

The logo is a circular emblem with a blue gradient. The outer ring contains the text 'O A U T H' at the top and 'H A U T H' at the bottom in a light blue, sans-serif font. The center of the logo features a large, stylized white number '2' set against a dark blue background with a white grid pattern.

Limitations of OAuth 2



Justin Richer
Internet Security Consultant
Bespoke Engineering

What's Wrong with OAuth2?

RFC6749

RFC6750

An aerial photograph of a two-lane asphalt road. A bright yellow line is painted on the road, starting from the bottom left and curving in a wavy pattern towards the top center. The road is flanked by green grass and some trees. In the background, a few houses and a red building are visible.

YOU HAD ONE JOB

Actual Application Code

FAPI

CIBA

JWT BCP

PoP

TokBind

UMA 2

DPoP

PRO

SPA BCP

HTTP Signing

Security BCP

RFC7636

RFC8414

PAR

RFC7515
RFC7516

RFC7517
RFC7518

RFC8252

RFC7662

Token Exchange

RFC7519

JARM

RFC7592

RFC7591

JAR

PAR

MTLS

Redirect URI Matching

TLS

OIDC

RFC7009

State parameter

RFC6819

CSRF

RFC8628

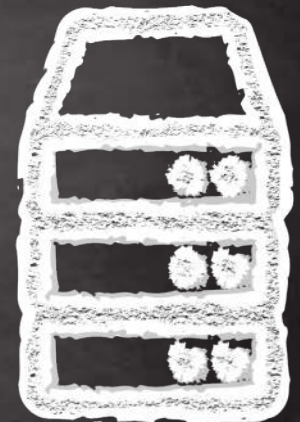
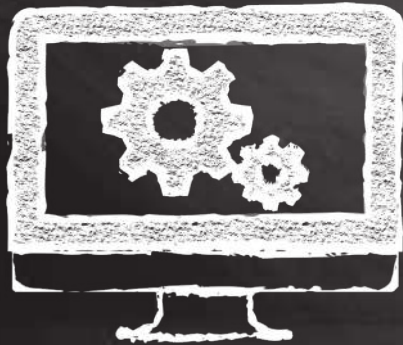
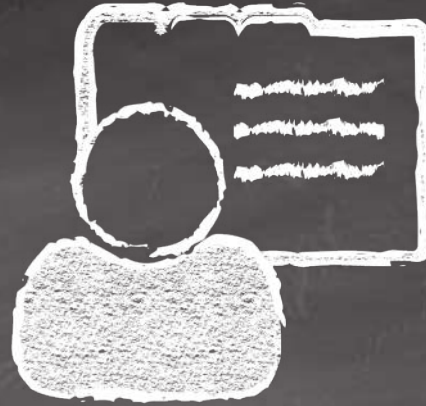
Grant type
Auth method
Client type
RFC6749

Header / param
RFC6750

The Front Channel



- User is present
- Browser is flexible



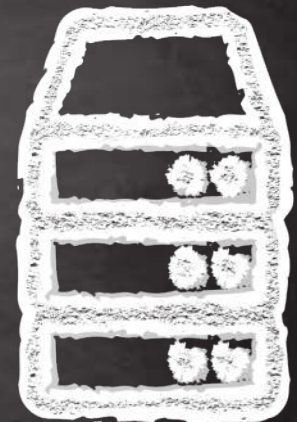
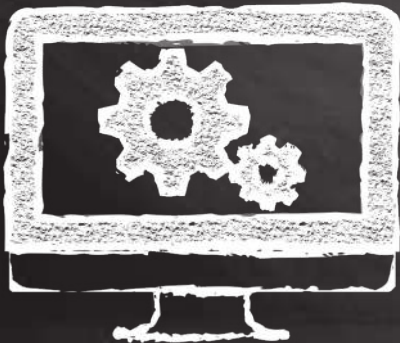
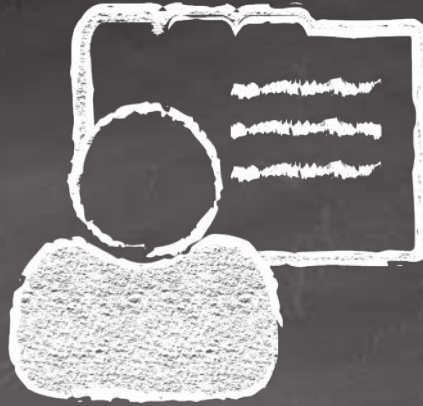
The Front Channel



