<DevSum>

Level Up Your Security: OpenID Connect/OAuth Update

Roland Guijt

Agenda

OAuth 2.1 changes

- PKCE
- BFF

PAR

DPoP

(Private Key JWT)

Assumed Knowledge

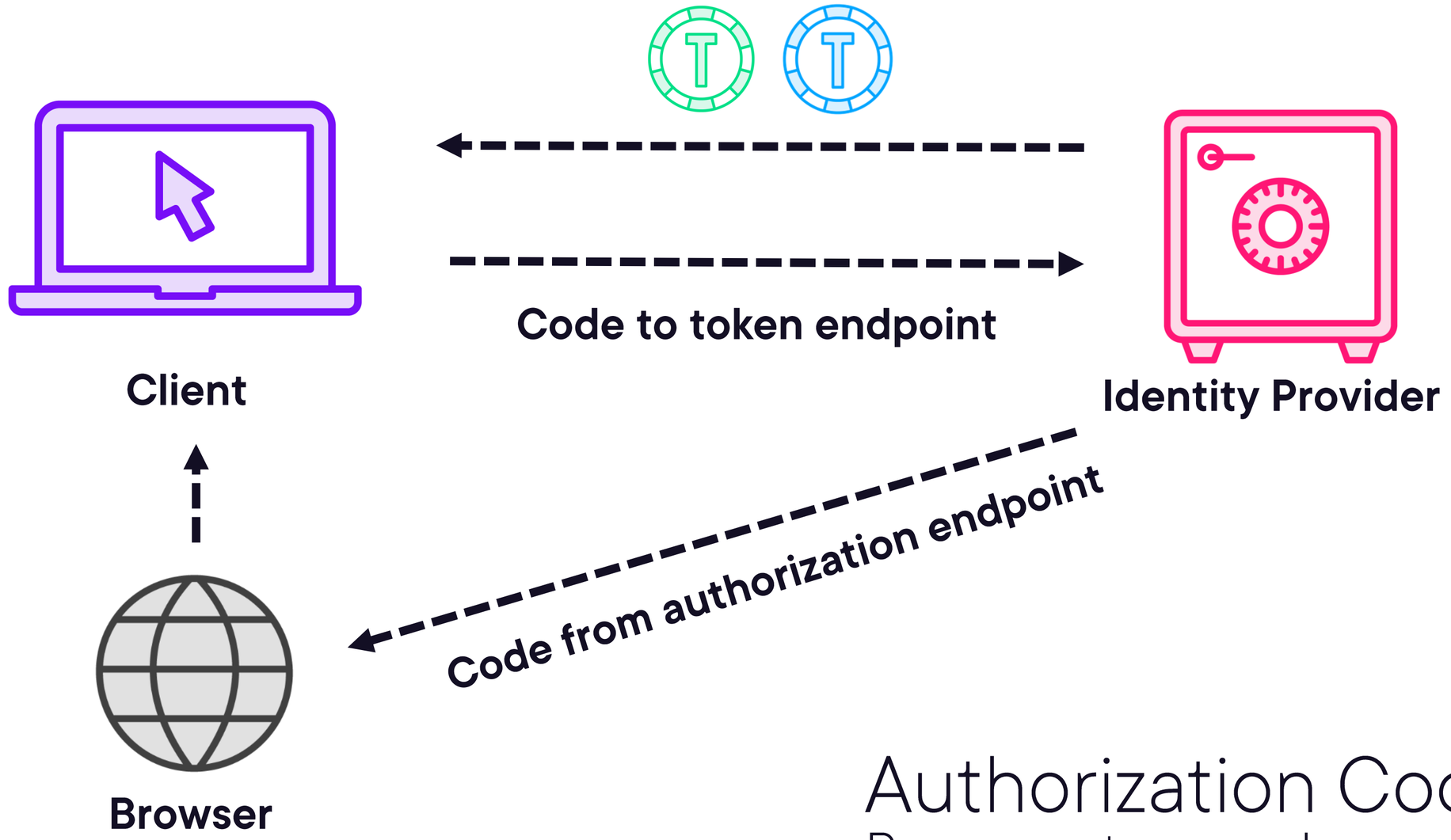
OpenID Connect/OAuth

OAuth 2.1 Main Changes So Far

PKCE (Proof Key for Code Exchange) required for authorization code flow

Implicit and resource owner password grant omitted

Refresh tokens for public clients must either be sender-constrained or for one-time use



