HL7® FHIR® Security

Education Event

API Security:
Navigating the Yellow Brick Road

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

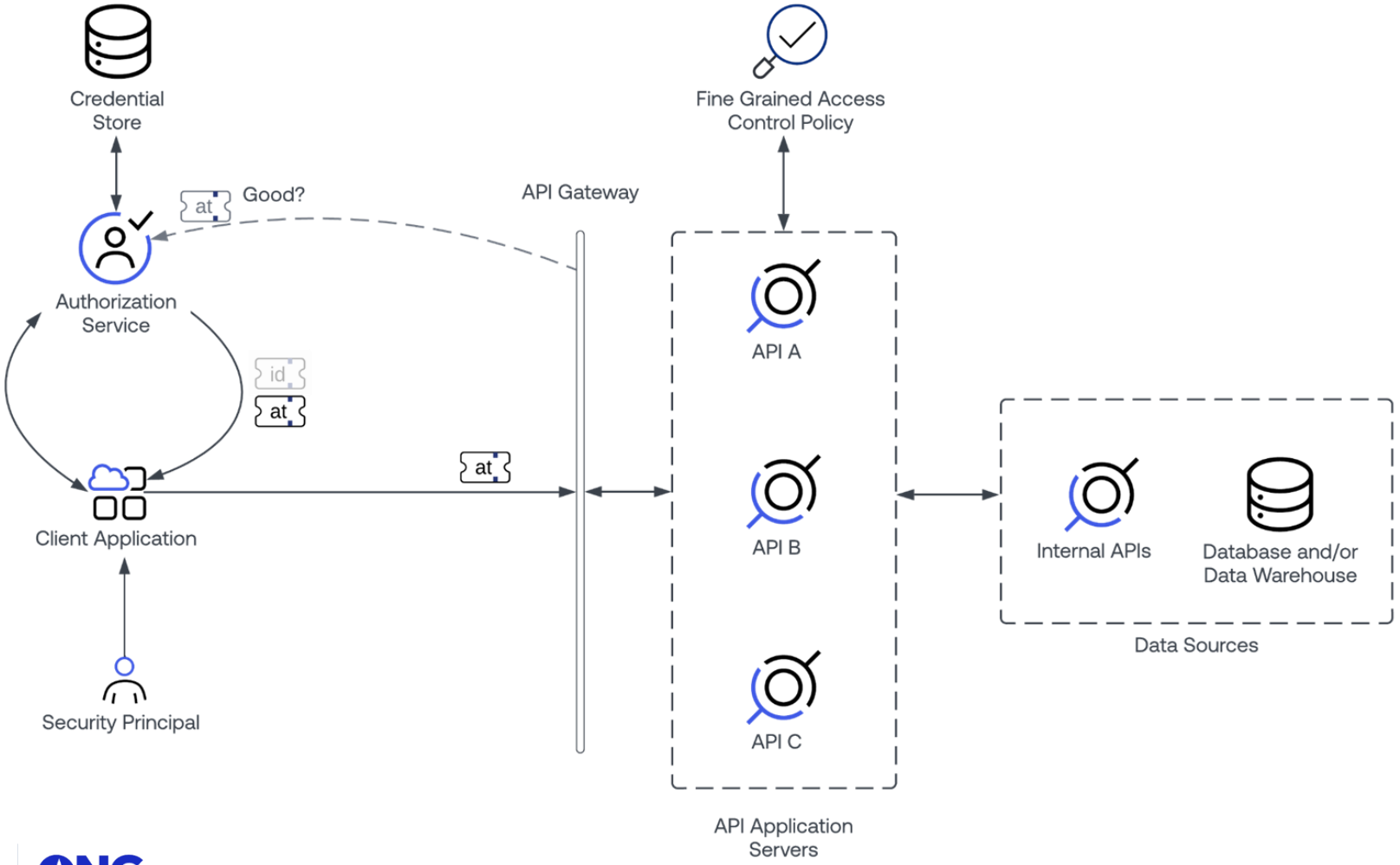
About Me

- Minnesota Native
- 15 years in the Identity Industry
- Working with HL7 Since 2020
- CISSP Since 2013
- Software Development Background

