FAPI-SIG Community 21st Meeting

@Web Conference

23 Jun 2021

PROPOSED DRAFT

Table of Contents

Major Topics

Status Updates from 20th Meeting

Discussion :

Support security profiles beyond FAPI 1.0, which and how?

Proposal :

Apply for CfP to Devconf.cz 2022 as FAPI-SIG

Working Items Status

Major Topics

Major Topics

- keycloak

  Keycloak 14 has been released.

- FAPI 1.0

  Keycloak 14 officially supported FAPI 1.0 Baseline/Advanced support as default client profile.

  FAPI-SIG's automated conformance test run environment provided FAPI1 Advanced Final conformance tests against keycloak 14 as default.

- FAPI 2.0

  [PAR]

  PR sent, waiting for its review.

  [RAR]

  [Grant Management]

- FAPI-CIBA

Major Topics

- FAPI-JARM

  PR sent, waiting for its review.

- Common Security Features
- Client Policies

  Keycloak 14 officially supported Client Policies.

- SPA/Native App
- PSD2

Status Updates from 20th Meeting
Common Security Features

OIDC Client’s Public Key Management

Wait for Review Phase-2/4 Allow to register client public key for ECDSA/RSASSA-PSS

🔥 KEYCLOAK-18341 Support JWKS OAuth2 Client Metadata in the "by value" key loading method

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18341

GH PR: https://github.com/keycloak/keycloak/pull/7874

GH PR: https://github.com/keycloak/keycloak-documentation/pull/1195

Spec: https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/OIDC-Client-Keys/FAPI-SIG-Annex_OIDC_Client_Keys.pdf

Status Updates from 20th Meeting
FAPI 1.0

FAPI as default client profile

Keycloak 14 has been released that officially support Client Policies and its FAPI 2.0 Baseline and Advanced security profile as default client profile.

https://www.keycloak.org/2021/06/keycloak-1400-released.html

Status Updates from 20th Meeting
FAPI 2.0

Components of FAPI 2.0 Advanced

In Progress OAuth 2.0 Pushed Authorization Requests (PAR)

🔥 KEYCLOAK-18353 Implement Pushed Authorization Request inside the Keycloak

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18353

GH PR: https://github.com/keycloak/keycloak/pull/8144

Components of FAPI 2.0 Advanced

In Progress OAuth 2.0 Rich Authorization Requests (RAR)

- Design Document : https://github.com/keycloak/keycloak-community/pull/266
- Implementation : (WIP) https://github.com/tnorimat/keycloak/pull/24

In Progress Grant Management for OAuth 2.0

- Design Document : https://github.com/keycloak/keycloak-community/pull/265
- Implementation : (WIP) https://github.com/tnorimat/keycloak/pull/23

Status Updates from 20th Meeting FAPI-CIBA

Upstreaming CIBA Support

[Features]

In Progress Support signed authentication request

🔥 KEYCLOAK-17936 FAPI-CIBA : support Signed Authentication Request

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-17936

GH PR: https://github.com/keycloak/keycloak/pull/8006

etc ...

[Conformance tests]

In Progress Pass conformance test for ID1

🔥 #65 FAPI-CIBA Conformance Test : Establish the way of running FAPI-CIBA OP poll w/ MTLS and w/ Private Key against CIBA Implementation

GH Issue: https://github.com/keycloak/kc-sig-fapi/issues/65

Status Updates from 20th Meeting SPA/Native App

Holder-of-Key Bound Token in SPA/Native App

In Progress OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)

