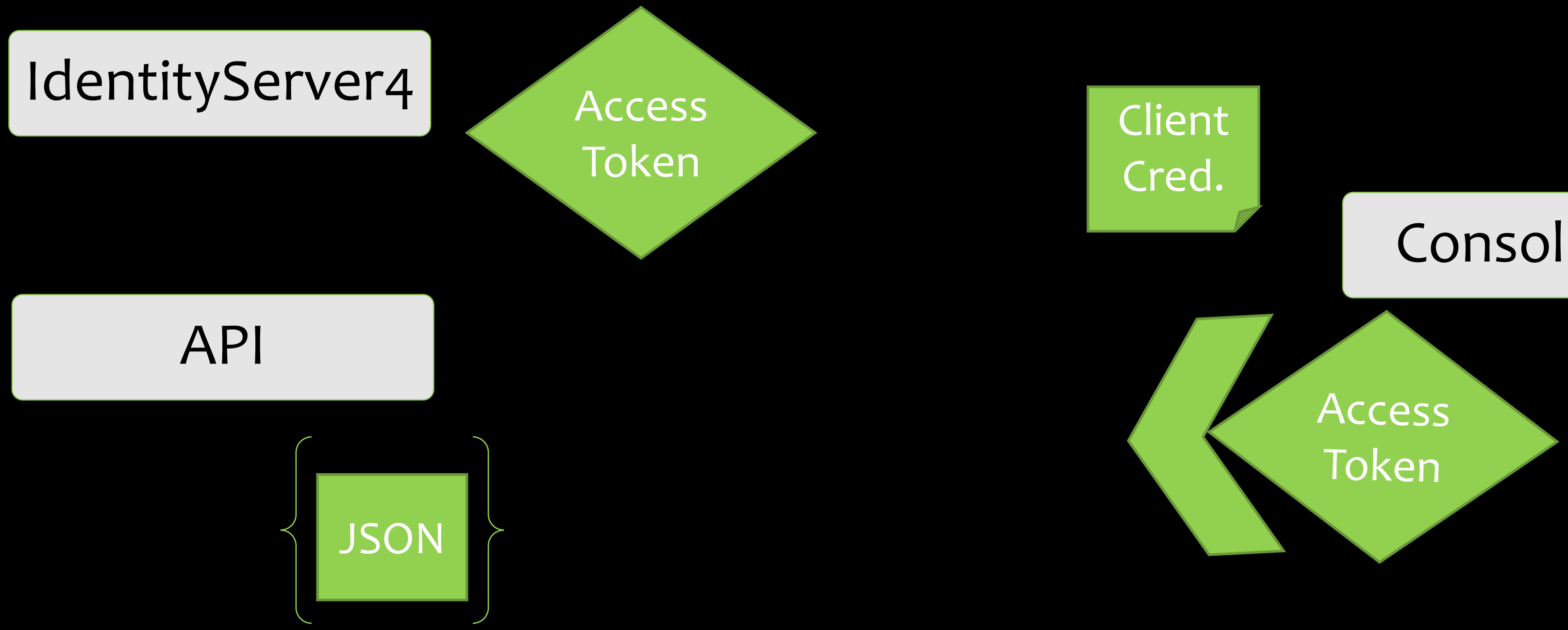
OAuth 2.0 Authorization Grant Type: Client Credentials

No user

Computer to Computer processes

bit.ly/bsidesok-idsvr4

OAuth 2.0 Authorization Grant Type: Client Credentials



OAuth 2.0 Authorization Grant Type: Code Flow

Front Channel
(Browser)

Back Channel
(Web Server to Auth Server)

OAuth 2.0 Implicit Flow

Front Channel
(Browser - SPA)

OAuth 2.0 Authorization Grant Types

Authorization Code
(with or without PKCE)

Implicit

Refresh token

OAuth 2.0 Authorization Grant Types cont..