- User is present
- Browser is flexible

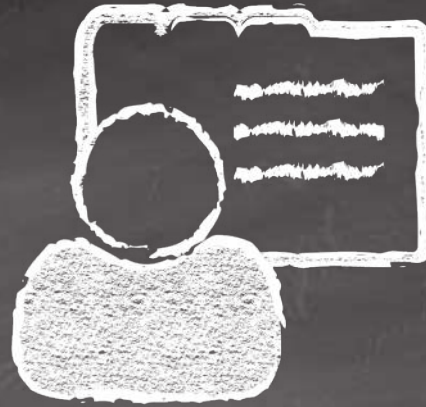


- Information leakage
- Tampering
- Injection
- URL size limitations
- HTTP Referrer headers
- HTTP server logs

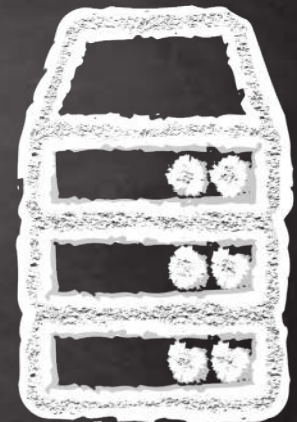
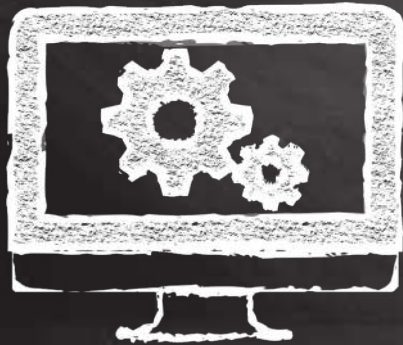


The Front Channel

- User authentication
- User interaction
- Client identifier
- Requested scope
- Application state
- etc...