Authorization Code

Response type: code
Scope: openid

Authorization Code Flow Problems

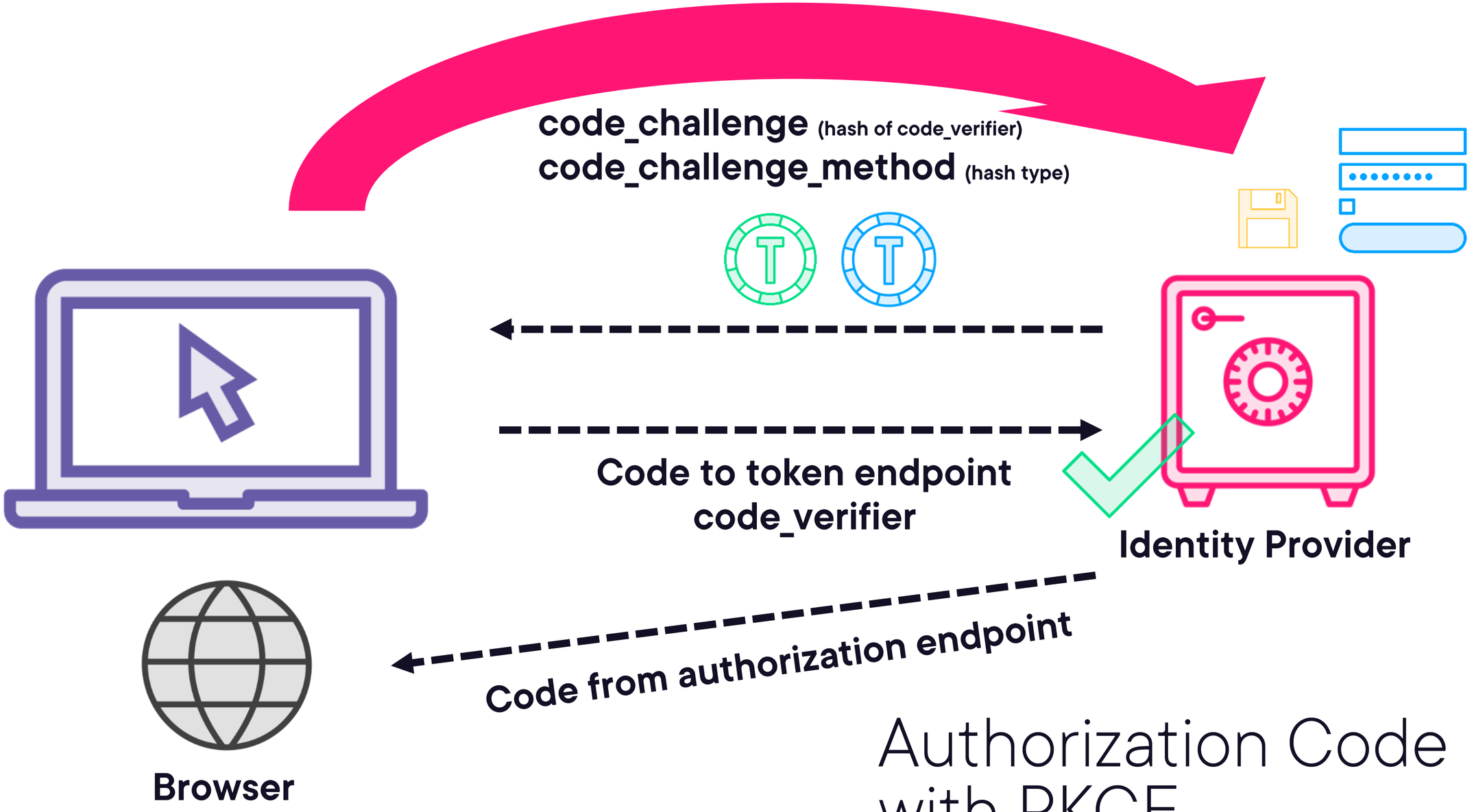
Authorization Code Interception Attack

Malicious apps can register a URL scheme matching the code target

Attacker could gain access to logs

Public clients are extra vulnerable (no client secret)

Solution: bind code to client



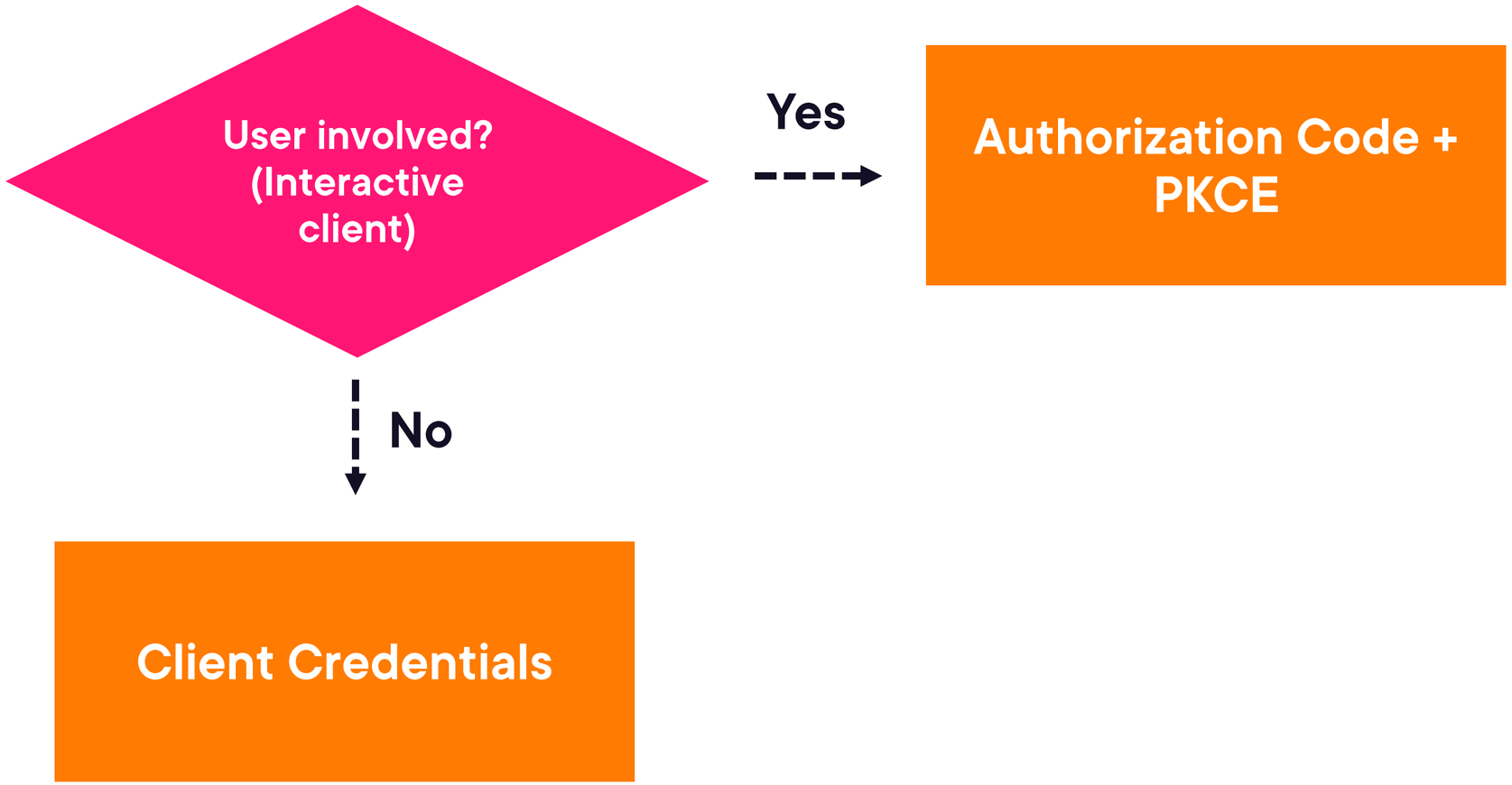
Authorization Code with PKCE

Response type: code
Scope: openid

Demo

PKCE

Which Flow?


