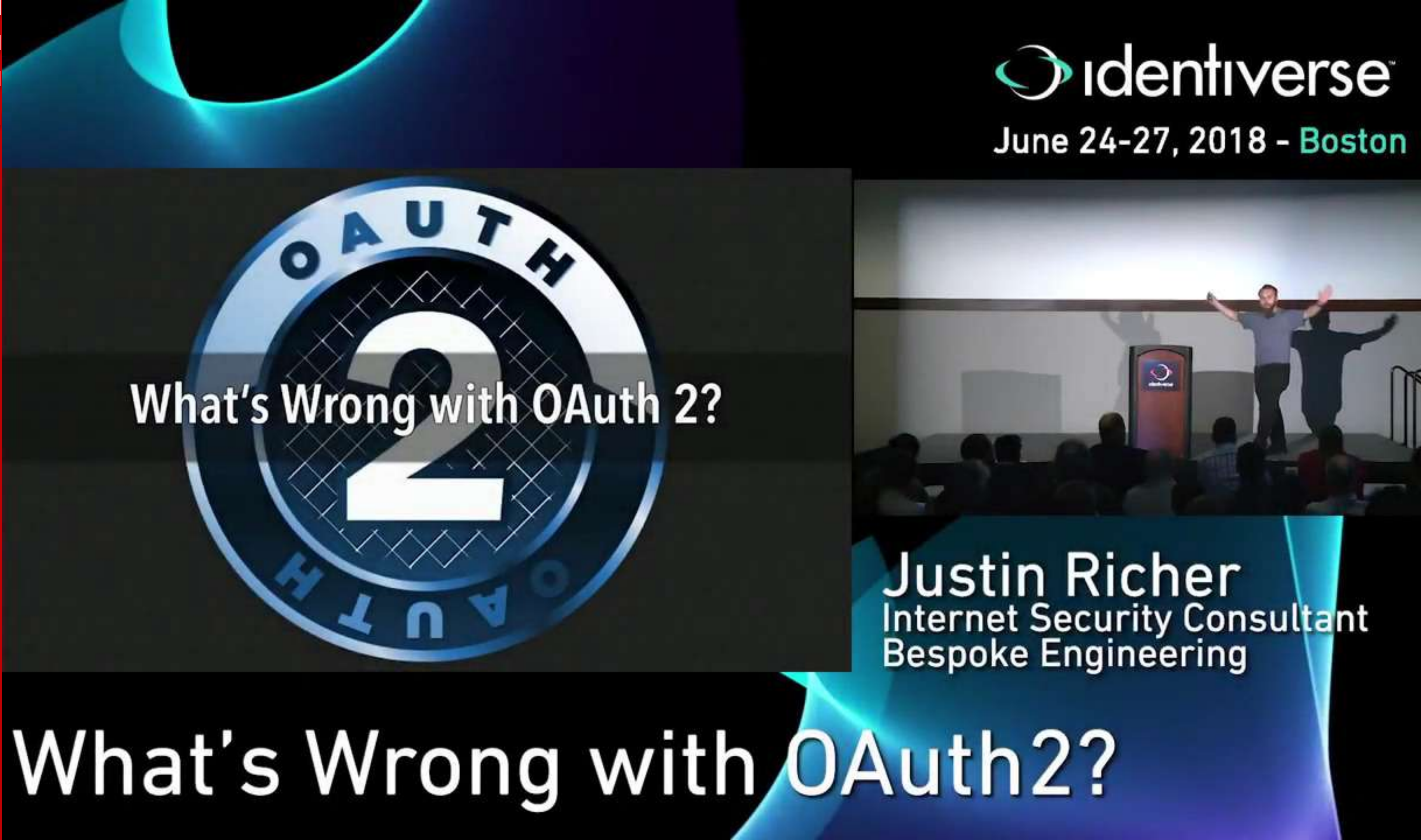
Limitations of OAuth 2

@justin__richer

https://bspk.io/



identiverse

June 24-27, 2018 - Boston

What's Wrong with OAuth 2?