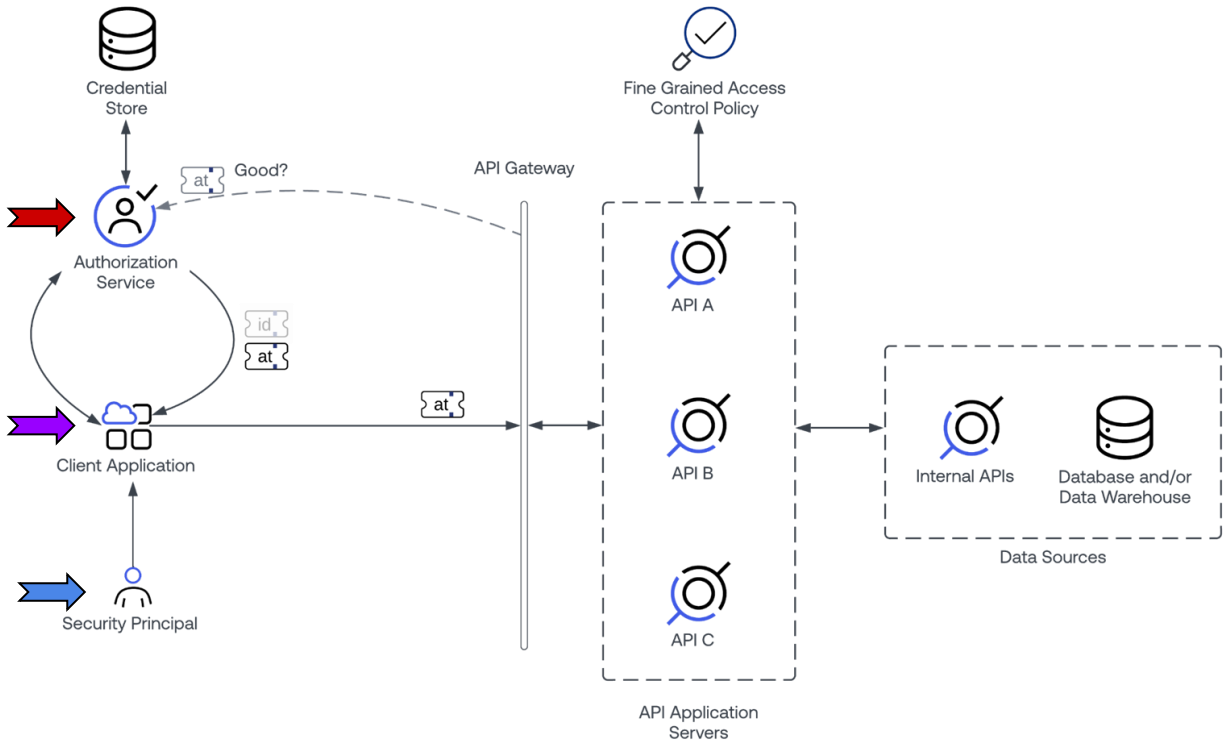
About the Session

- API Program Landscape Reference
- Access and Permissions
- Standards/Specifications
- What's Next?
- Q & A

A Typical Modern API Landscape



A Typical Modern API Landscape



Security Principal

People, APIs, Devices, Scripts, etc.

Client Application

Mobile applications, Web applications, Scripts, etc.

Acts on behalf of self, or another security principal (a person).