User involved? (Interactive client)
Yes
Authorization Code + PKCE
No
Client Credentials

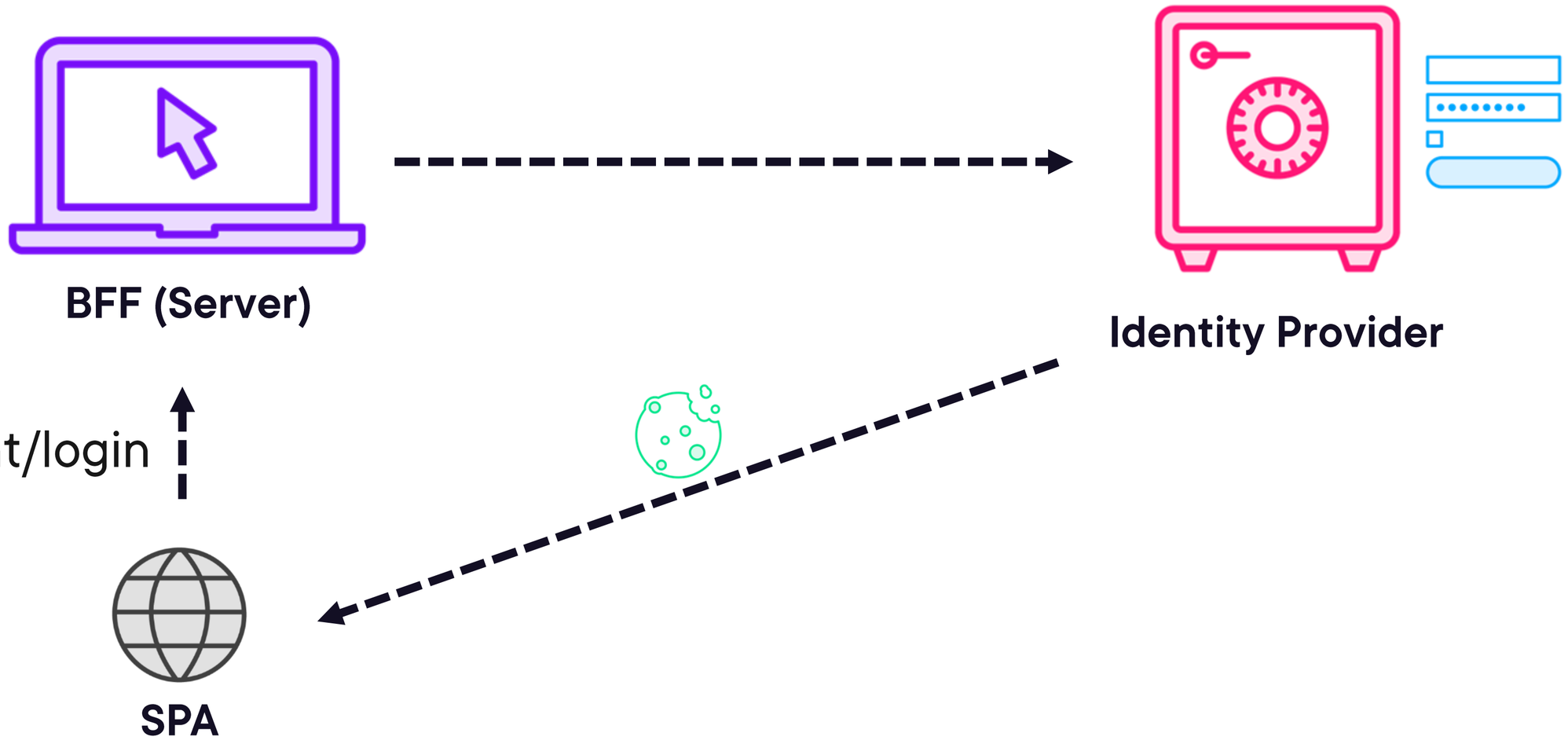
Working with SPAs

Implicit Flow is gone