🔥 Design Document : https://github.com/keycloak/keycloak-community/pull/254

- Implementation

Status Updates from 20th Meeting
Market Specific Features – PSD2

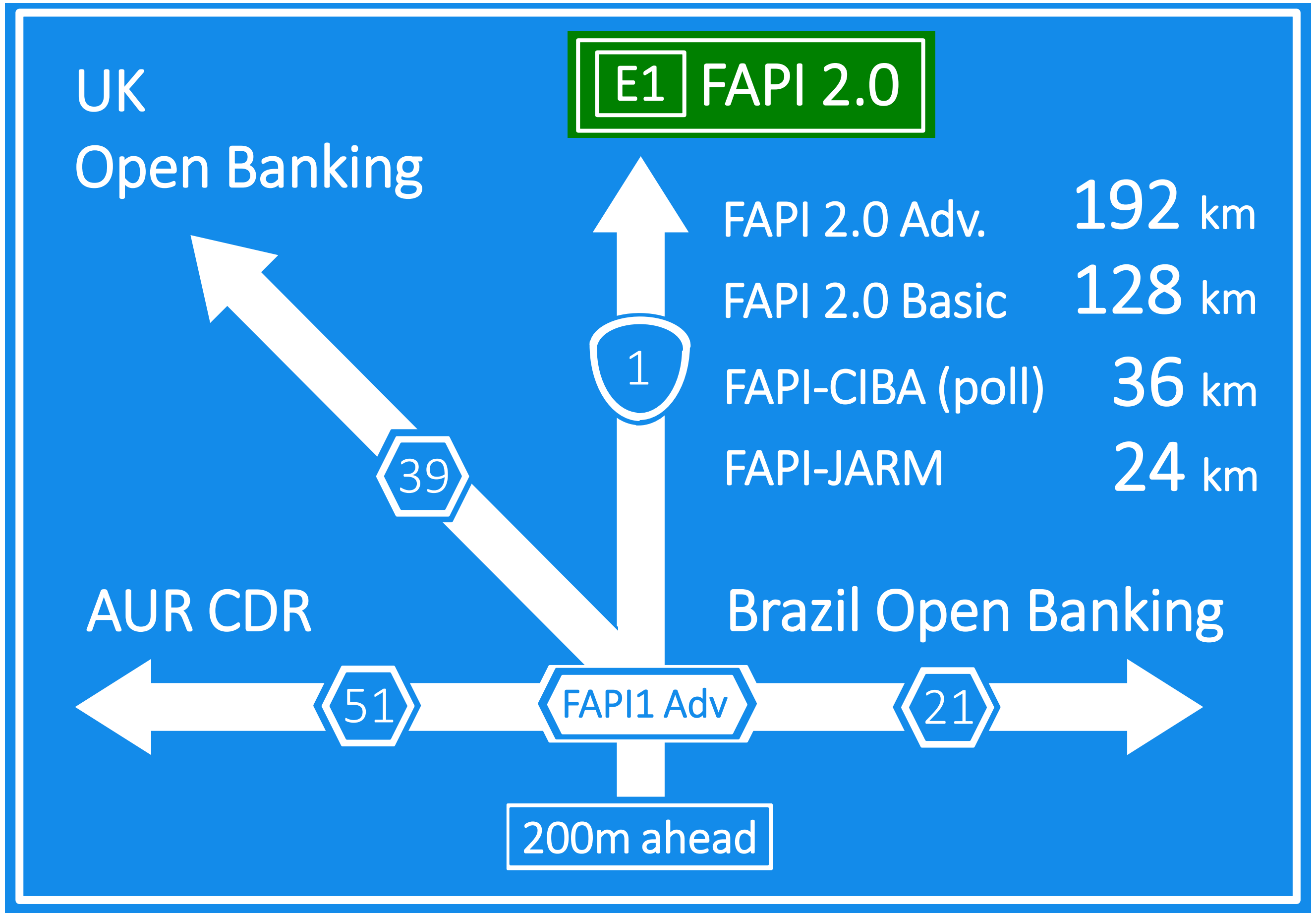
QWACS Verification et al.

In Progress MTLS Validation Extension (MTLS_Ext)

- Design Document : https://github.com/keycloak/keycloak-community/pull/267
- Implementation : (WIP) https://github.com/tnorimat/keycloak/pull/21

Discussion : Support security profiles beyond FAPI 1.0, which and how?

Which security profiles to be supported



After keycloak supporting FAPI 1.0, how and which we try to support other security profiles next?

PROPOSED DRAFT

Current status : FAPI related security profiles

#	Security Profile Specification	Conformance Profile of Certified OpenID Provider	Conformance Test Plan	Keycloak's Status
1	FAPI 1.0 Baseline	-	-	Completed
2	FAPI 1.0 Advanced	FAPI Adv. OP w/ MTLS FAPI Adv. OP w/ Private Key	FAPI1-Advanced-Final	Completed
3	FAPI 1.0 Advanced (PAR)	FAPI Adv. OP w/ MTLS, PAR FAPI Adv. OP w/ Private Key, PAR	FAPI1-Advanced-Final	In Progress
4	FAPI 1.0 JARM	FAPI Adv. OP w/ MTLS FAPI Adv. OP w/ Private Key	FAPI1-Advanced-Final	In Progress
5	FAPI 1.0 CIBA (poll)	FAPI-CIBA OP poll w/ MTLS FAPI-CIBA OP poll w/ Private Key	FAPI-CIBA-ID1	In Progress
6	FAPI 1.0 CIBA (ping)	FAPI-CIBA OP Ping w/ MTLS FAPI-CIBA OP Ping w/ Private Key	FAPI-CIBA-ID1	Not Yet
7	FAPI 2.0 Baseline	-	-	In Progress
8	FAPI 2.0 Advanced	-	-	Not Yet

In Progress : some PR sent or being created that can be used to support this security profile.