Authorization Service

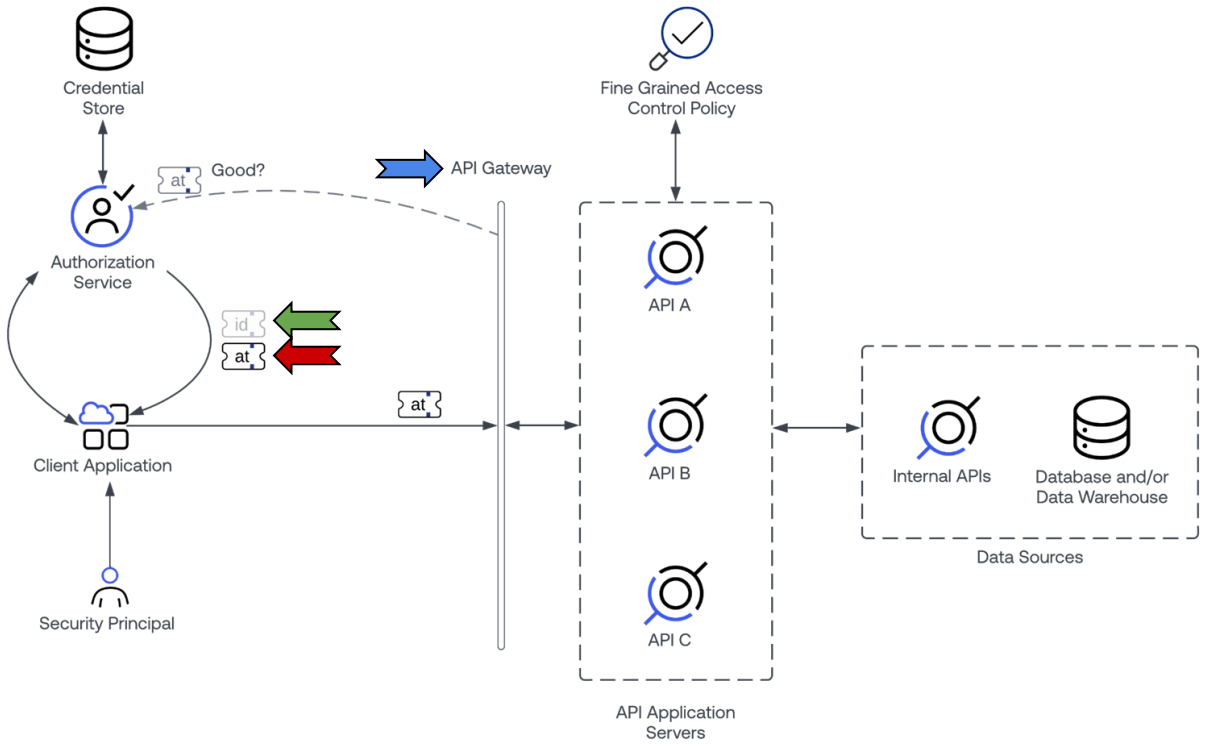
Authenticates the security principal AND client as applicable

Applies coarse grained authorization policy

Collects user<->client application consent as applicable

Mints security tokens used throughout the environment

A Typical Modern API Landscape



ID Token - Optional

Identifies the user to the client application.

Digitally signed, easily readable format (JWT).

Access Token

Authorizes the client to access the API on behalf of the security principal.

No predefined format- proprietary between authorization service and API. JWT is popular, but not universal.