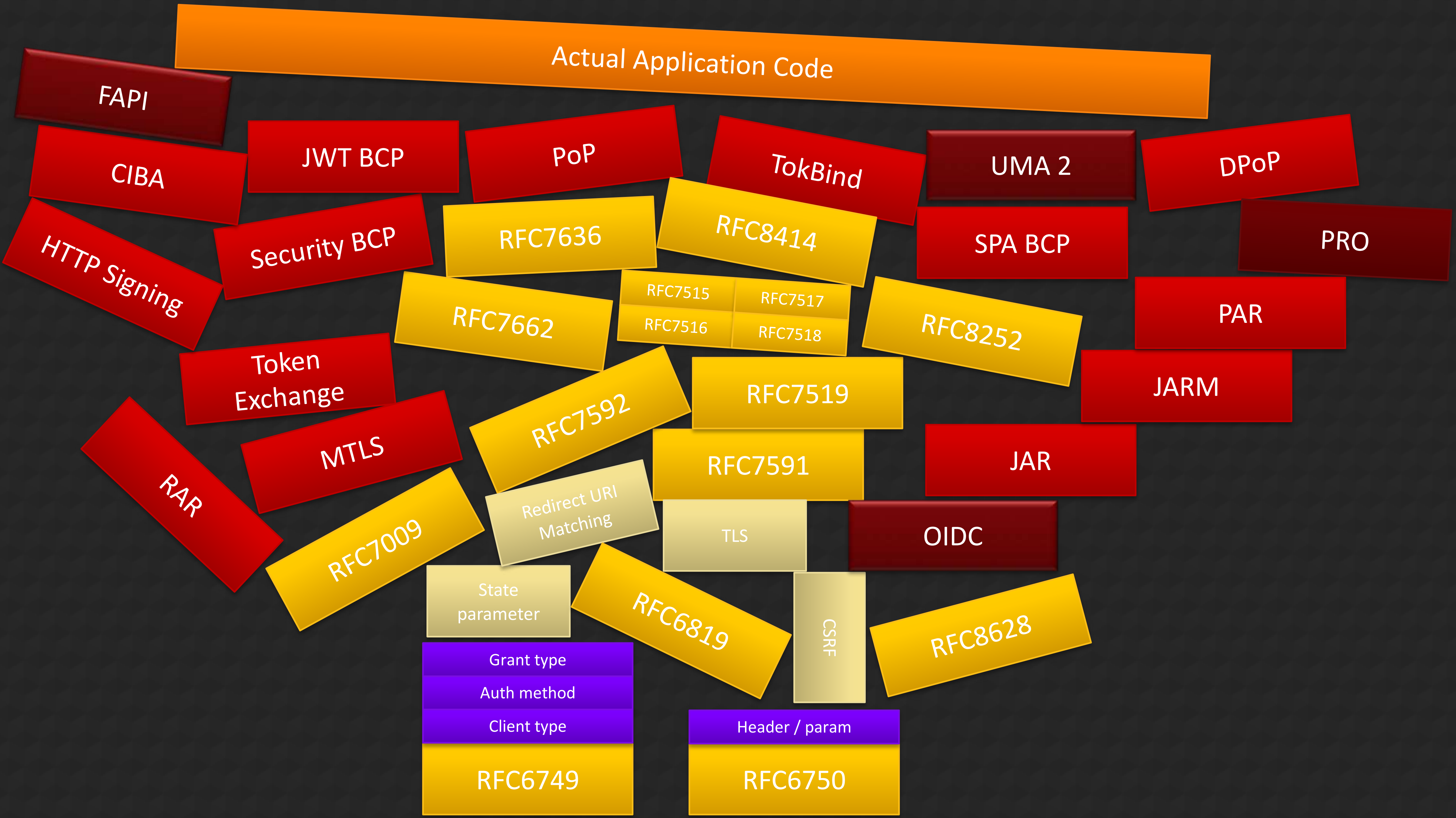
Justin Richer
Internet Security Consultant
Bespoke Engineering

What's Wrong with OAuth2?