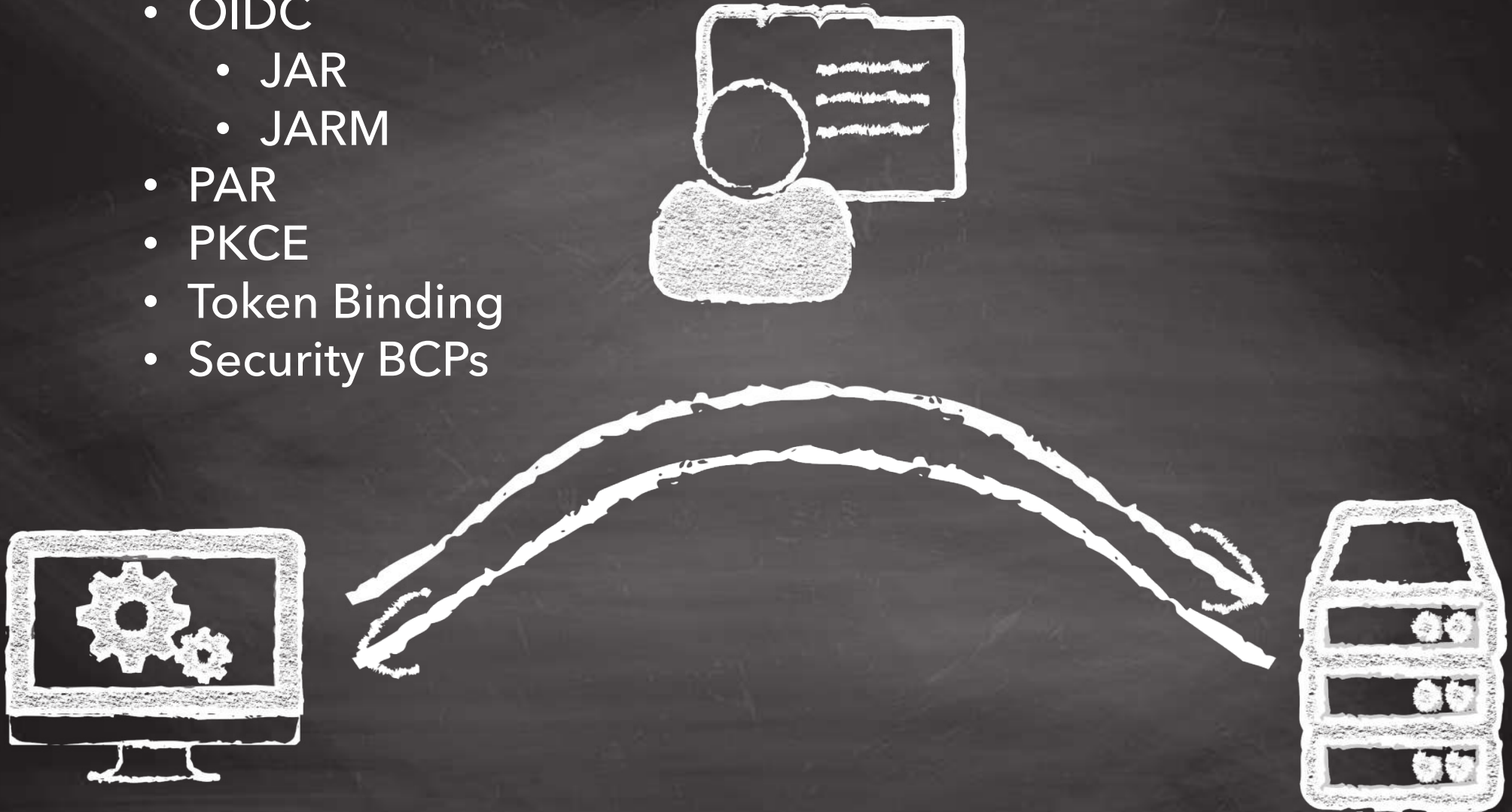


- Authorization code
- Access tokens
- Identity assertions
- Application state
- etc.



Trying to protect the front channel

- OIDC
 - JAR
 - JARM
- PAR
- PKCE
- Token Binding
- Security BCPs





Implicit
flow

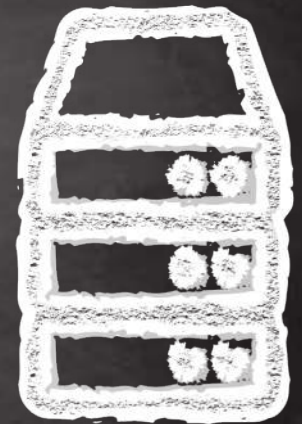
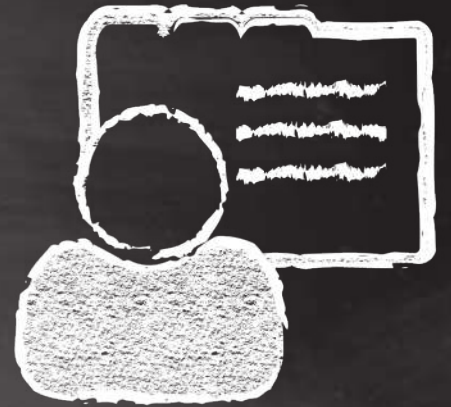
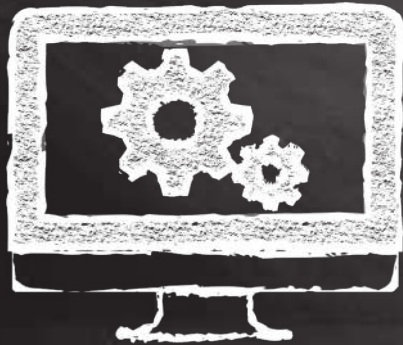
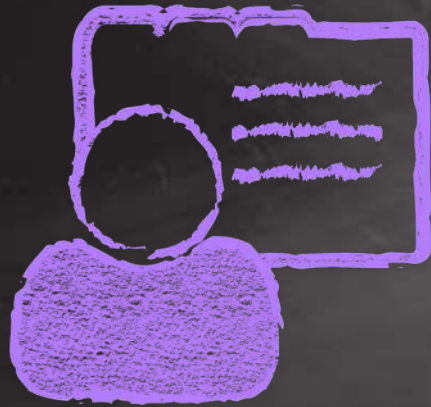
Developers

Is this security?

OAuth's single Resource Owner



UMA Requesting Party



Registration and Discovery

- OAuth assumes a static world
 - Client needs to be registered with a client ID
 - AS has several different endpoints
- Dynamic registration helps but a bad match for many auth servers
 - Overhead for ephemeral clients

Token Presentation

A photograph of a person's legs from the knees down, wearing a bright blue t-shirt and purple shorts. The person is sitting on a light blue surface. A large white text overlay is centered on the image, reading "Token Binding?".

Token Binding?

Scopes

What does a scope mean?

- The kind of thing that I want (email, profile)
- Functionality switching (openid, offline_access)
- Where is it (resource server name)
- When do I want it (online_access)
- The specific thing I want (account:12345)

But wait, there's more!

- "resource" indicator
- "aud" parameter (PoP token key restriction)
- "claims" from OIDC
- Rich Authorization Requests