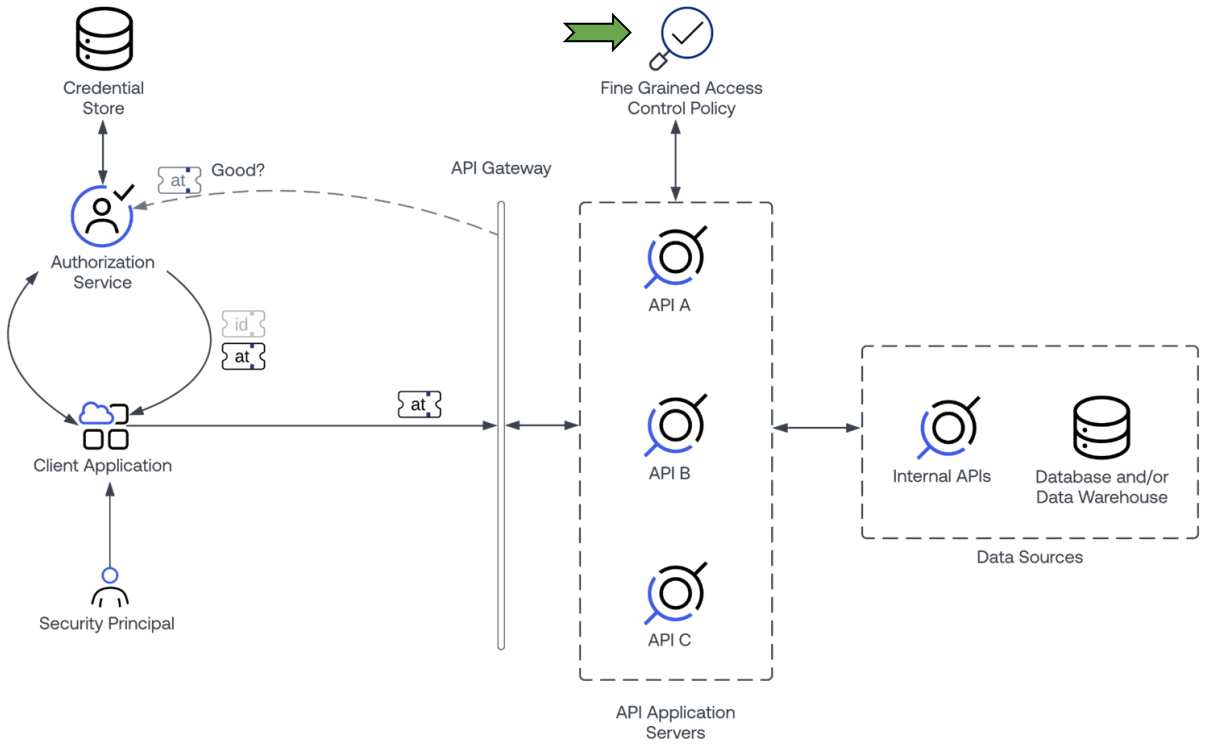
API Gateway

Validates the access token and enforces coarse grained access control.

Passes validated traffic to/from the API endpoints.

Offers many other value-added services.