RFC6749

RFC6750

YOU HAD ONE JOB



Actual Application Code

FAPI

CIBA

JWT BCP

PoP

TokBind

UMA 2

DPoP

HTTP Signing

Security BCP

RFC7636

RFC8414

SPA BCP

PRO

RFC7515

RFC7517

RFC7516

RFC7518

RFC7662

RFC8252

PAR

Token Exchange

RFC7519

JARM

RFC7592

MTLS

RAR

RFC7591

JAR

Redirect URI Matching

TLS

OIDC

RFC7009

State parameter

RFC6819

CSRF

RFC8628

Grant type

Auth method

Client type

Header / param

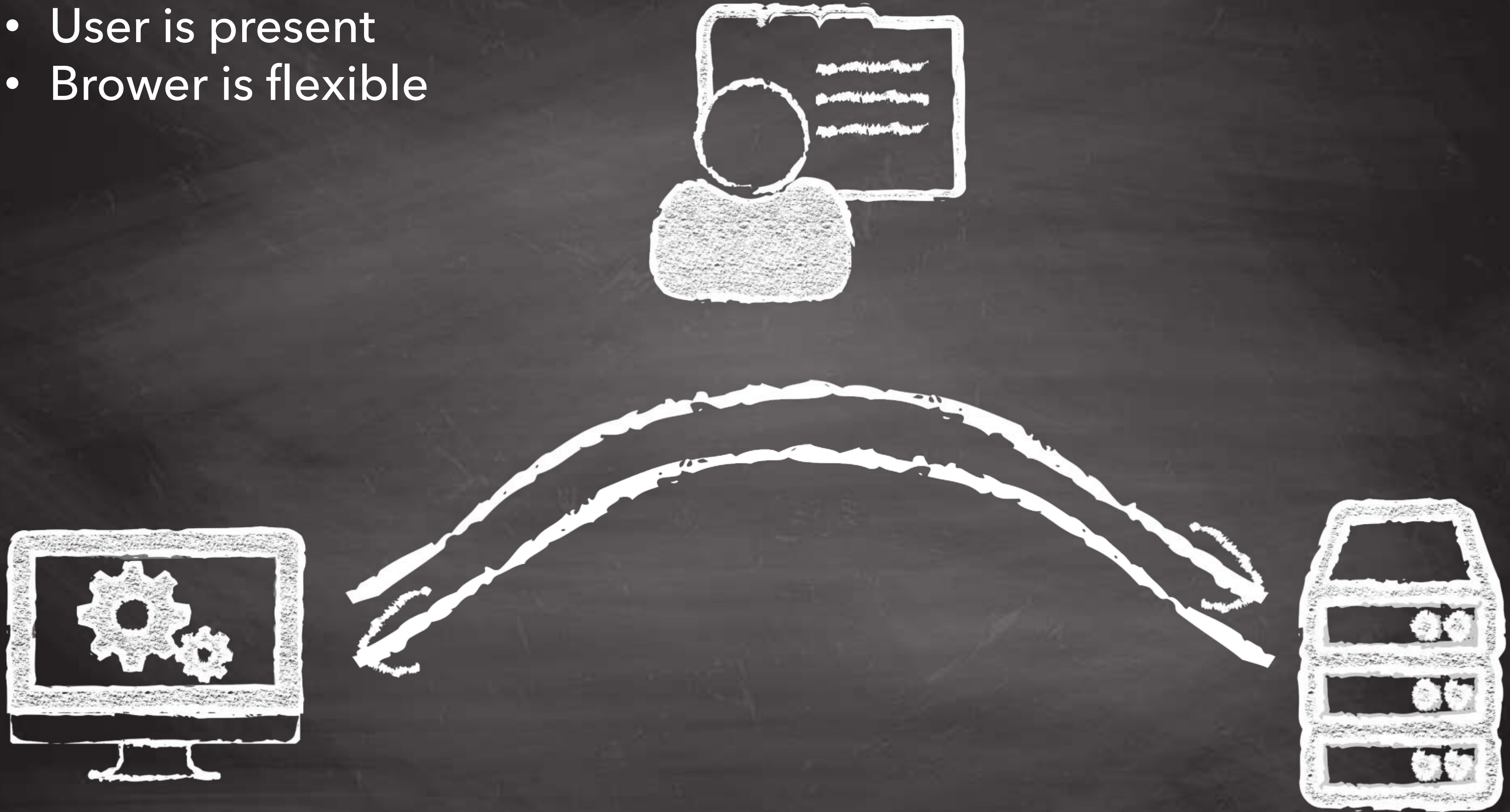
RFC6749

RFC6750

The Front Channel

☑

- User is present
- Brower is flexible



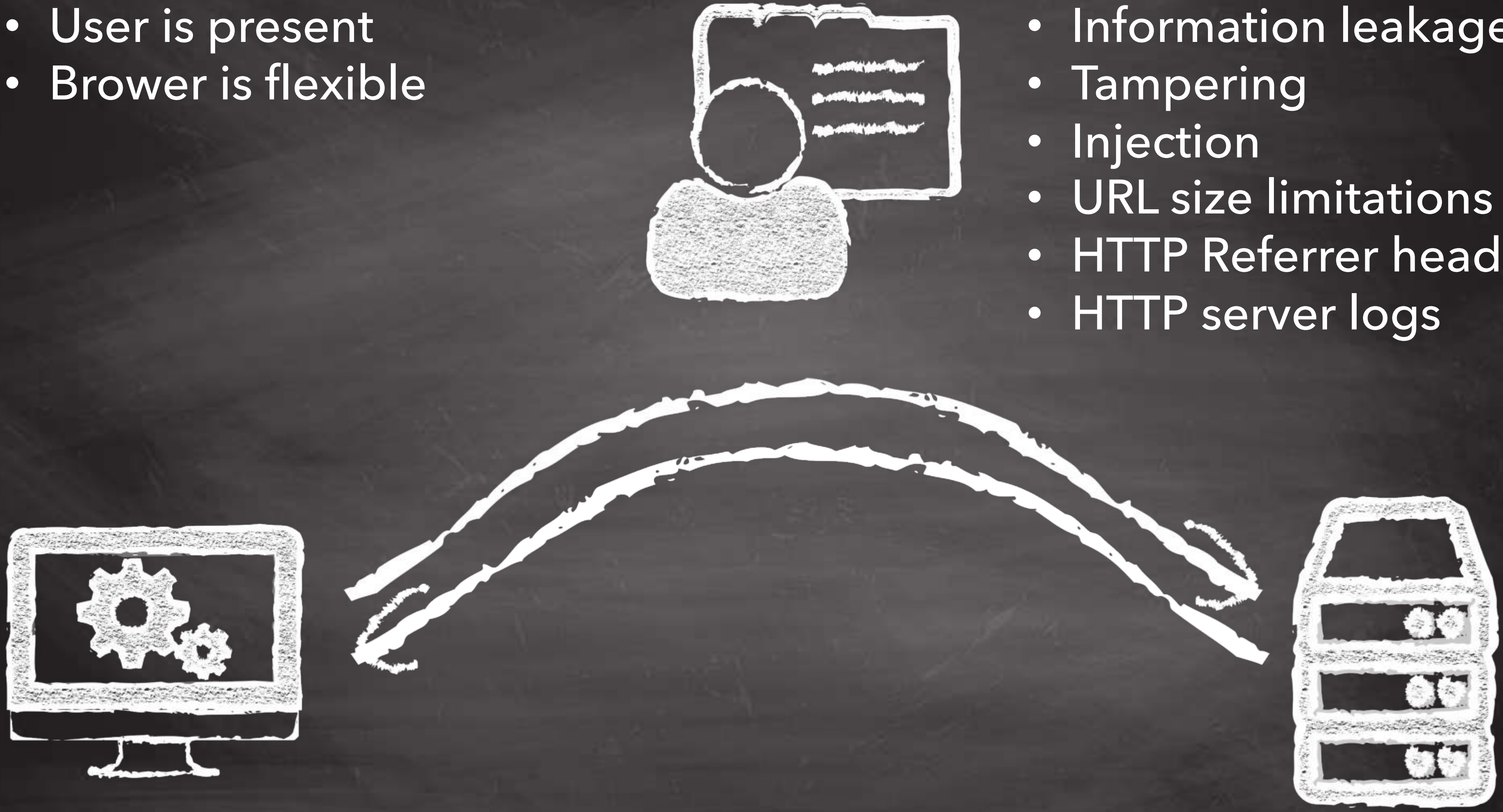
The Front Channel

☑

- User is present
- Brower is flexible

