

@Web Conference
1 Sep 2021

FAPISIG Community 26th Meeting

Table of Contents

Major Topics

Proposal :

PII returned from Token Introspection

Working Items Status

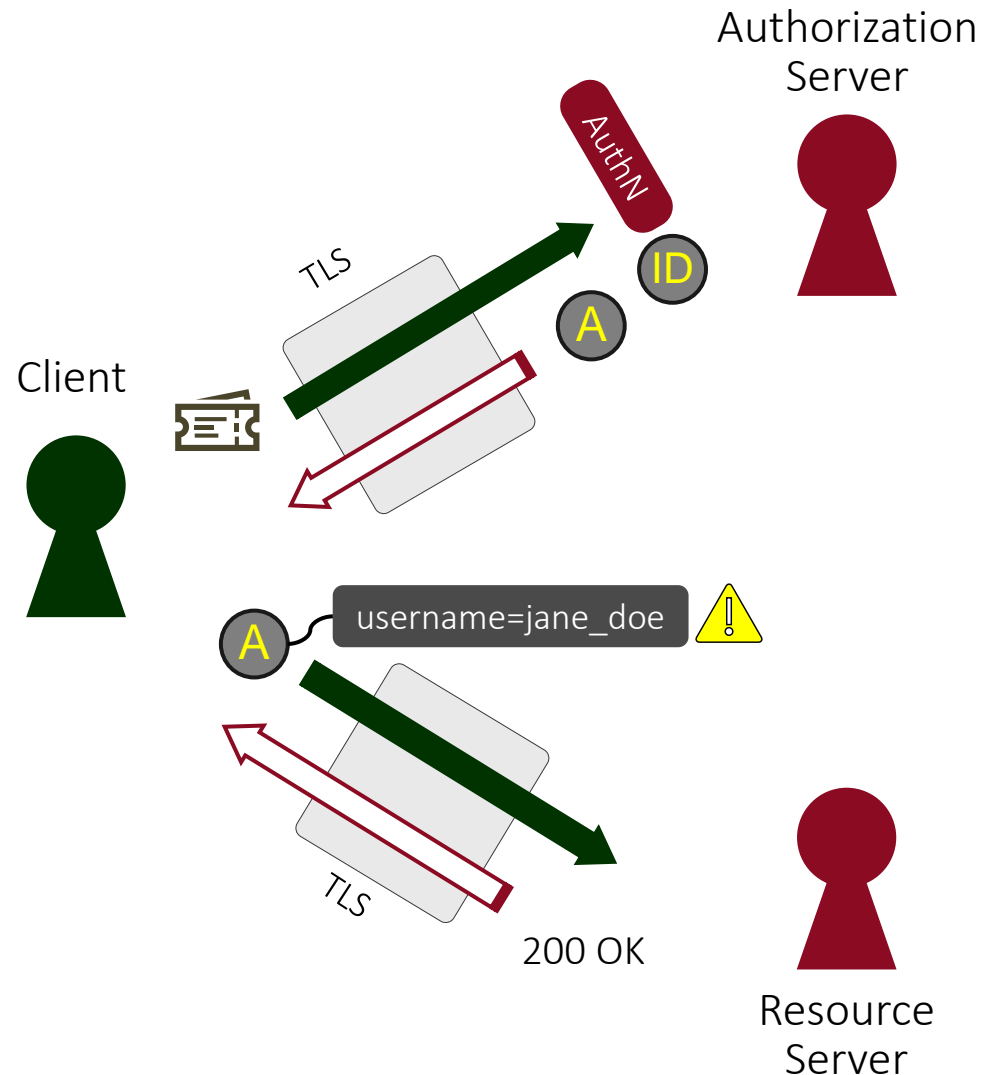
Major Topics

Major Topics

It seems that nothing special happens.