A Typical Modern API Landscape



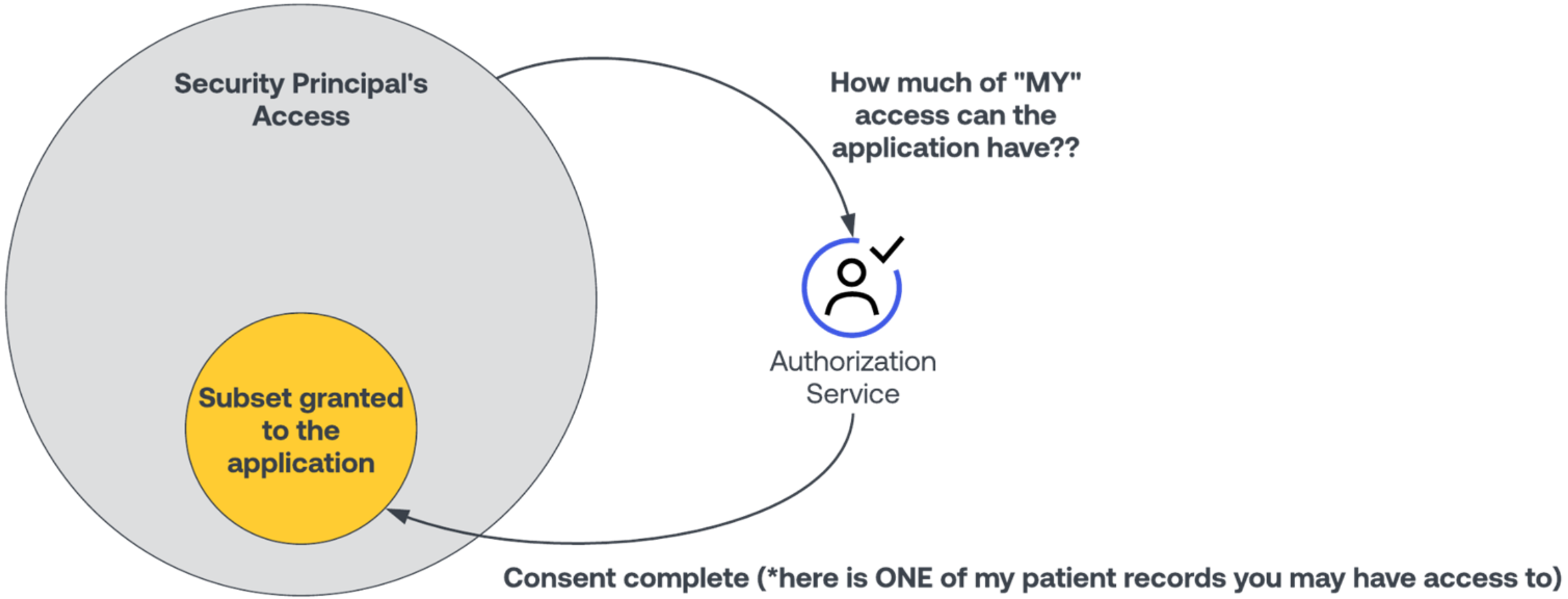
Fine Grained Authorization Service

Enforces granular resource and sub-resource level access.

Example: Out of 3 million patients, what subset does the security principal have access to?

Exact enforcement mechanisms vary.

Access and Permissions



Levels of Access Control

Coarse	"Medium"	Fine
Global allow/deny	Allow/deny based upon entitlement/role assigned to the security principal	Record-level access
Allow/deny scoped to resource type	Granularity determined by entitlement granularity	Access to 10k out of 100k records
SMART v1*	SMART v2	Time and/or location
		Largely proprietary

Standards/Specifications

(HL7 IG) SMART Launch Framework	++ Healthcare specific flows for supporting PHI data access use cases (among many others)
OpenID Connect	++ User identity/id token concepts
(HL7 IG) FAST Security / UDAP	++ Scalable client management & authentication
Standard OAuth2 Authorization Framework	Defines base concepts/components/flows

What's Next?