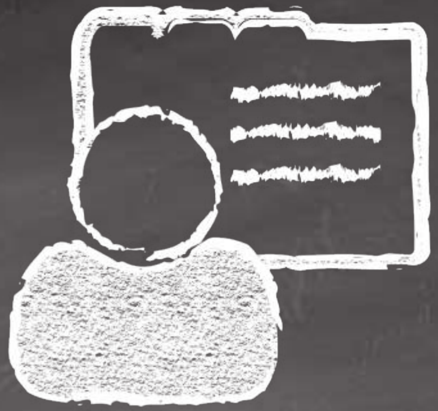
☒

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

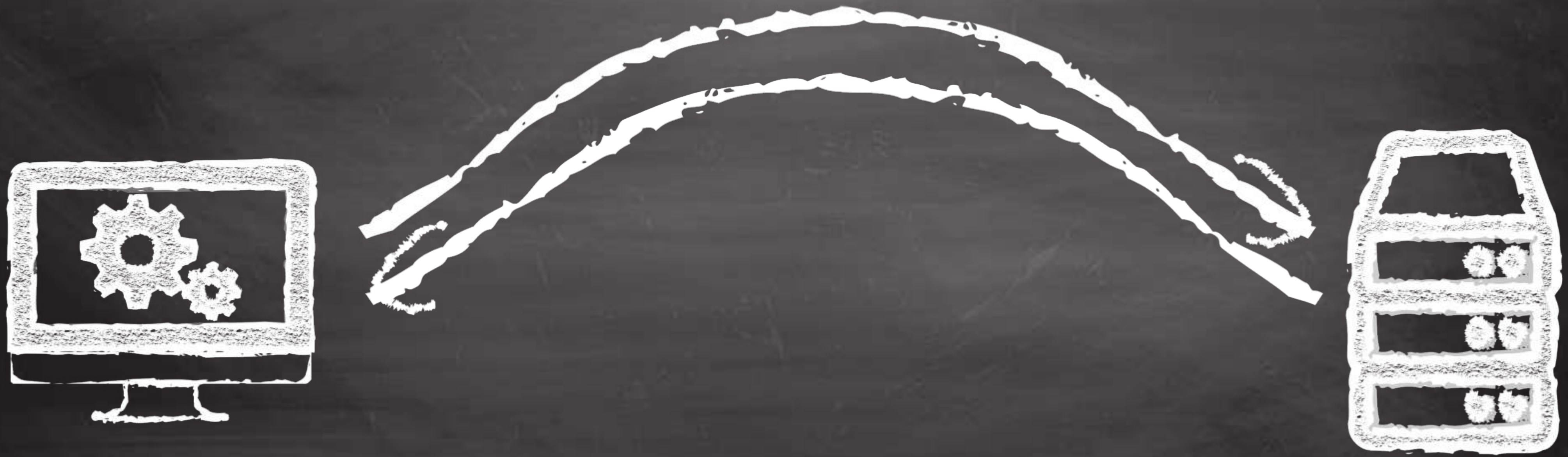


The Front Channel

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

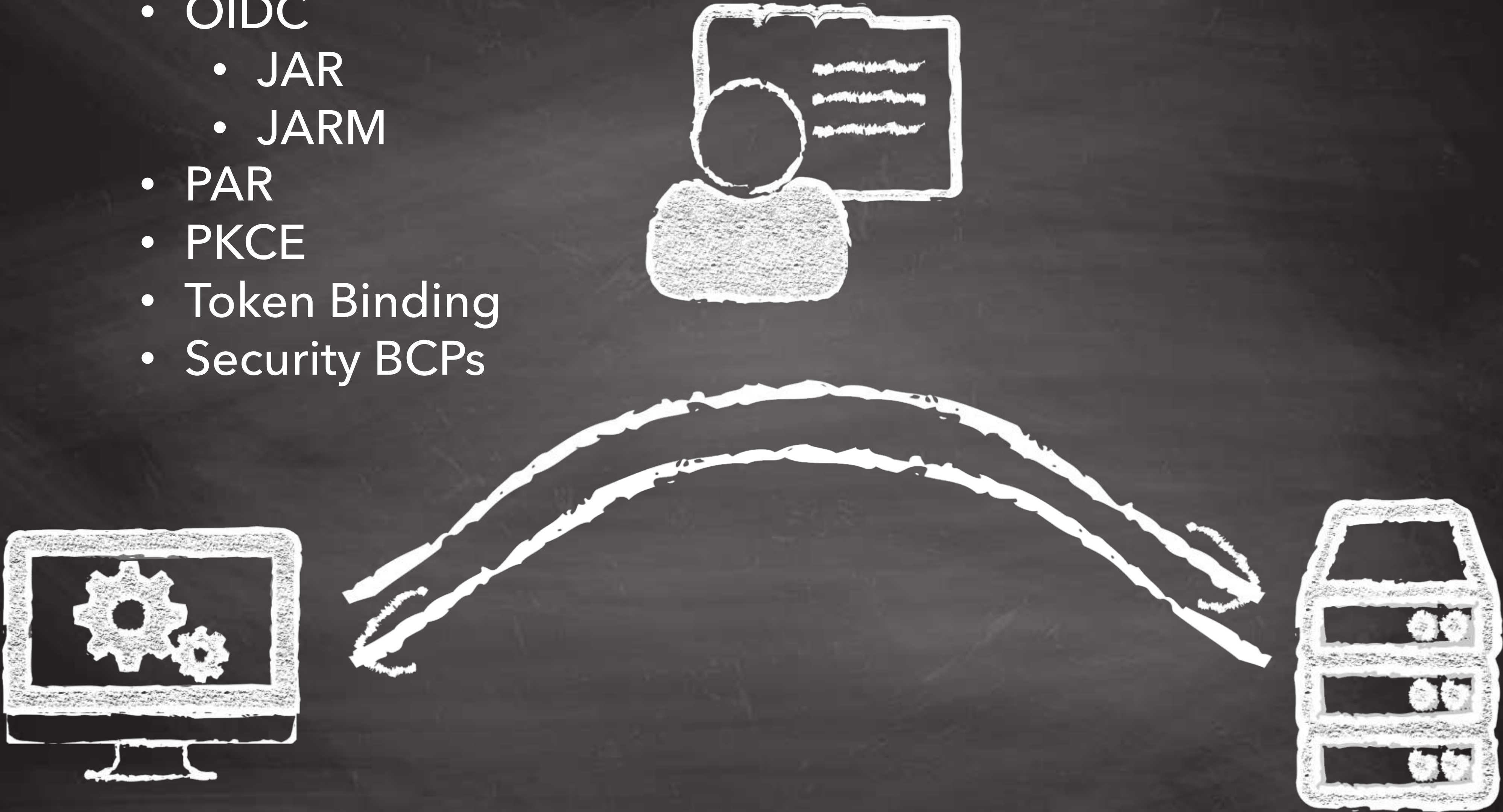


- Authorization code
- Access tokens
- Identity assertions
- Application state
- etc.