Proposal : PII returned from Token Introspection

Situation

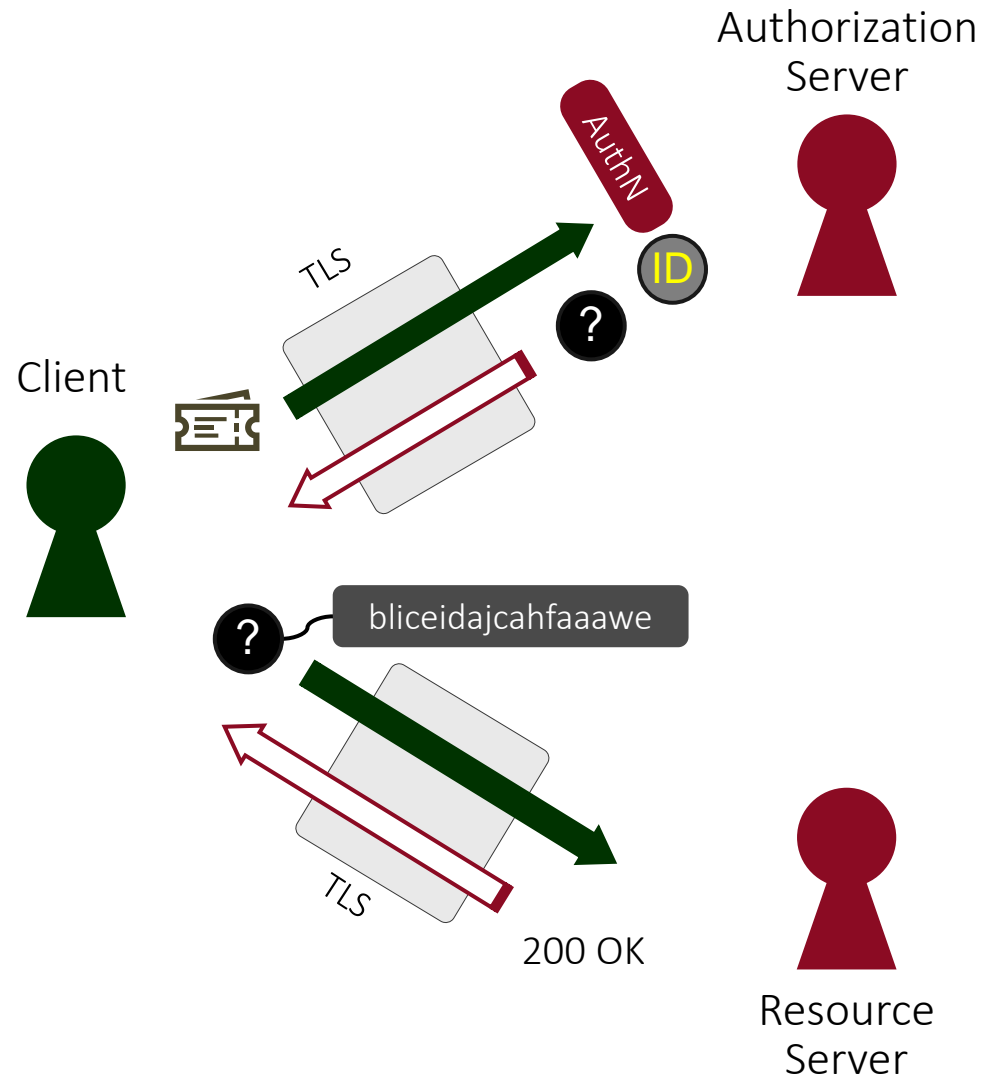


Keycloak allows us to select which data is put onto an access token.

In some case, it is not preferable for the access token to include PII.

However, a resource server receiving the access token needs to know who is authenticated to make access control decision.