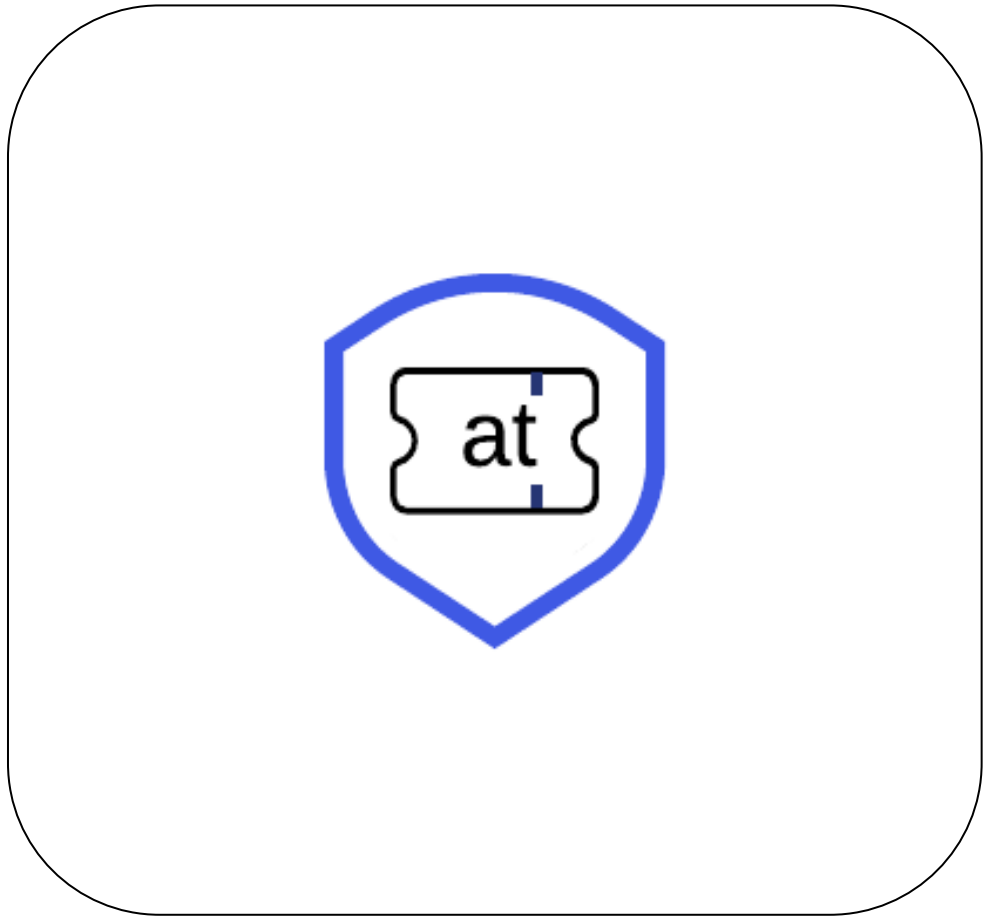
Proof of Possession

What is it?
Additional public/private key secrets exchange during the authorization process.

Benefits
Prevents the use of replayed or stolen access tokens.

Standards
RFC 9449 - DPoP

RFC 8705 - mTLS bound access tokens



What's Next?

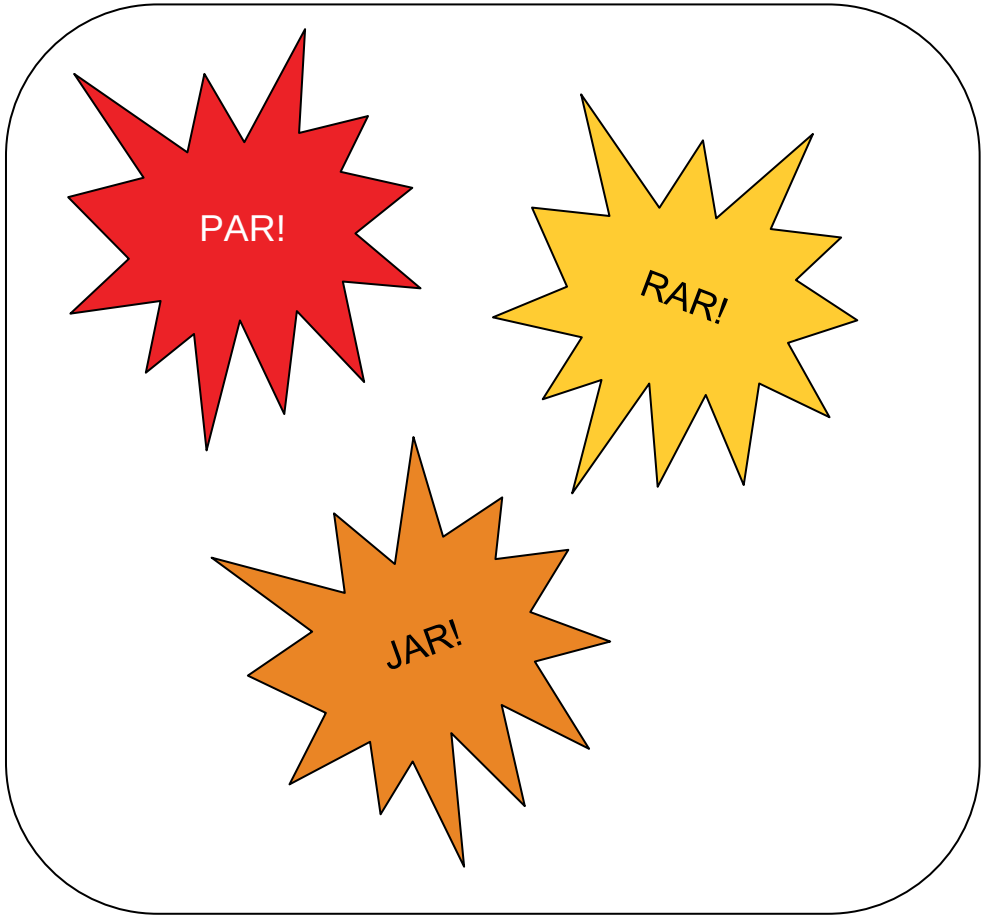
OAuth2 Request Hardening

What is it?
Provides more assurance that authorization request details from clients have not been tampered with.

