

@Web Conference  
29 Sep 2021

# FAPI-SIG Community 27<sup>th</sup> Meeting

# Table of Contents

Major Topics

Discussion :

Client Policies vs Client Setting

Working Items Status

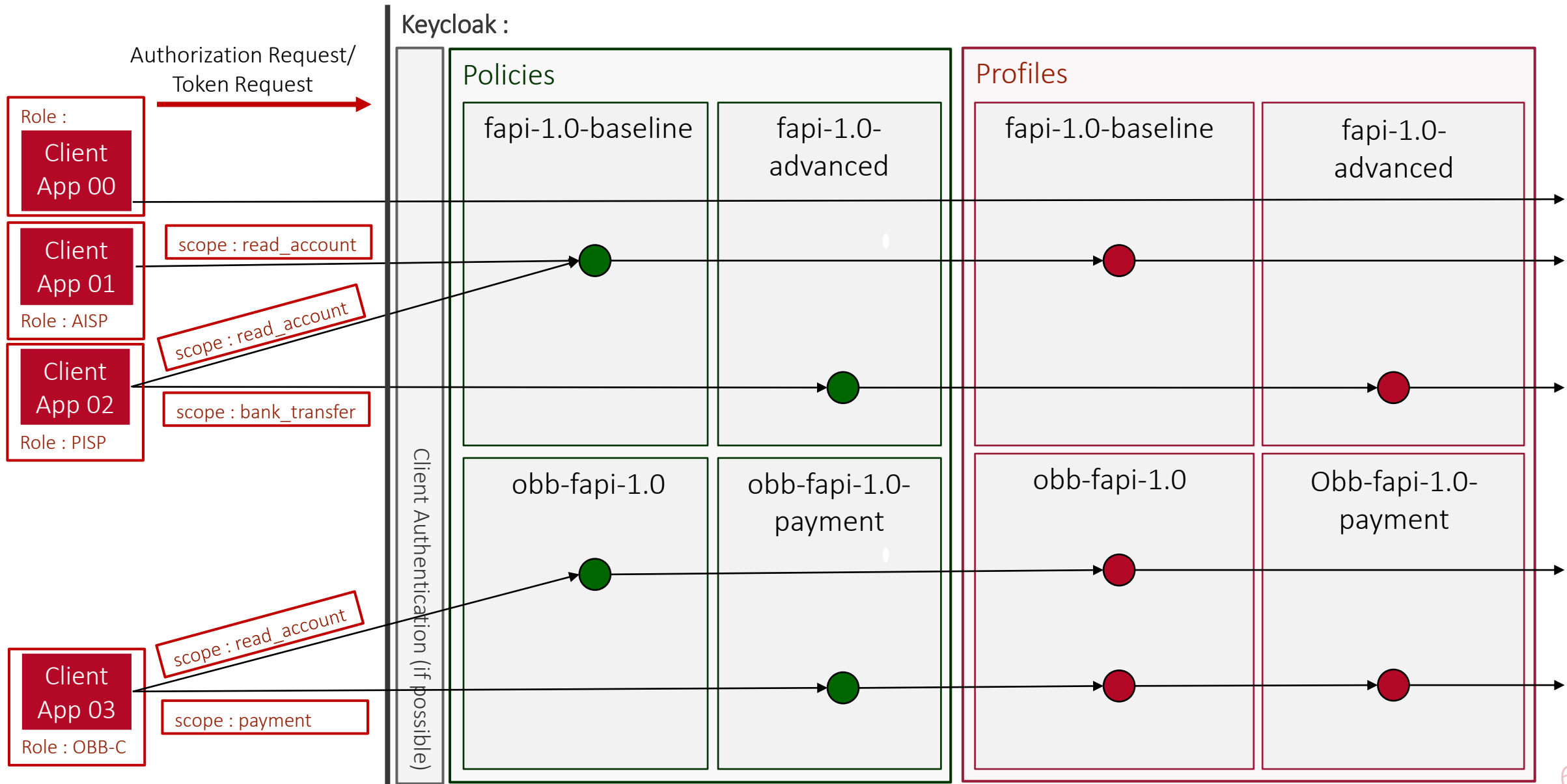
# Major Topics

# Major Topics

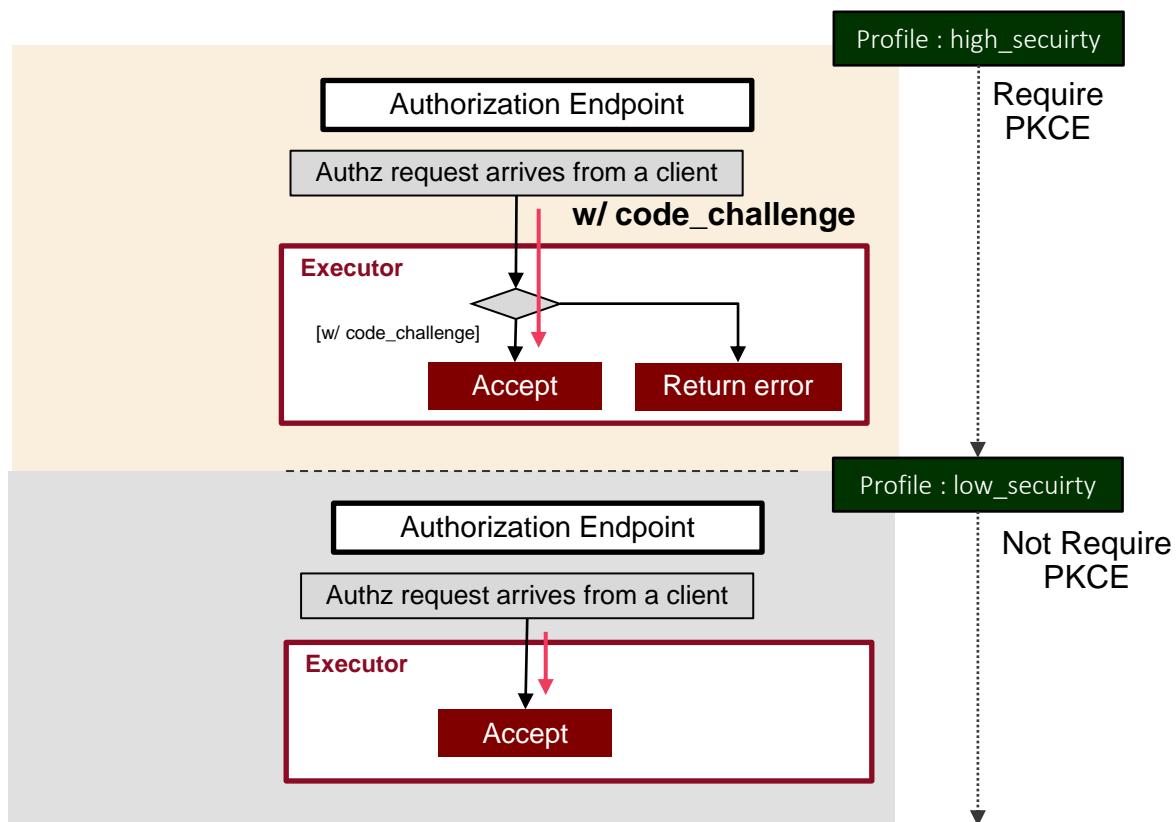
- [OBB] Open Banking Brasil FAPI 1.0 Security Profile draft version up (ID1 -> ID2)
- [FAPI 2.0] OAuth 2.0 Pushed Authorization Requests (PAR) became RFC 9126