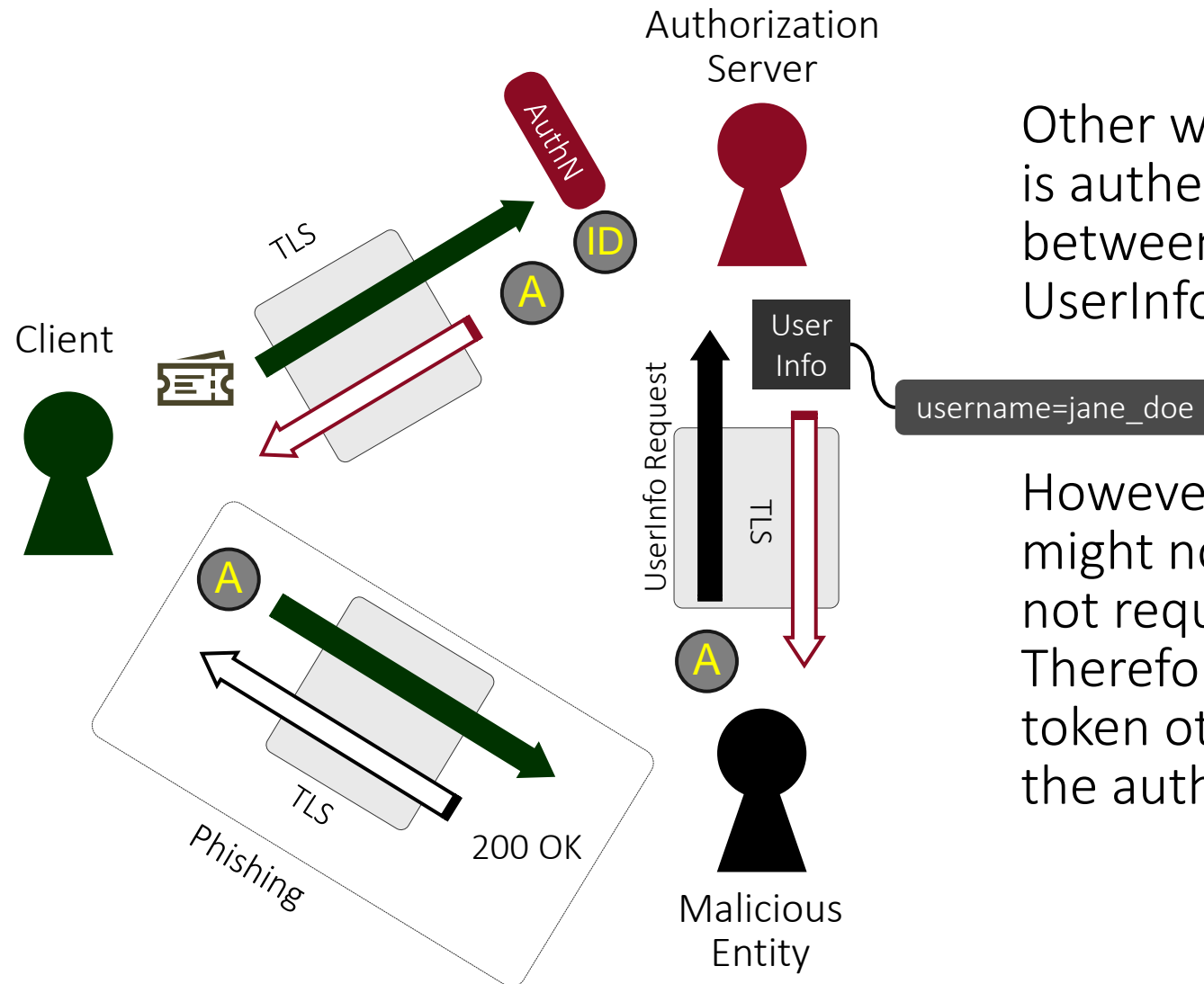
Situation



One way for resource server to know who is authenticated without revealing PII between client and resource server is to encrypt the access token in JWE.

However, JWE/JWA does not cover encryption among multi parties.