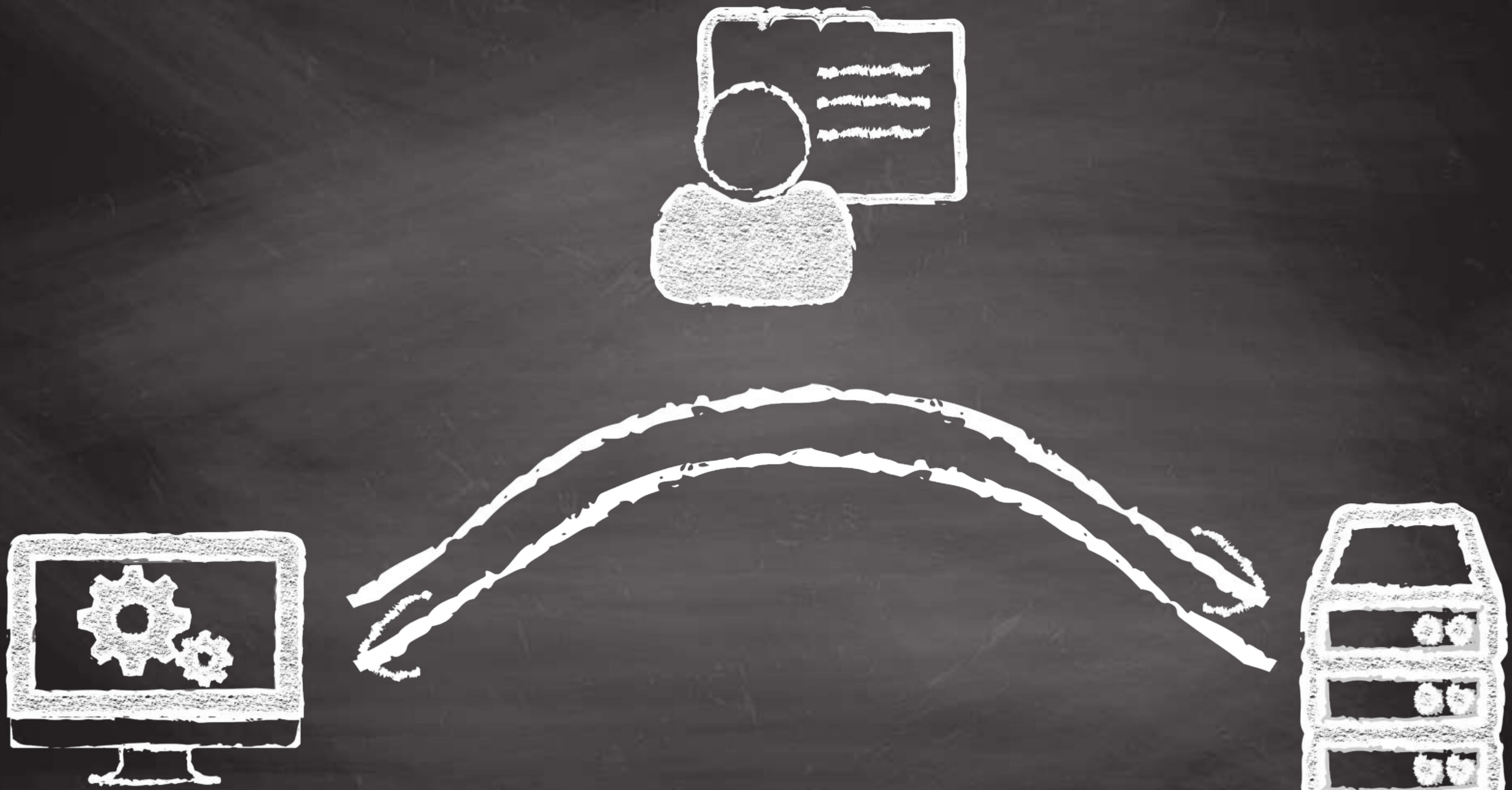
Trying to protect the front channel

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