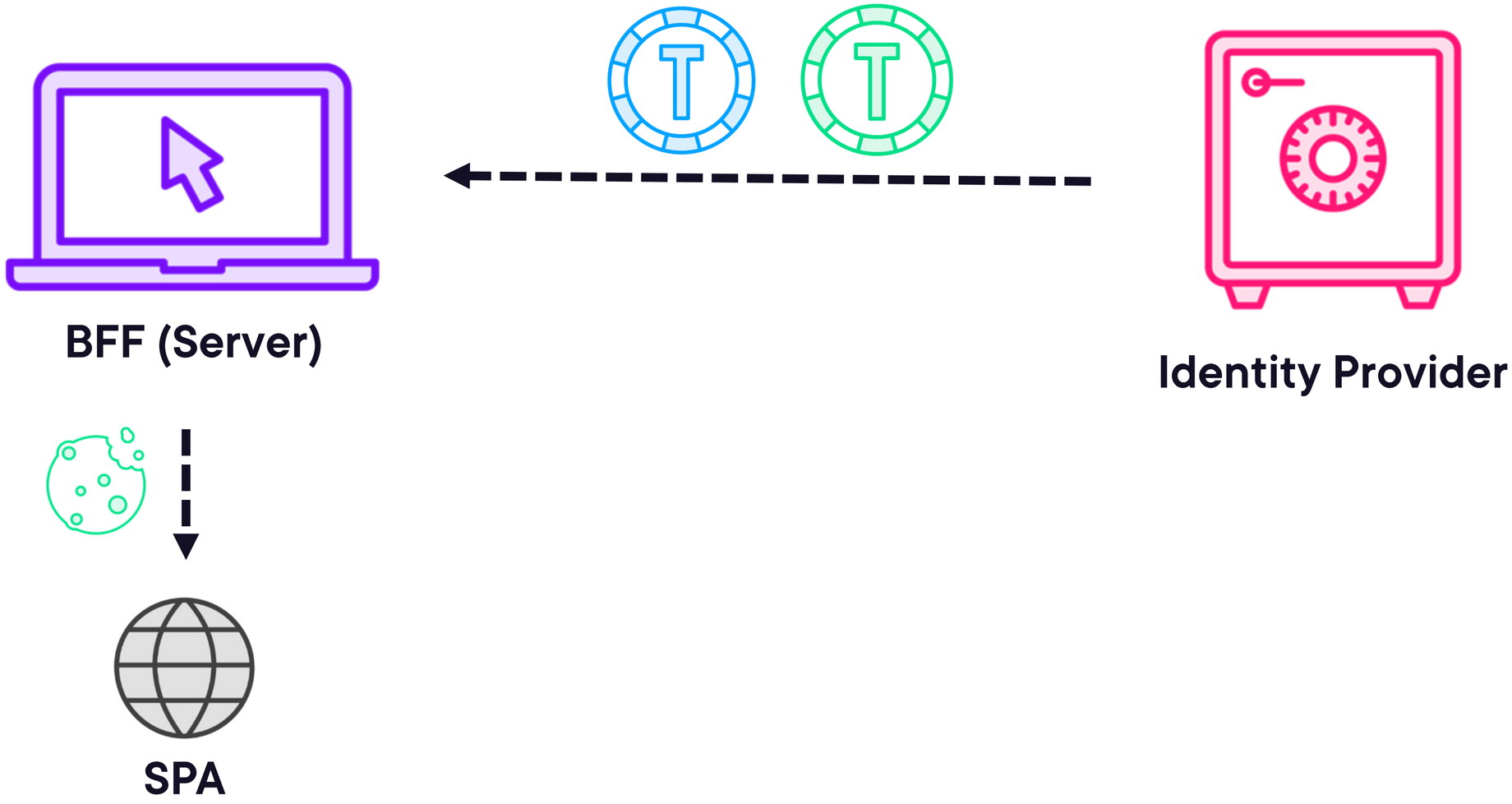
Authorization Code Flow too dangerous

Solution: BFF

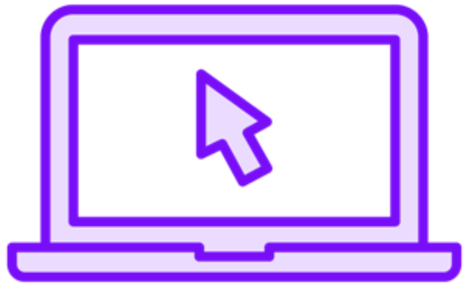
BFF



BFF



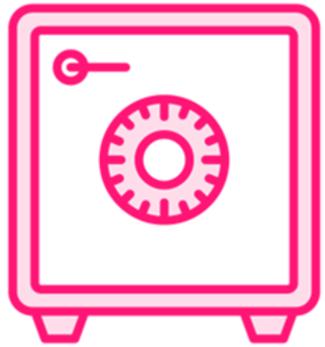
BFF



BFF (Server)