Client Credentials

Resource Owner Password Credentials

OAuth 2.0 Access Tokens

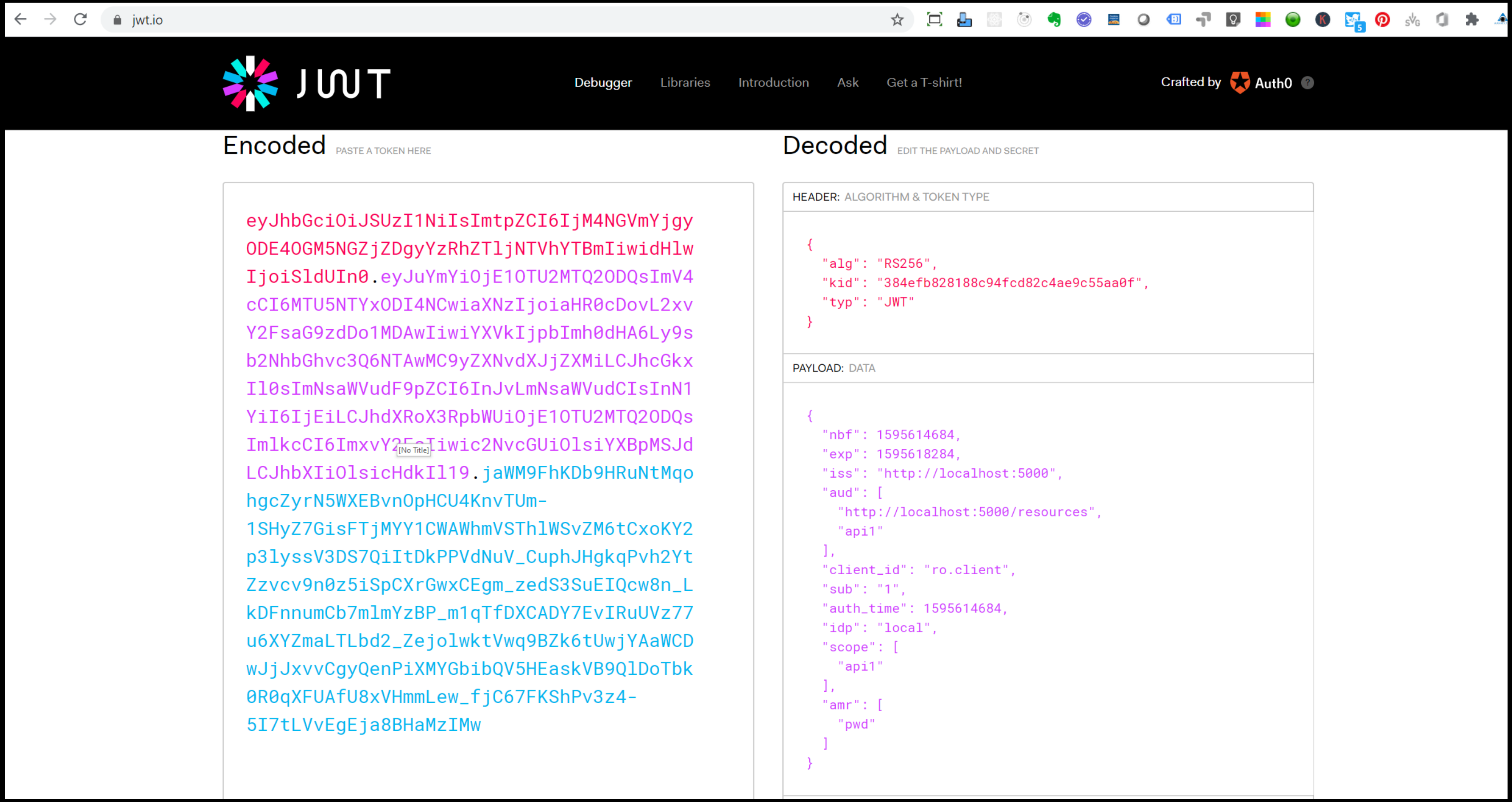
Reference

Self contained - JWTs

bit.ly/bsidesok-idsvr4

OAuth 2.0 Access Tokens

JWT.IO



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjM4NGVmYjgy
ODE4OGM5NGZjZDgyYzRhZTljNTVhYTBmIiwidHlw
IjoiSldUIn0.eyJuYmYiOjE1OTU2MTQ2ODQsImV4
cCI6MTU5NTYxODI4NCwiaXNzIjoiaHR0cDovL2xv
Y2FsaG9zdDo1MDAwIiwiYXVkIjpbImh0dHA6Ly9s
b2NhbGhvc3Q6NTAwMC9yZXNvdXJjZXMiLCJhcGkx
Il0sImNsaWVudF9pZCI6InJvLmNsaWVudCIsInN1
YiI6IjEiLCJhdXRoX3RpbWUiOjE1OTU2MTQ2ODQs