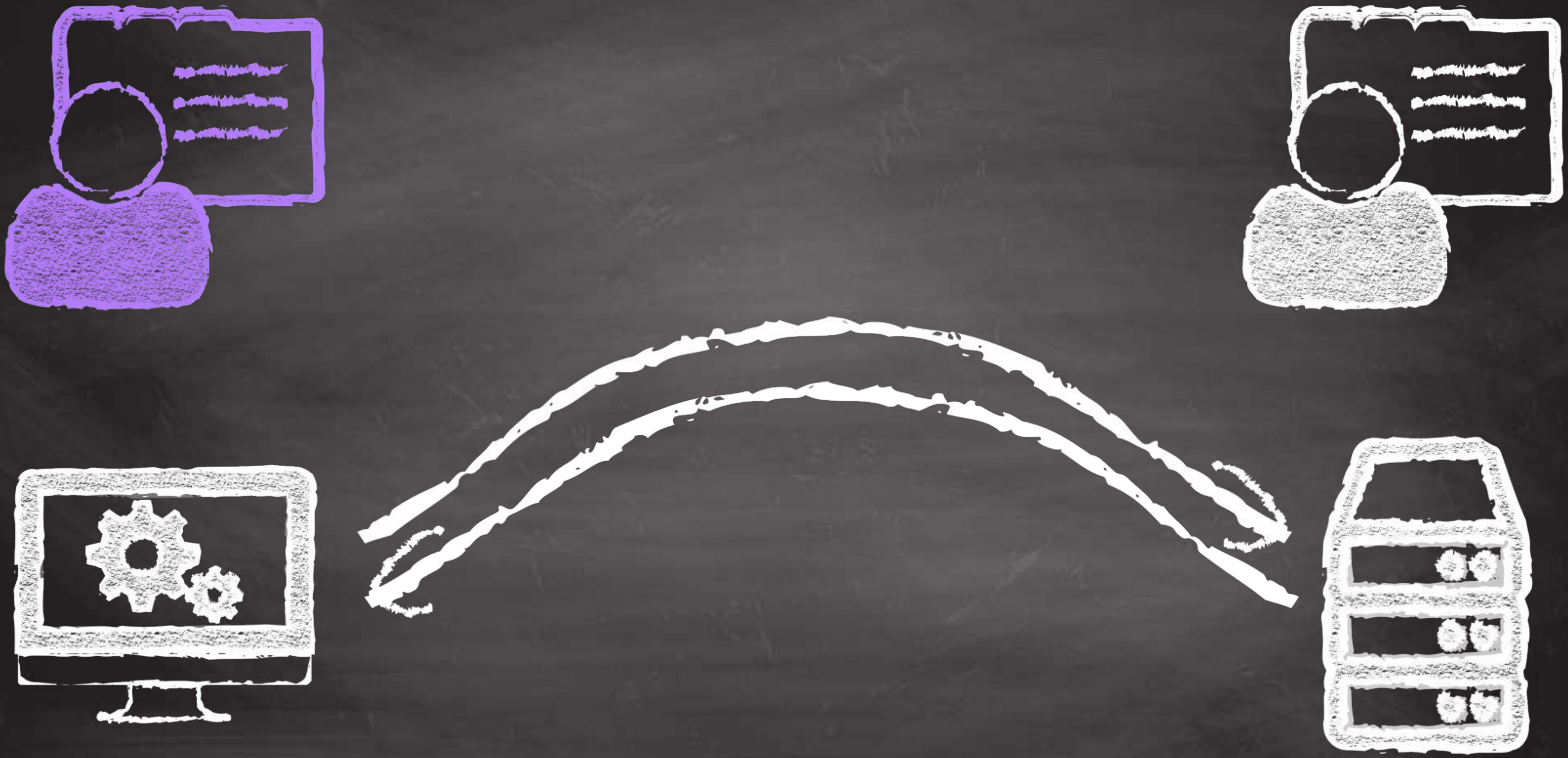


Implicit flow
Developers
Is this security?
百科事典

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

Token Binding?