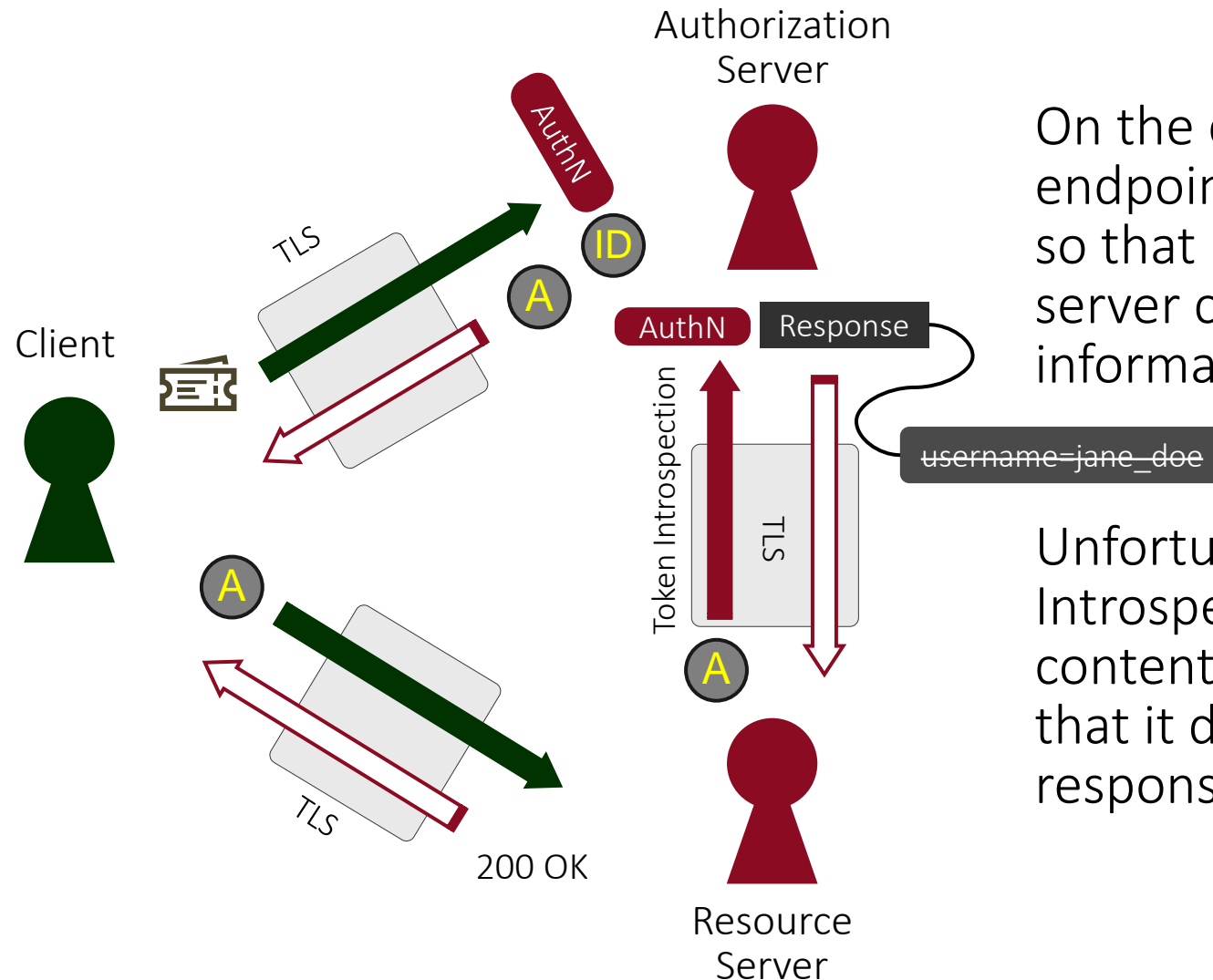
Situation



Other way for resource server to know who is authenticated without revealing PII between client and resource server is to use UserInfo endpoint.

However, it seems that UserInfo endpoint might not be not so secure because it does not require the client authentication. Therefore, everybody holding the access token other than the resource server can get the authenticated user information

Situation



On the contrary, Token Introspection endpoint requires the client authentication so that it might be good if the resource server could get the authentication user information from it.