ImlkcCI6ImxvY2FsIiwic2NvcGUiOlsiYXBpMSJd
LCJhbXIiOlsicHdkIl19.jaWM9FhKDb9HRuNtMqo
hgcZyrN5WXEBvnOpHCU4KnvTUm-
1SHyZ7GisFTjMYY1CWAWhmVSThlWSvZM6tCxoKY2
p3lyssV3DS7QiItDkPPVdNuV_CuphJHgkqPvh2Yt
Zzvcv9n0z5iSpCXrGwxCEgm_zedS3SuEIQcw8n_L
kDFnnumCb7mlmYzBP_m1qTfDXCADY7EvIRuUVz77
u6XYZmaLTLbd2_ZejolwktVwq9BZk6tUwjYAaWCD
wJjJxvvCgyQenPiXMYGbibQV5HEaskVB9QlDoTbk
0R0qXFUAfU8xVHmmLew_fjC67FKShPv3z4-
5I7tLVvEgEja8BHaMzIMw
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "kid": "384efb828188c94fcd82c4ae9c55aa0f",
  "typ": "JWT"
}
```

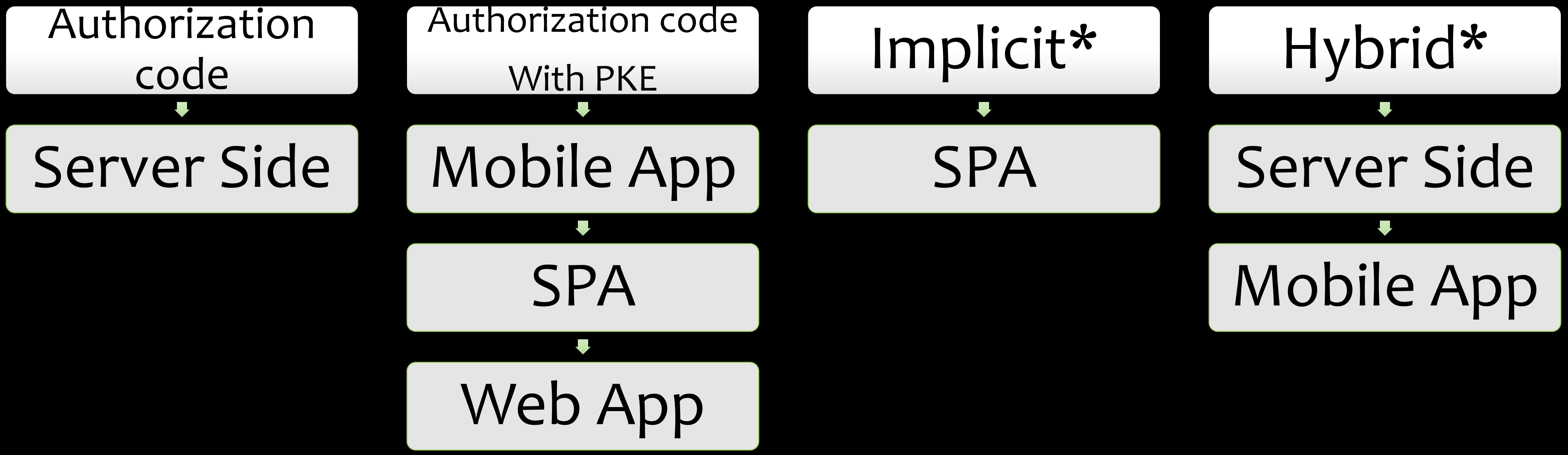
PAYLOAD: DATA