- [FAPI 2.0] OAuth 2.0 Rich Authorization Requests (RAR)  
Design document's review is in progress.
- [FAPI 2.0] OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)  
Design document's review is in progress.

# Discussion : Client Policies vs Client Setting

# Motivation : change security profiles dynamically



# Objectives

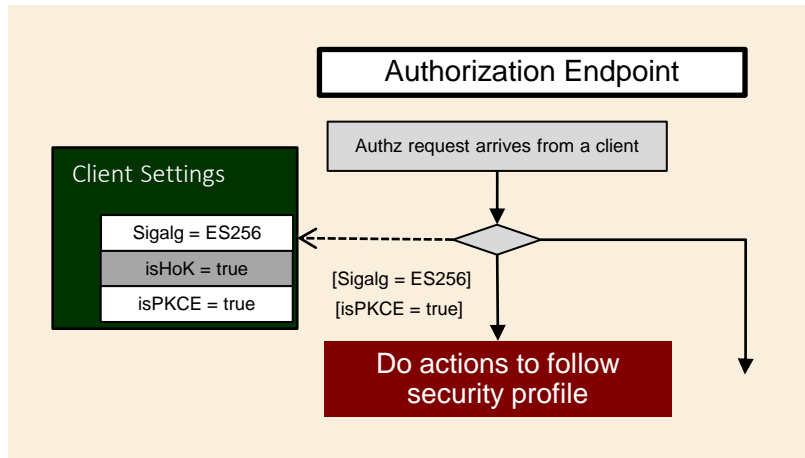


Current client policies have some limitation on dynamically changing security profiles per client request.