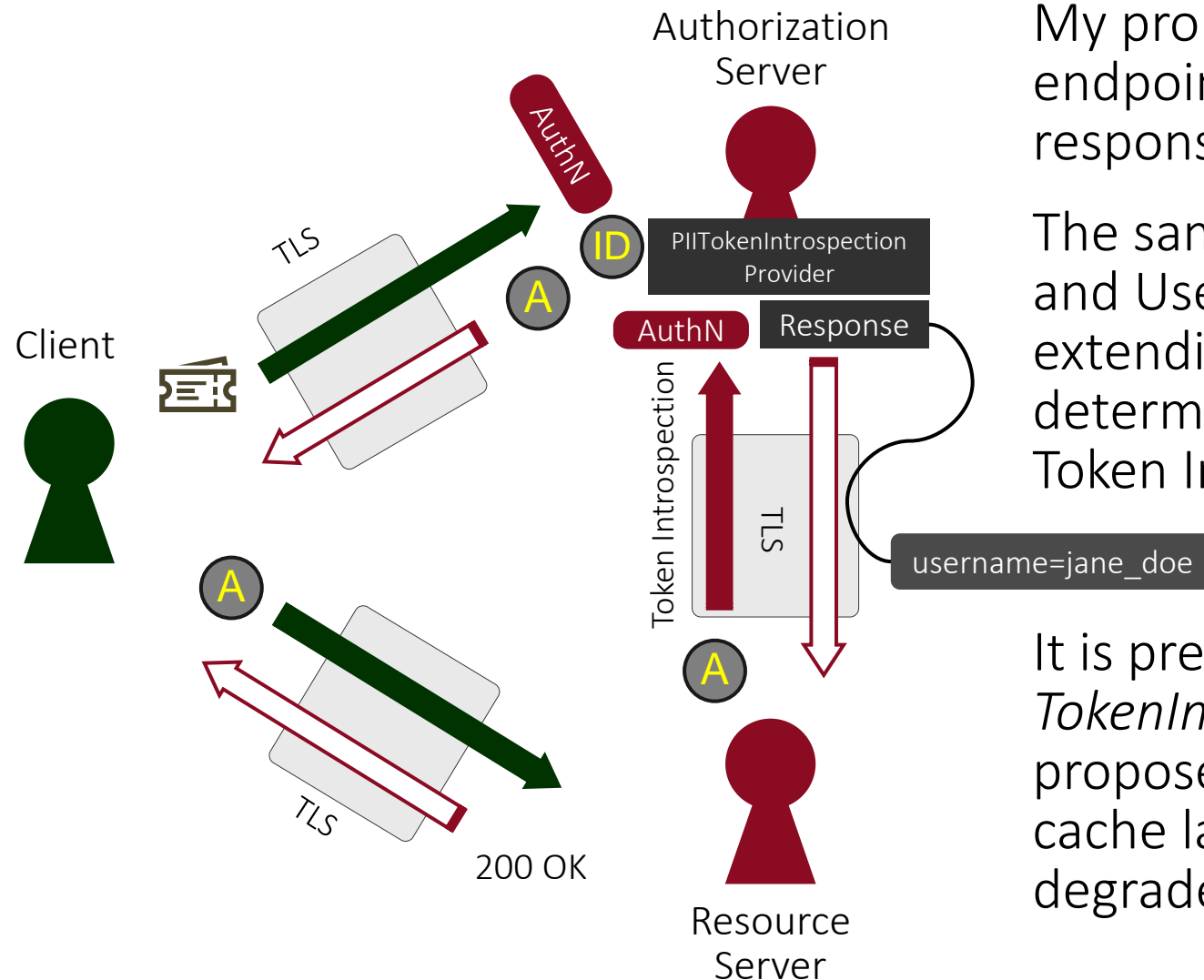
Unfortunately, the current Token Introspection endpoint only returns the contents of the access token it receives so that it does not include other claims onto its response.

Situation

My proposal is to make Token Introspection endpoint include other claims onto its response.

The same way for the access token, ID token and UserInfo response, protocol mappers extending *AbstractOIDCProtocolMapper* can determine whether its claim is included in Token Introspection response.

It is preferable to realize it by *TokenIntrospectionProvider* because the proposed feature needs to access DB or cache layer to retrieve data, which leads to degrade performance.