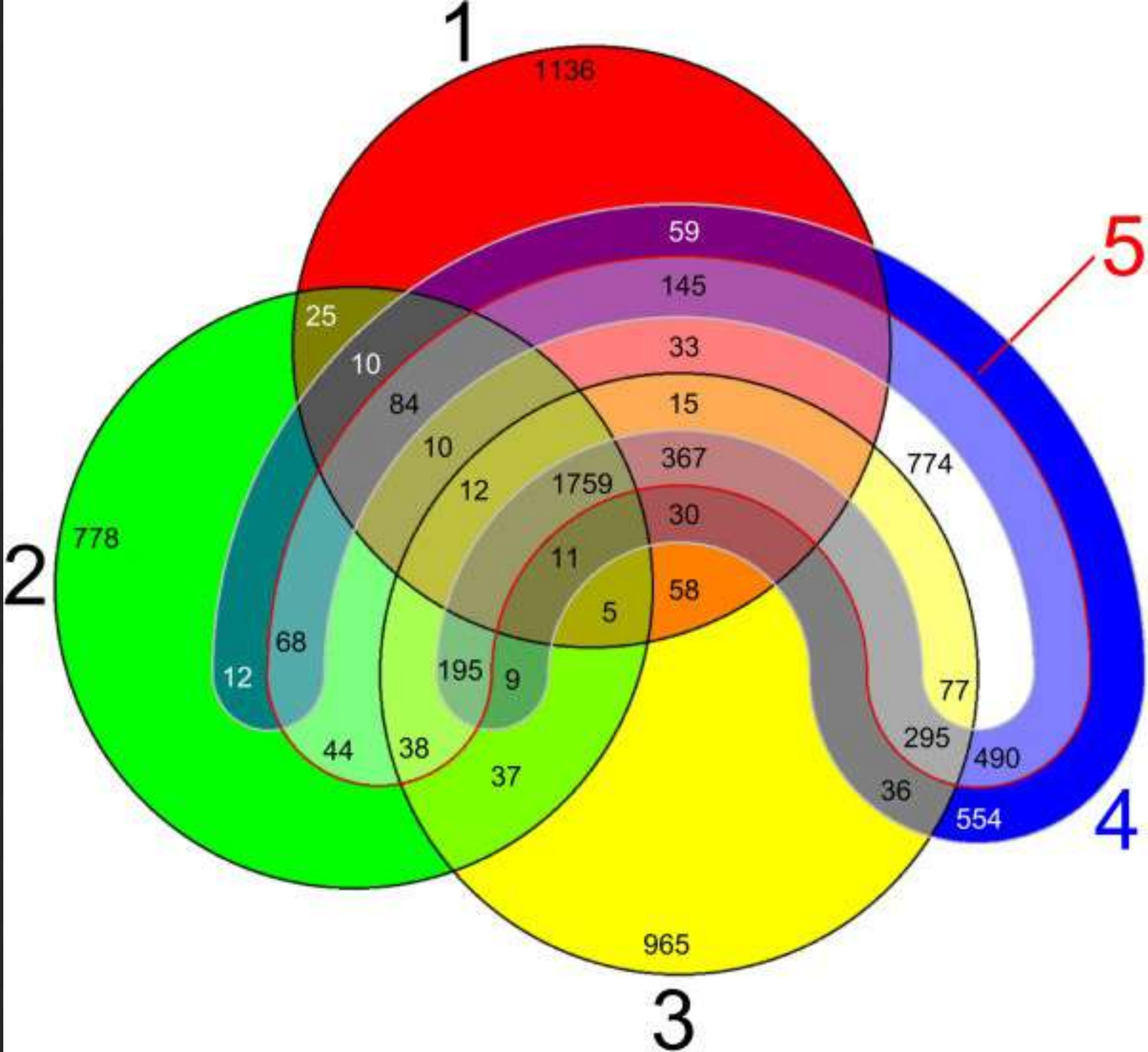
Scopes

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


1
2
3
4
5
1136
59
145
33
15
367
30
58
25
10
84
10
12
1759
11
5
774
778
68
12
195
9
77
295
490
44
38
37
36
554
965