Client Policies Revised tries to get rid of this limitation.

To do so, client policies does not rely on client settings as much as possible.

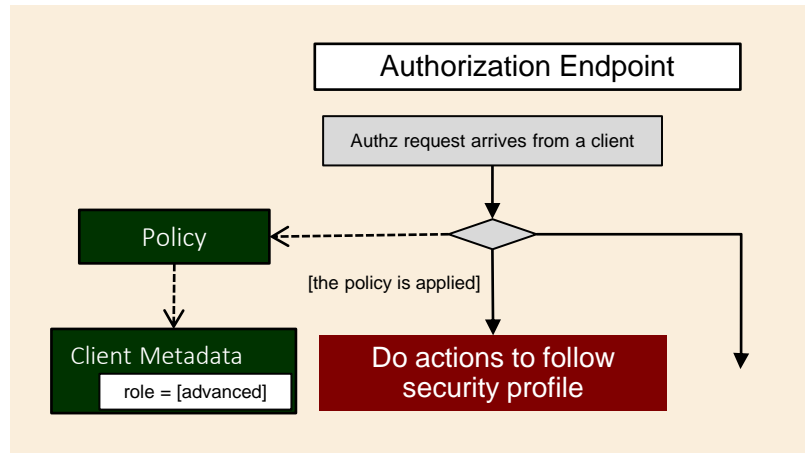
# Settings vs Policies



## [By Settings]

By referring values of client settings, determine whether security profile related actions and checks are executed.

- pros : leverages existing logics.
- cons : one setting per client



## [By Policies]

By evaluating a policy, determine whether security profile related actions and checks are executed.

- pros : change security profiles dynamically and flexibly.
- cons : need additional logics



# Basic Strategy

## [Default Logics]

Execute logics defined by standard specification or keycloak's specification by referring values of client settings.

## [Executor Logics]

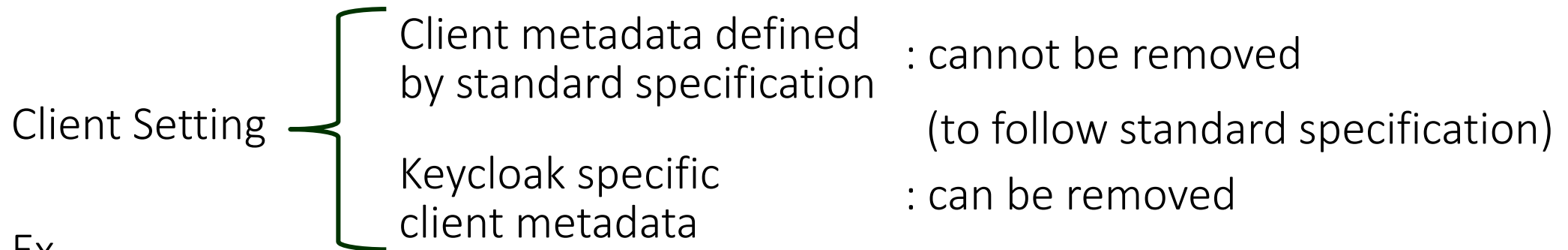
If an executor is executed, override default logics, ignore client settings and enforce executor logics against a client's request.

It is equivalent of changing client settings and executing default logics temporarily.

# Basic Strategy

## [Removing Client Settings]

By enforcing logics by executors, some client settings can be removed.



Ex.