Working Items Status

Working Items

[Security Features]

<Common>

In Progress OIDC Client's Public Key Management

1st phase -> 2nd phase

In Progress Client Policies Revised



Hitachi



Hitachi

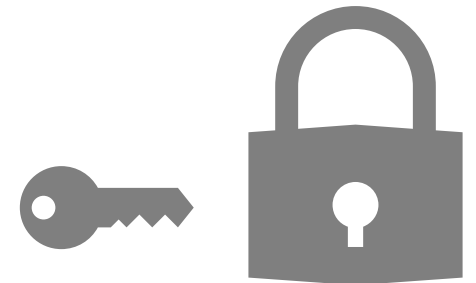
[Security Features]

<SPA/Native App>

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



Backbase



Working Items

[Security Features]

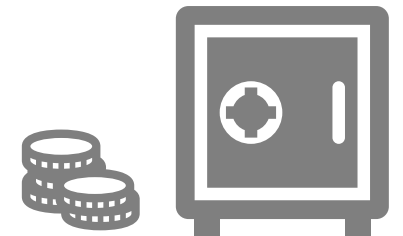
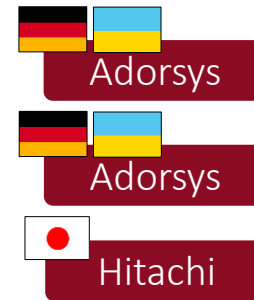
<High Level Security>