```
{
  "nbf": 1595614684,
  "exp": 1595618284,
  "iss": "http://localhost:5000",
  "aud": [
    "http://localhost:5000/resources",
    "api1"
  ],
  "client_id": "ro.client",
  "sub": "1",
  "auth_time": 1595614684,
  "idp": "local",
  "scope": [
    "api1"
  ],
  "amr": [
    "pwd"
  ]
}
```

DEMO 1

Client Credentials
Console App/Windows Service
accessing a secured API

OpenID Connect: Authentication Flows



Authorization code

Server Side

Authorization code With PKE

Mobile App

SPA

Web App

Implicit*

SPA

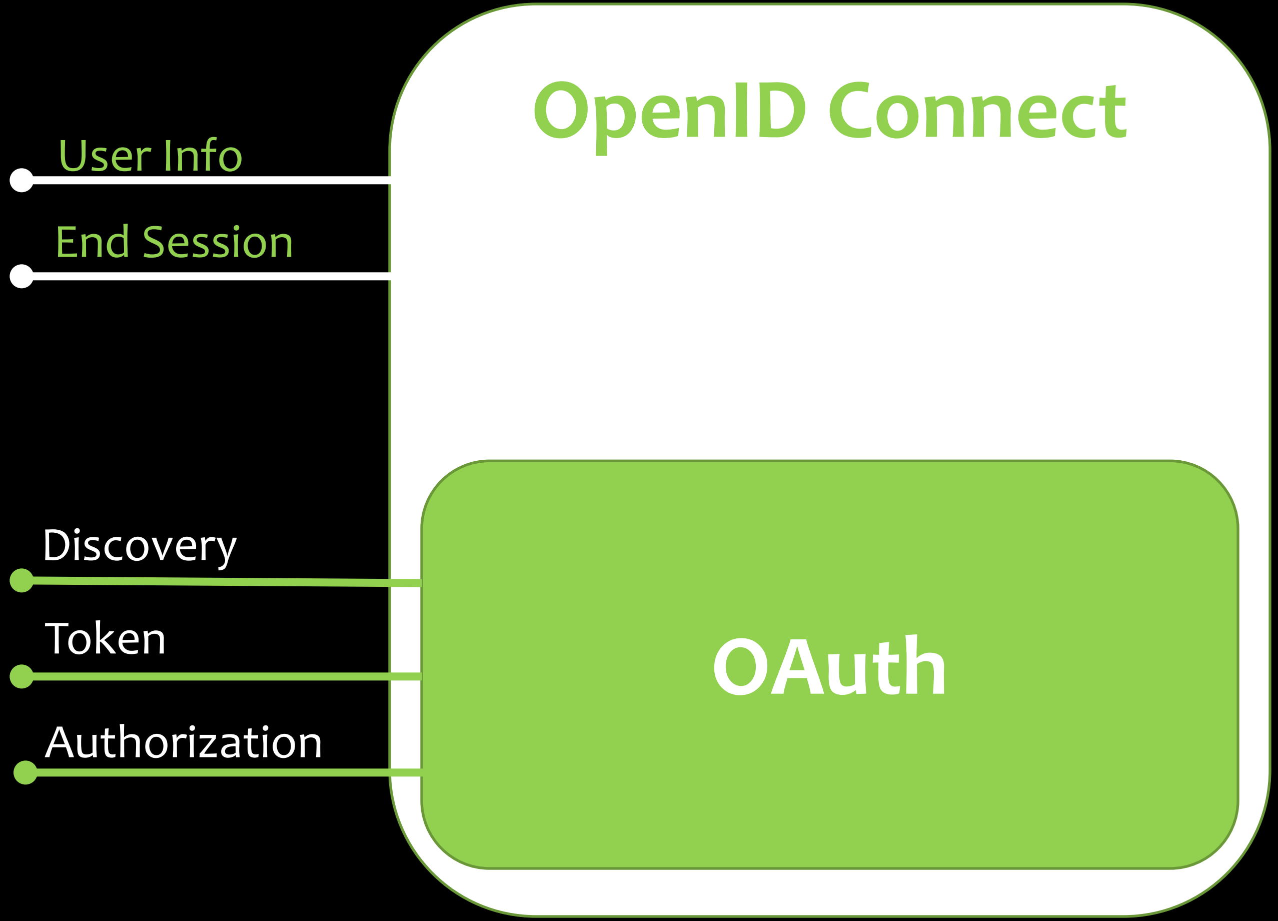
Hybrid*

Server Side

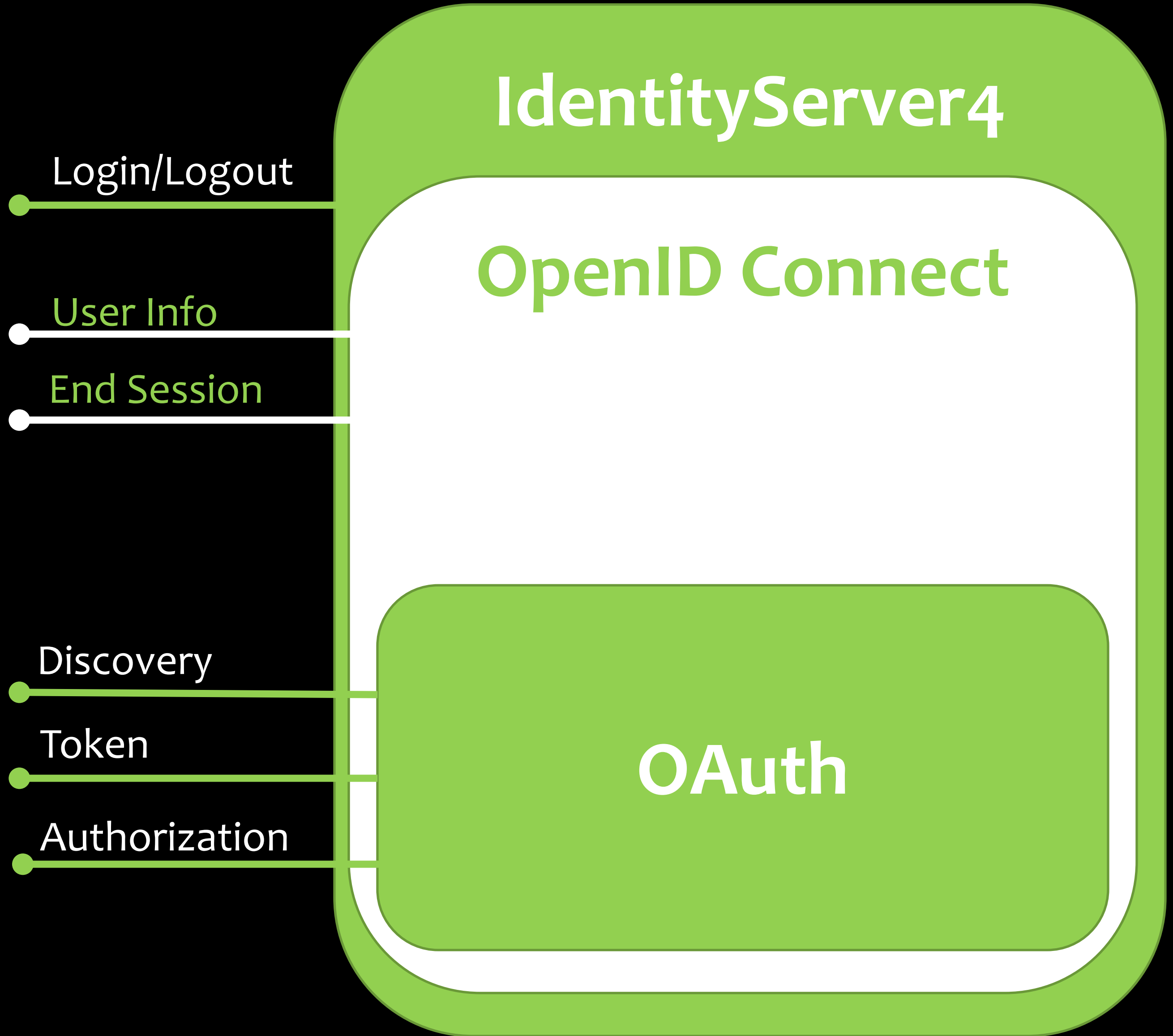
Mobile App

bit.ly/bsidesok-idsvr4

Authentication & Authorization



Authentication



DEMO 2

Application Authentication & Authorization
MVC Web and JavaScript Clients

When to use IdentityServer4

- Ok with using .NET Core & C# (IdentityServer4)
  - *Dotnet new -i IdentiyServer4.Templates*
- Your application has external users
- You want to quickly & easily implement OAuth 2.0 & OpenID Connect standards

When to use IdentityServer4

Security is like life insurance…

We should all have some, but how much is up to you.

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

IdentityServer4 Demo Server
https://demo.identityserver.io/

Q & A

Twitter :: @cajunAA
Instagram :: double_a_ralls
Stackoverflow :: aaronR
Blog :: https://arkeytek.com

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