- PKCE : can be removed

Keycloak specific client metadata :

OIDCConfigAttributes.PKCE\_CODE\_CHALLENGE\_METHOD

- Holder-of-Key bound token : cannot be removed

Standard client metadata : `tls_client_certificate_bound_access_tokens`

# Working Items Status

# Working Items

## [Security Features]

### <Common>

**In Progress** OIDC Client's Public Key Management

1<sup>st</sup> phase -> 2<sup>nd</sup> phase

**In Progress** Client Policies Revised



Hitachi



Hitachi

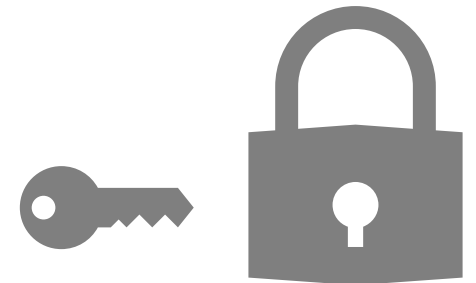
## [Security Features]

### <SPA/Native App>

**In Progress** OAuth 2.0 Demonstration of  
Proof-of-Possession (DPoP)



Backbase



# Working Items

[Security Features]

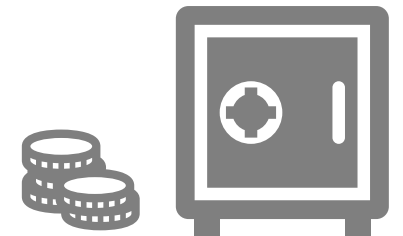
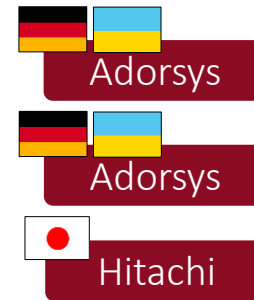
<High Level Security>

- FAPI 2.0 (baseline/advanced)

In Progress Rich Authorization Request (RAR)