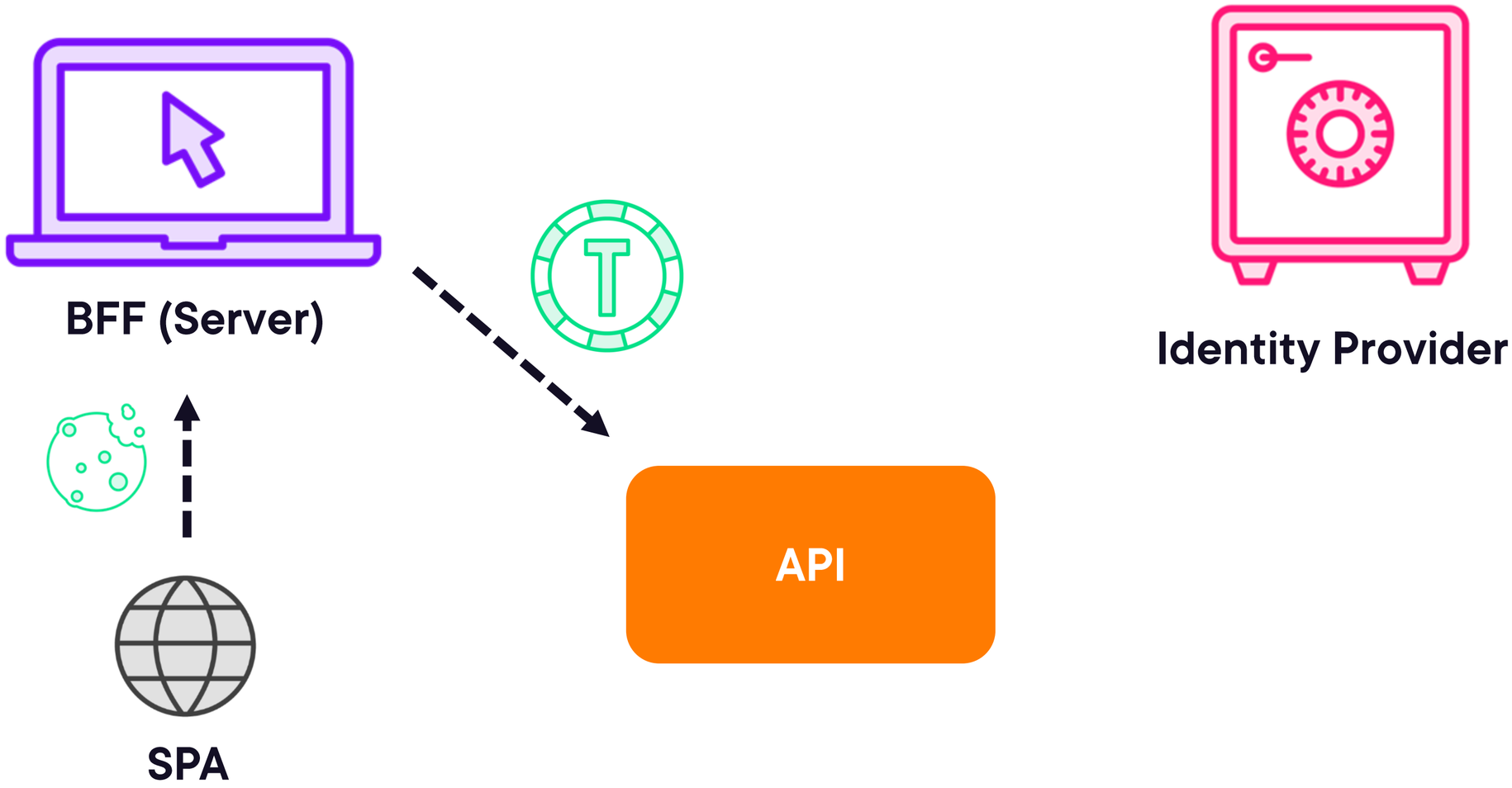
/account/user

SPA



Identity Provider

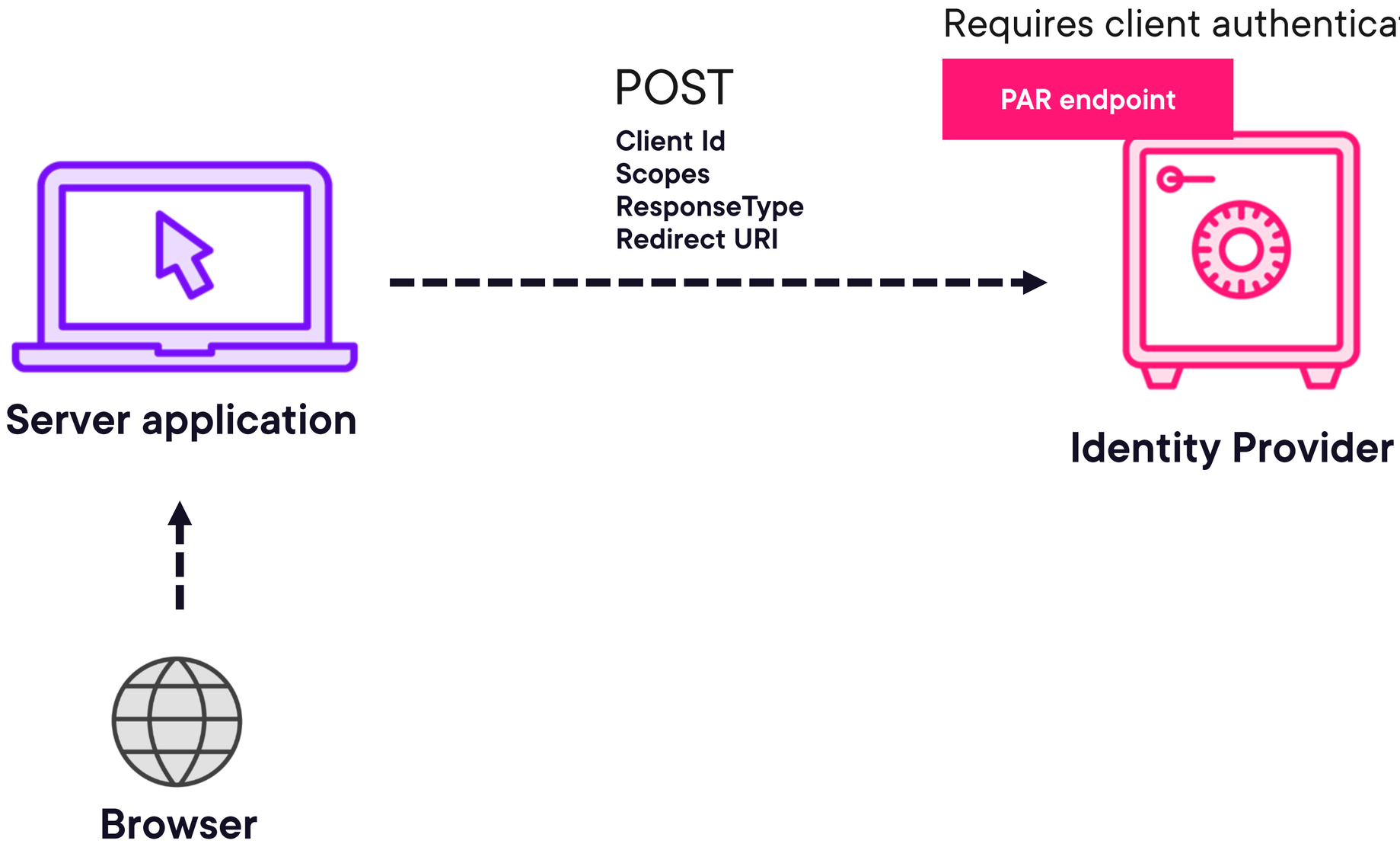
BFF: External APIs



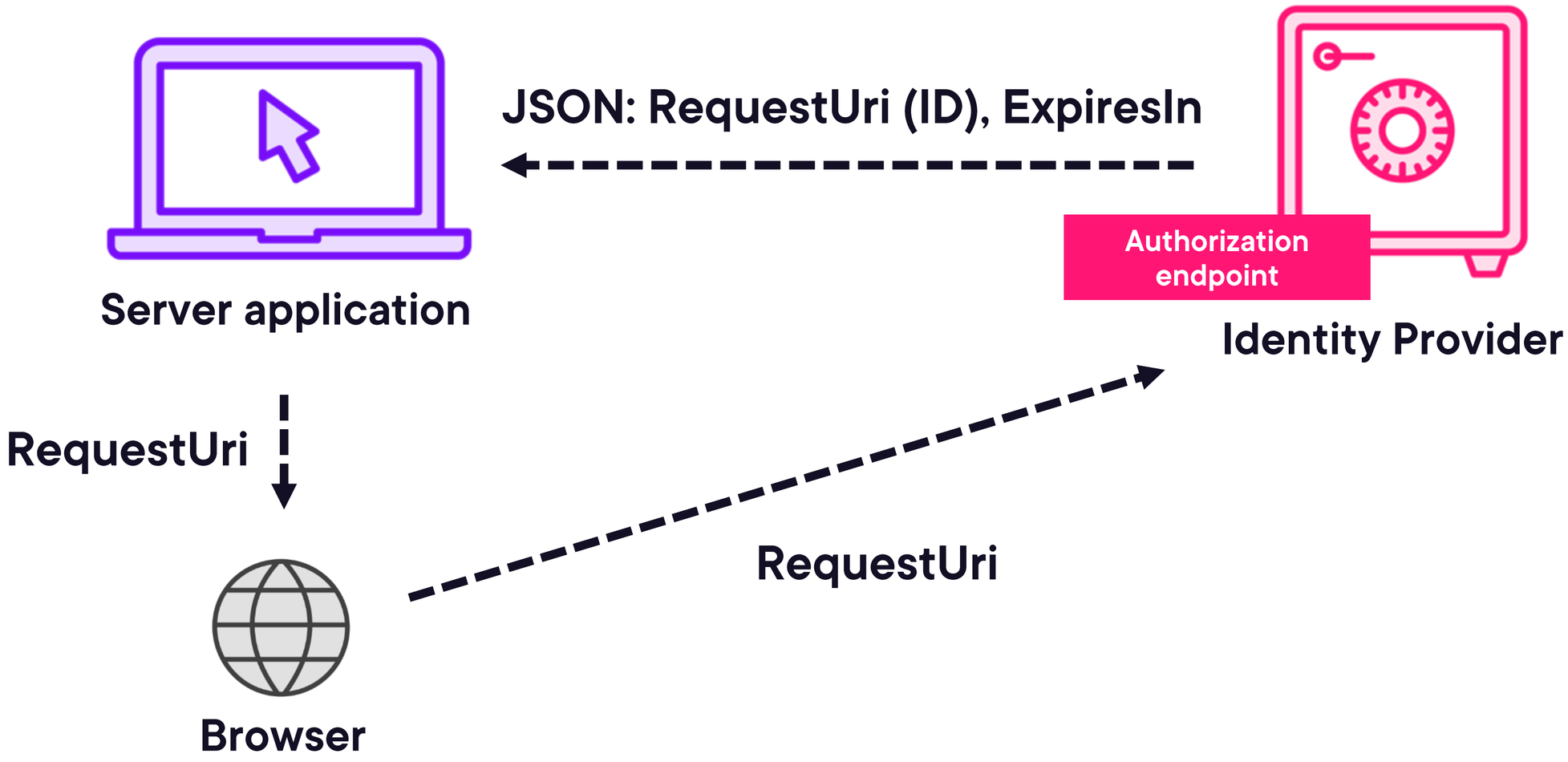
Demo

BFF

PAR


Requires client authentication
POST
Client Id
Scopes
ResponseType
Redirect URI
PAR endpoint
Server application
Identity Provider
Browser

PAR


JSON: RequestUri (ID), ExpiresIn
Server application
Authorization endpoint
Identity Provider
RequestUri
RequestUri
Browser

Demo

PAR

Remember This?

Refresh tokens for public clients must be either be sender-constrained or for one-time use

DPoP

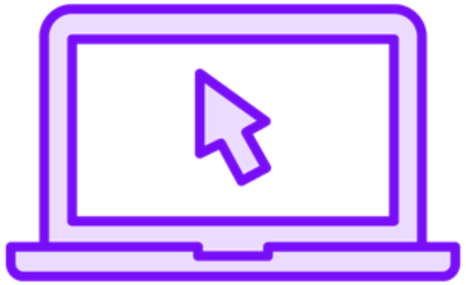
Demonstrating Proof of Possession

mTLS came before it

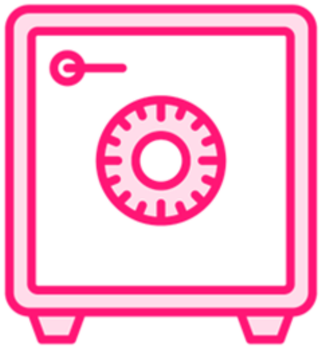
Purpose: bind access/refresh tokens to the client