PROPOSED DRAFT

Current status : FAPI related security profiles

#	Security Profile Specification	Conformance Profile of Certified OpenID Provider	Conformance Test Plan	Keycloak's Status
9	UK Open Banking	UK-OB Adv. OP w/ MTLS UK-OB Adv. OP w/ Private Key	FAPI1-Advanced-Final	Not Yet
10	Australia CDR	AU-CDR Adv. OP w/ Private Key	FAPI1-Advanced-Final	Not Yet
11	Australia CDR (PAR)	AU-CDR Adv. OP w/ Private Key, PAR	FAPI1-Advanced-Final	Not Yet
12	Brazil Open Banking	-	FAPI1-Advanced-Final	Not Yet

Current status : FAPI-CIBA (poll)

#	Security Profile Specification	Conformance Profile of Certified OpenID Provider	Conformance Test Plan	Keycloak's Status
5	FAPI 1.0 CIBA (poll)	FAPI-CIBA OP poll w/ MTLS FAPI-CIBA OP poll w/ Private Key	FAPI-CIBA-ID1	In Progress

In Progress Support signed authentication request

KEYCLOAK-17936 FAPI-CIBA : support Signed Authentication Request

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-17936

GH PR: https://github.com/keycloak/keycloak/pull/8006

and more needed ...

Current status : FAPI-JARM

#	Security Profile Specification	Conformance Profile of Certified OpenID Provider	Conformance Test Plan	Keycloak's Status
4	FAPI 1.0 JARM	FAPI Adv. OP w/ MTLS FAPI Adv. OP w/ Private Key	FAPI1-Advanced-Final	In Progress

In Progress Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0

KEYCLOAK-18452 FAPI JARM: JWT Secured Authorization Response Mode for OAuth 2.0

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18452

GH PR: https://github.com/keycloak/keycloak/pull/8158

Current status : FAPI 1.0 Advanced (PAR) / FAPI 2.0 Baseline

#	Security Profile Specification	Conformance Profile of Certified OpenID Provider	Conformance Test Plan	Keycloak's Status
3	FAPI 1.0 Advanced (PAR)	FAPI Adv. OP w/ MTLS, PAR FAPI Adv. OP w/ Private Key, PAR	FAPI1-Advanced-Final	In Progress
7	FAPI 2.0 Baseline	-	-	In Progress

In Progress OAuth 2.0 Pushed Authorization Requests (PAR)

KEYCLOAK-18353 Implement Pushed Authorization Request inside the Keycloak

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18353

GH PR: https://github.com/keycloak/keycloak/pull/8144

Proposal : Apply for CfP to Devconf.cz 2022 as FAPI-SIG

Presentation in DevConf.cz 2022

How about presenting our activities and achievements
to OSS developer’s community?

- FAPI-SIG’s activity and its contribution to keycloak
- Actual use cases of keycloak using FAPI

DevConf.cz :

https://www.devconf.info/cz/

Annual OSS developers event held in Feb on Brno, Czech Republic.

https://devconfcz2021.sched.com/

https://www.youtube.com/playlist?list=PLU1vS0speL2YQ9WXMnY-glVErAIsTsSAl

https://devconfcz2020a.sched.com/

https://www.youtube.com/playlist?list=PLU1vS0speL2Z08BeKSwSqfxPEl3ta5UK3

PROPOSED DRAFT

Working Items Status

Working Items

[Security Features]

<Common>

In Progress OIDC Client’s Public Key Management Hitachi

1st phase -> 2nd phase

[Security Features]

<High Level Security>

● FAPI-JARM

New In Progress PR sent, waiting for its review.

Working Items

[Security Features]

<High Level Security>

- FAPI 2.0 (baseline/advanced)

In Progress Pushed Authorization Request (PAR) — Adorsys, Hitachi

New
- PR sent, waiting for its review.

In Progress Rich Authorization Request (RAR) — Adorsys

In Progress Grant Management API — Adorsys

- FAPI-CIBA

In Progress FAPI-CIBA : Signed Authentication — Hitachi, Banfico

In Progress Passing conformance tests for ID1 — Banfico, Hitachi

<SPA/Native App>

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

Working Items

[Market Specific Features]

<PSD2>

- Following eIDAS regulations

In Progress QWAC verification

Adorsys

- Consent Management

<UK OpenBanking>

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

Roadmap

Security	2020 Sep	2021 Apr
Common Client Policies	• Implemented as Preview • New Admin REST API support	• Migrate Client Registration Policy • Move Preview to Official Support -> leads to FAPI 1.0 Official Support
High Level Security		
FAPI 1.0	• Supported ID2 ver • Passed ID2 conformance test	• Support Final ver • Pass Final ver conformance test
FAPI 2.0		• Start design and implementation PAR, RAR, Grant Management API
FAPI-CIBA	• Supported Pure CIBA (poll mode) as Preview	• Support FAPI-CIBA (poll mode) • Pass conformance test
SPA/Native App DPoP		• Start design and implementation