Benefits
Enables sensitive information to be conveyed and validated in the authorization request (PAR and JAR).

Enables finer granularity on both the authorization request and response (RAR).

Standards
RFC9126 (PAR), RFC9396 (RAR), RFC9101 (JAR)



What's Next?

CIBA

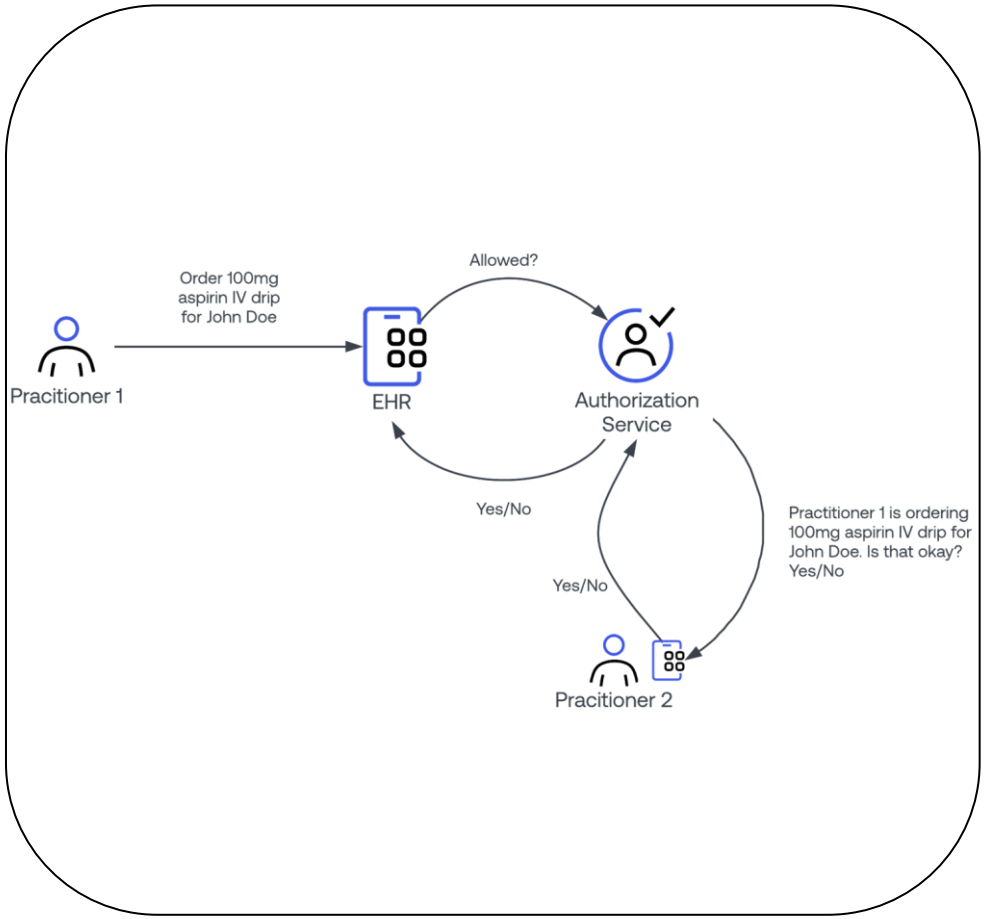
What is it?
Client-Initiated Backchannel Authentication

OpenID standard for transactional and/or out of band authentication

Benefits
Enables a standardized way of challenging users immediately upon a sensitive transaction (like EPCS).

CIBA recipient need not be the same person as the application user.

Standards
[OpenID Connect Client-Initiated Backchannel Authentication Flow - Core 1.0]



Q & A