DPoP

Generate private-public key pair

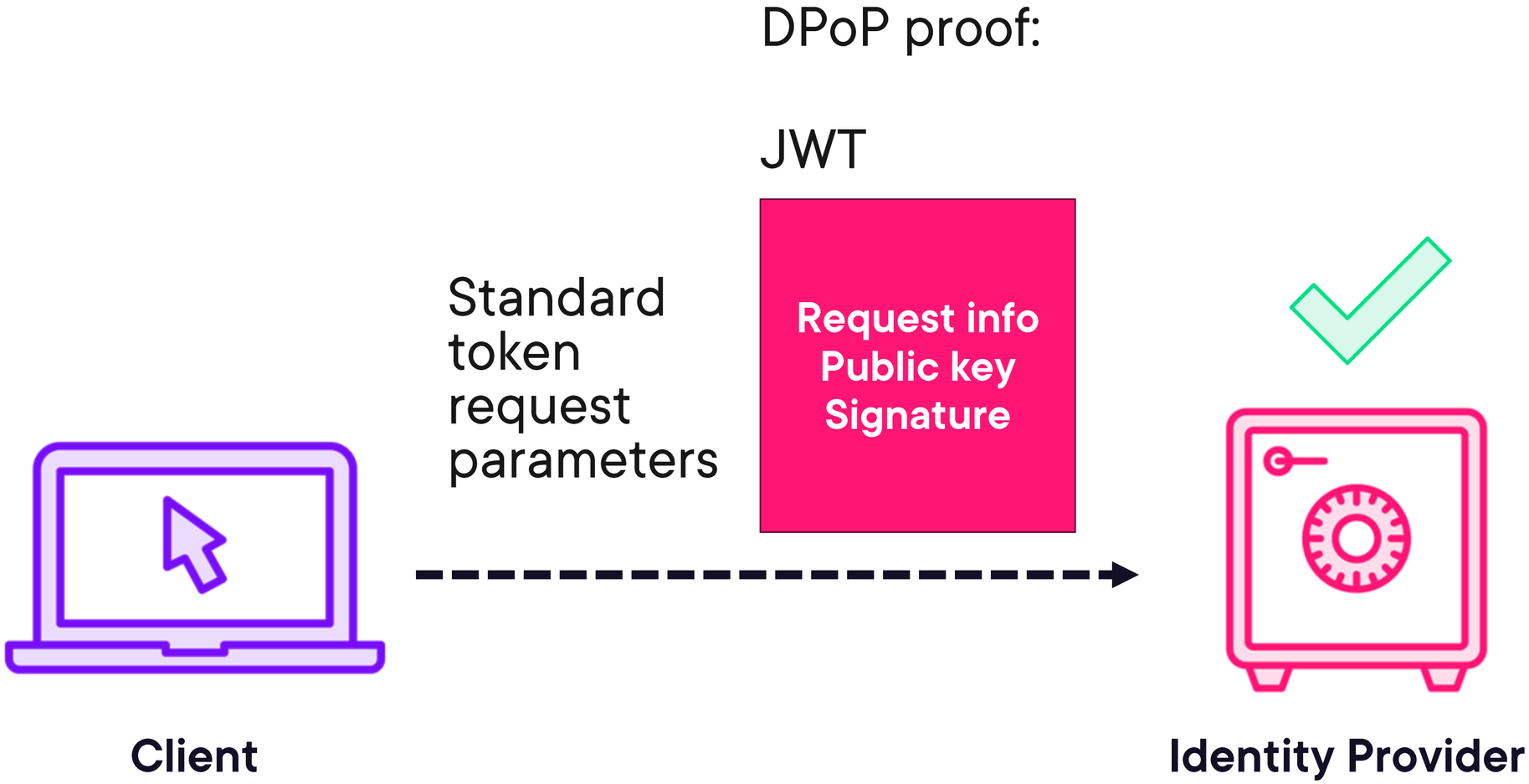


Client

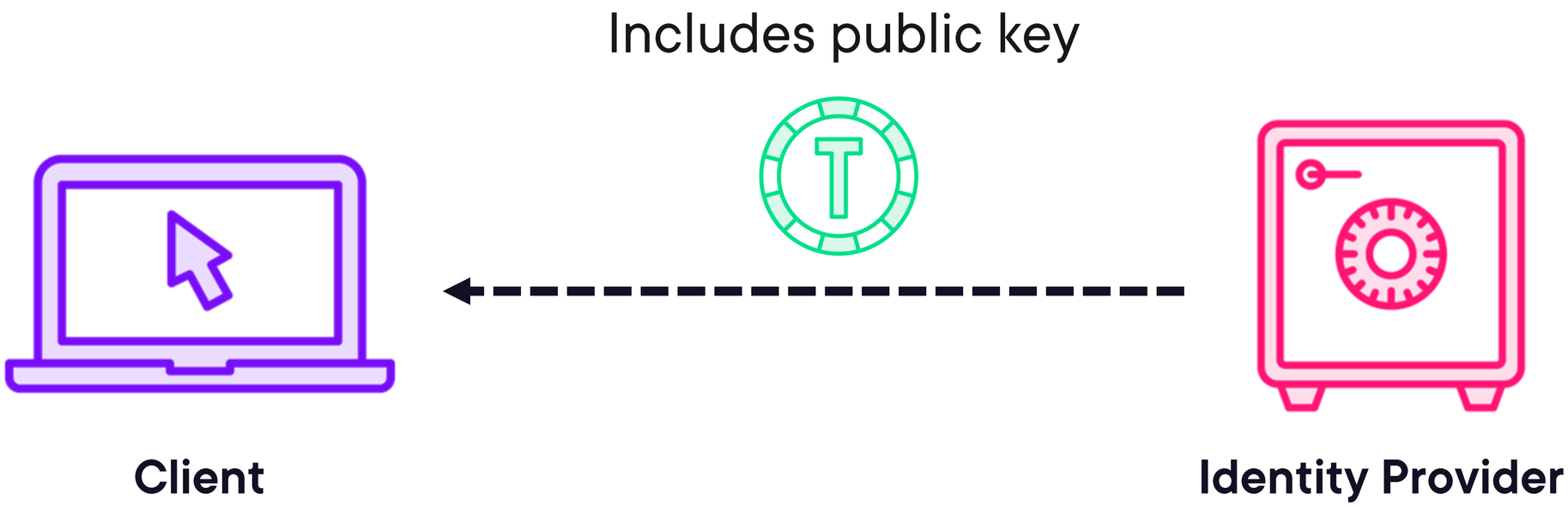


Identity Provider

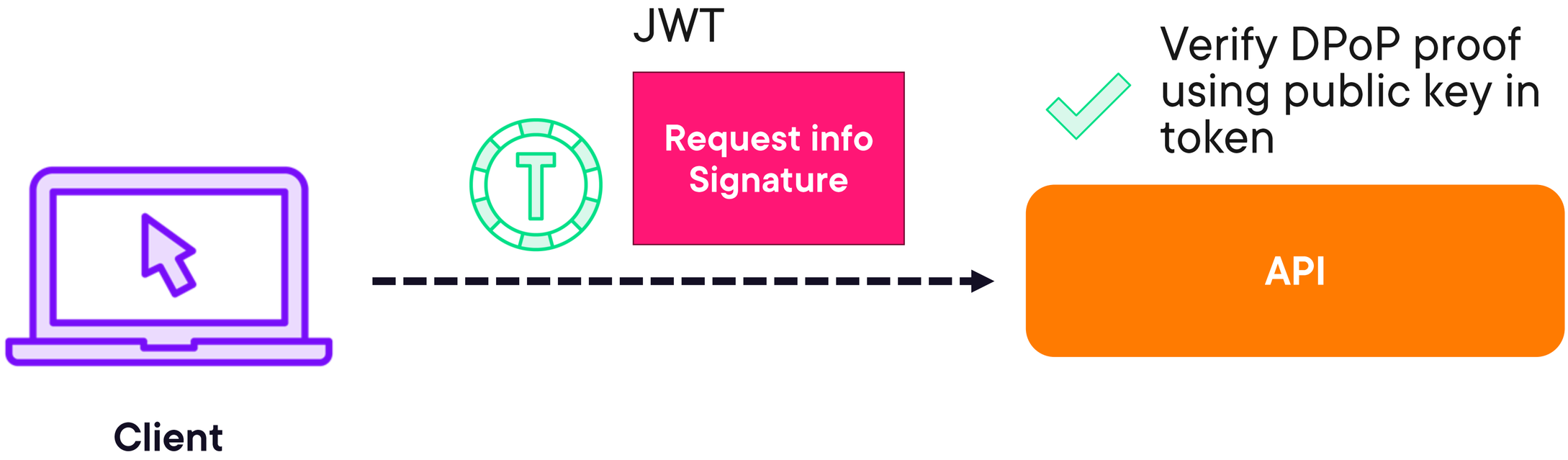
DPoP


DPoP proof:
JWT
Request info
Public key
Signature
Standard
token
request
parameters
Client
Identity Provider

DPoP



DPoP



The client demonstrated proof of possession of the private key