In Progress Grant Management API

In Progress Other requirements support



# Working Items

## [Market Specific Features]

<PSD2> 

- Following eIDAS regulations

 QWAC verification

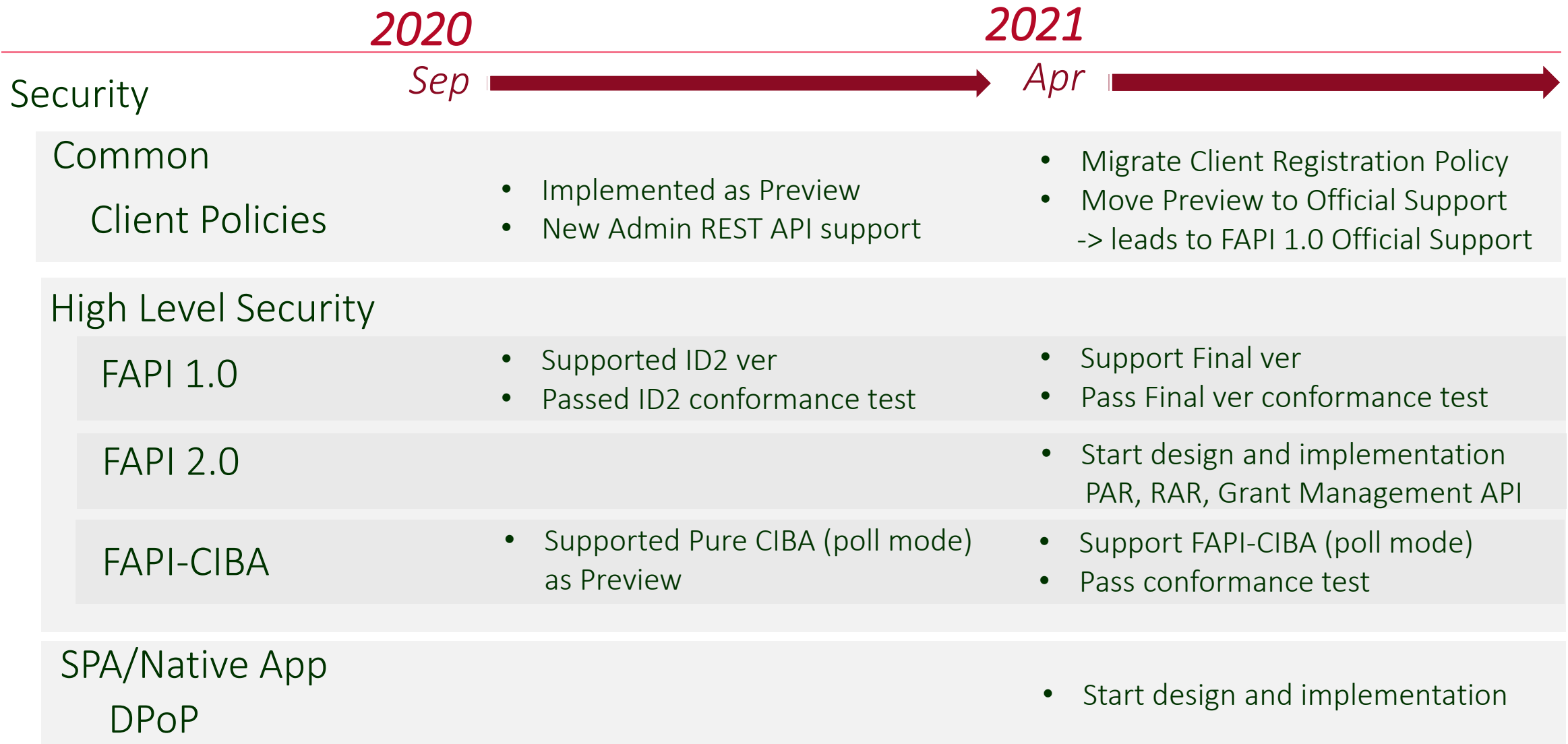


- Consent Management

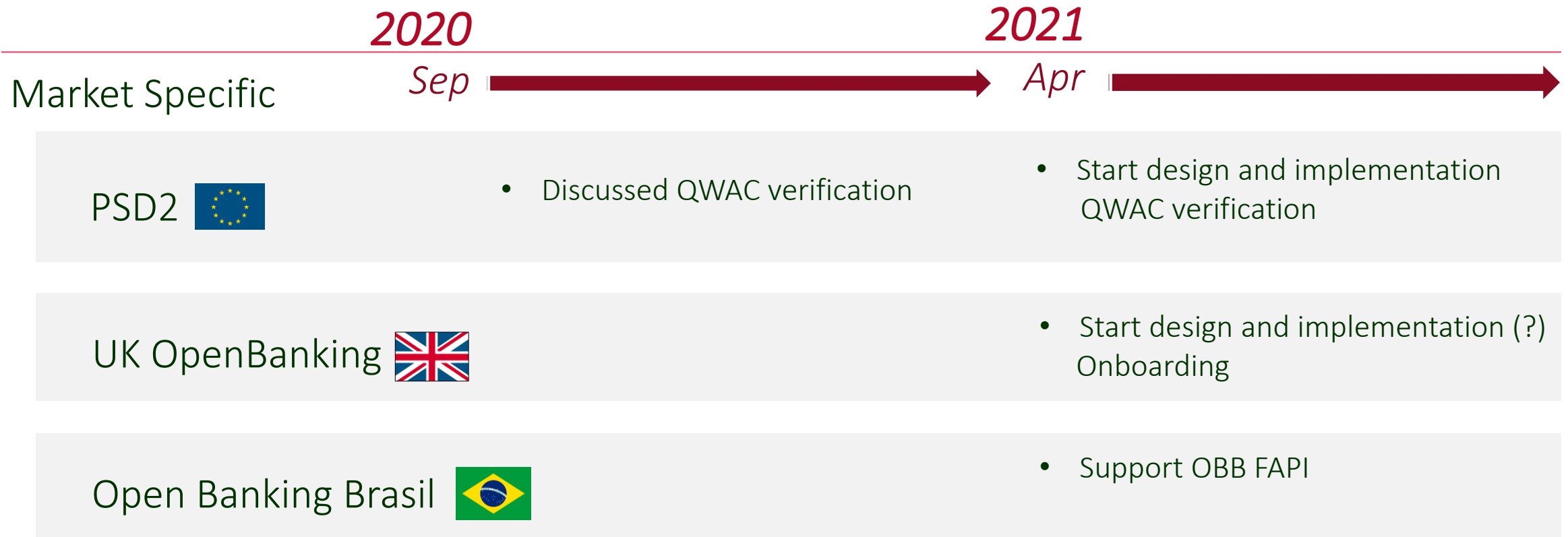
<UK OpenBanking> 

- Onboarding
  - Software Statement Support
  - Software Statement Assertion (SSA) Verification

# Roadmap



# Roadmap





END