- 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

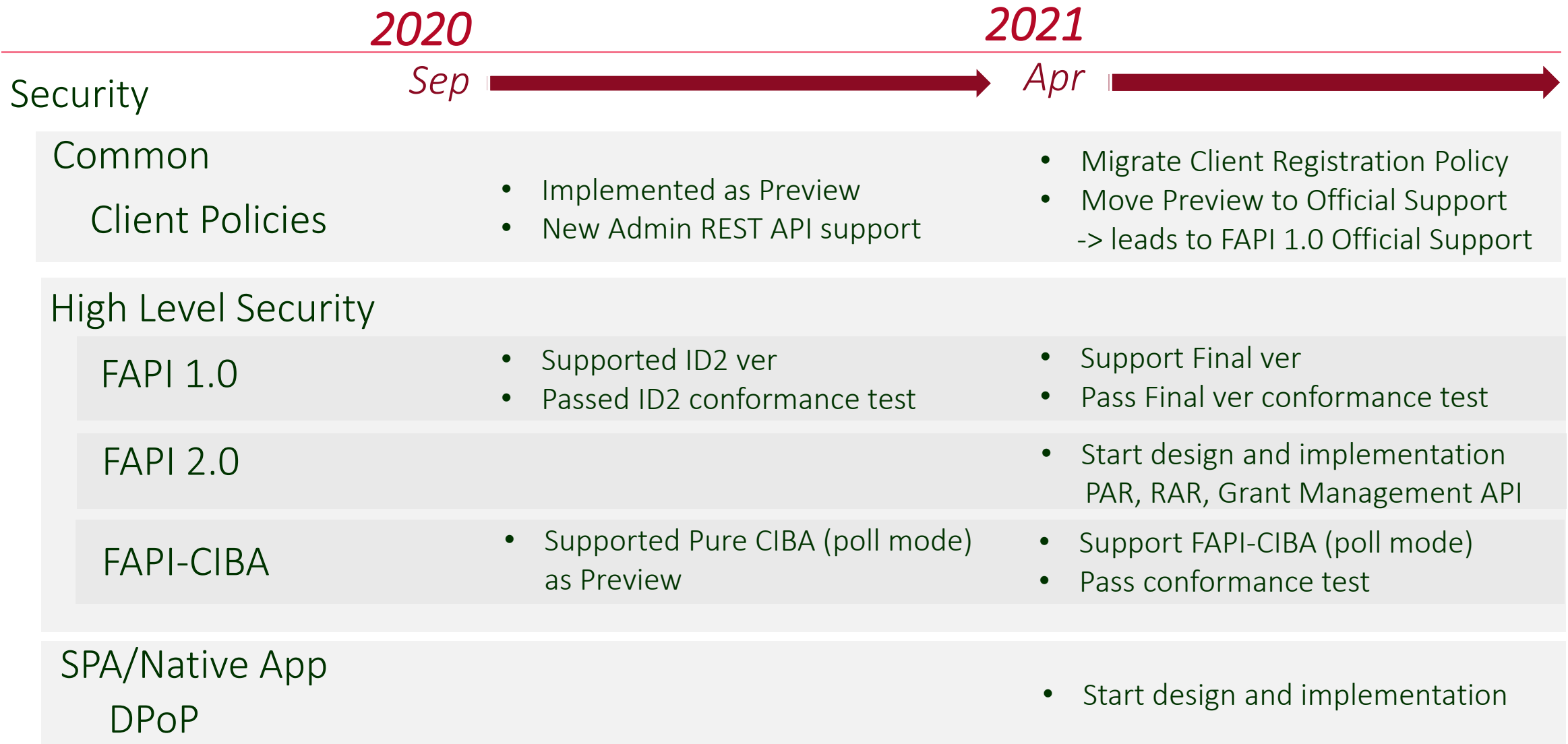
<UK OpenBanking> 

- Onboarding

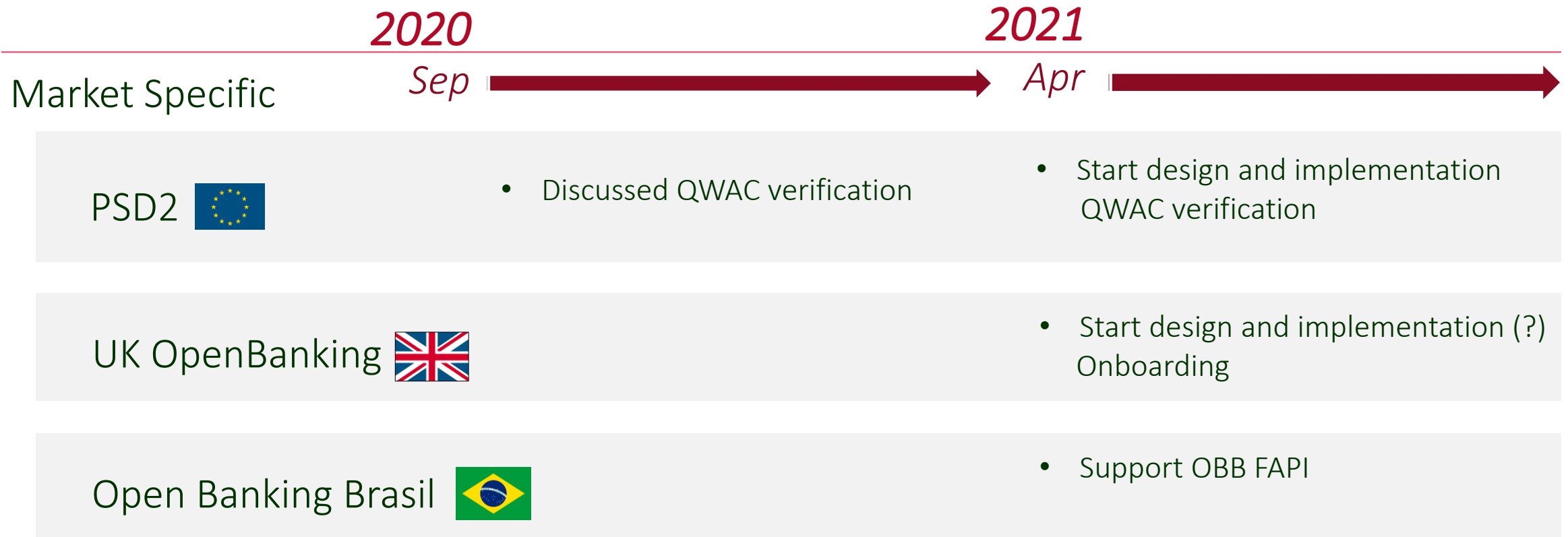
- Software Statement Support
- Software Statement Assertion (SSA) Verification



Roadmap



Roadmap



END