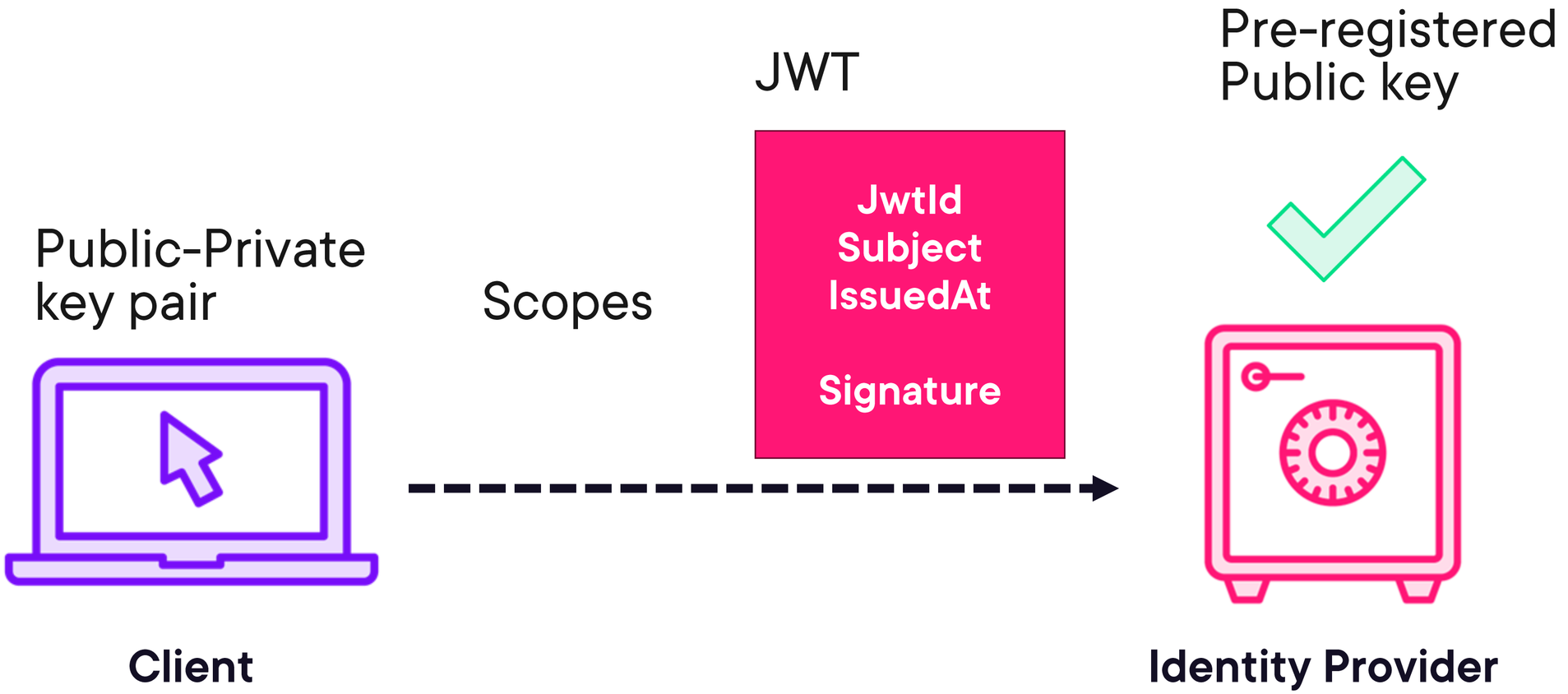
Demo

DPoP

Tip: Financial grade API Security Profile (FAPI) by the Open Banking Initiative

https://openid.net/specs/fapi-2_0-security-02.html

private_key_jwt



private_key_jwt

Demo

private_key_jwt

Thanks!

Roland Guijt

Freelance Trainer and Consultant | Microsoft MVP

@rolandguijt | roland.guijt@gmail.com