PROPOSED DRAFT

Roadmap

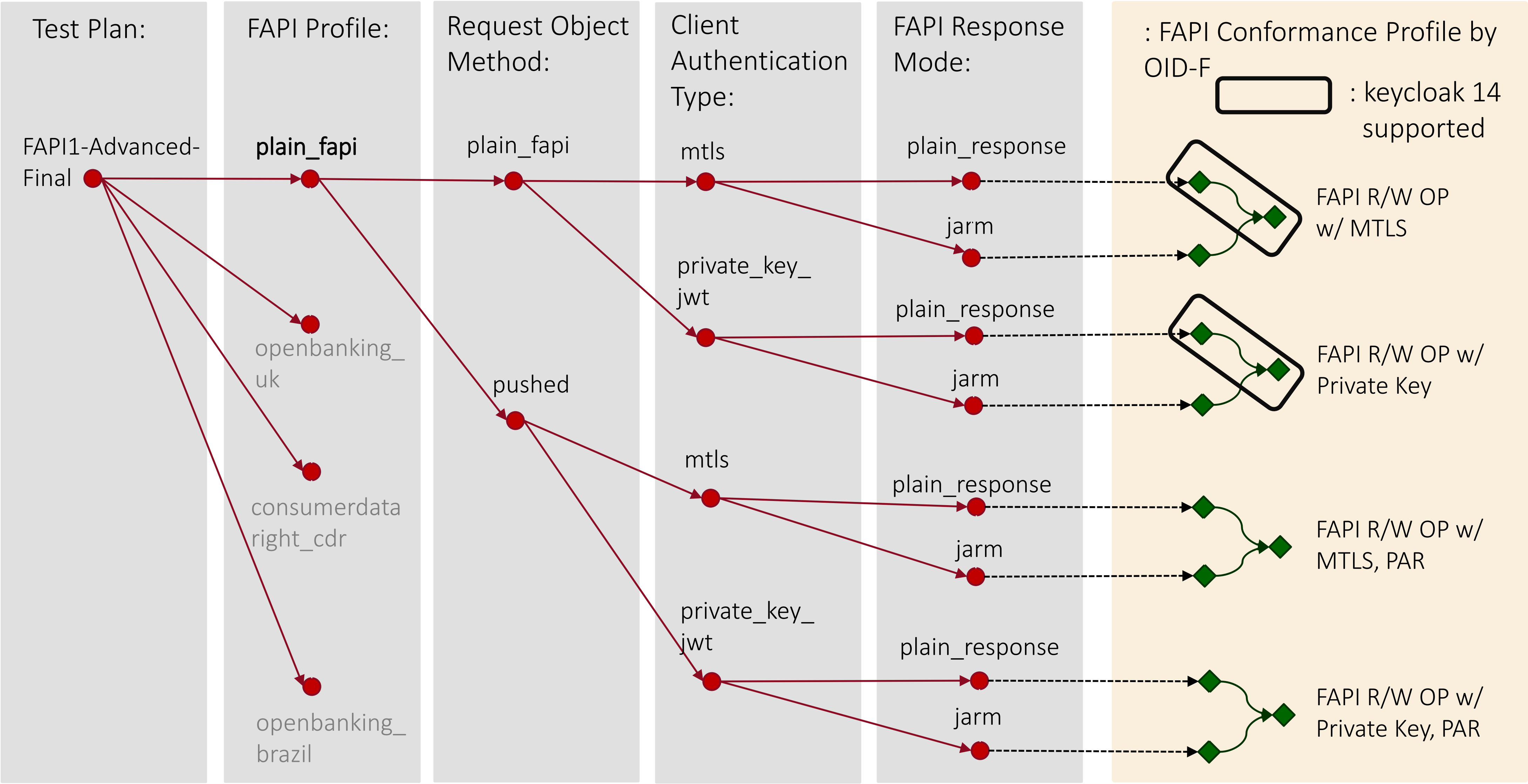
Market Specific	2020 Sep	2021 Apr
PSD2	- Discussed QWAC verification	- Start design and implementation QWAC verification
UK OpenBanking		- Start design and implementation (?) Onboarding

Appendix

Conformance suite test plan vs FAPI conformance profile

FAPI1 Advanced Final : Plain FAPI

conformance-suite ver : release-4.1.12



Test Plan:

FAPI1-Advanced-Final

FAPI Profile:

plain_fapi

openbanking_uk

consumerdataright_cdr

openbanking_brazil

Request Object Method:

plain_fapi

pushed

Client Authentication Type:

mtls

private_key_jwt

mtls

private_key_jwt

FAPI Response Mode:

plain_response

jarm

plain_response

jarm

plain_response

jarm

plain_response

jarm

: FAPI Conformance Profile by OID-F

: keycloak 14 supported

FAPI R/W OP w/ MTLS

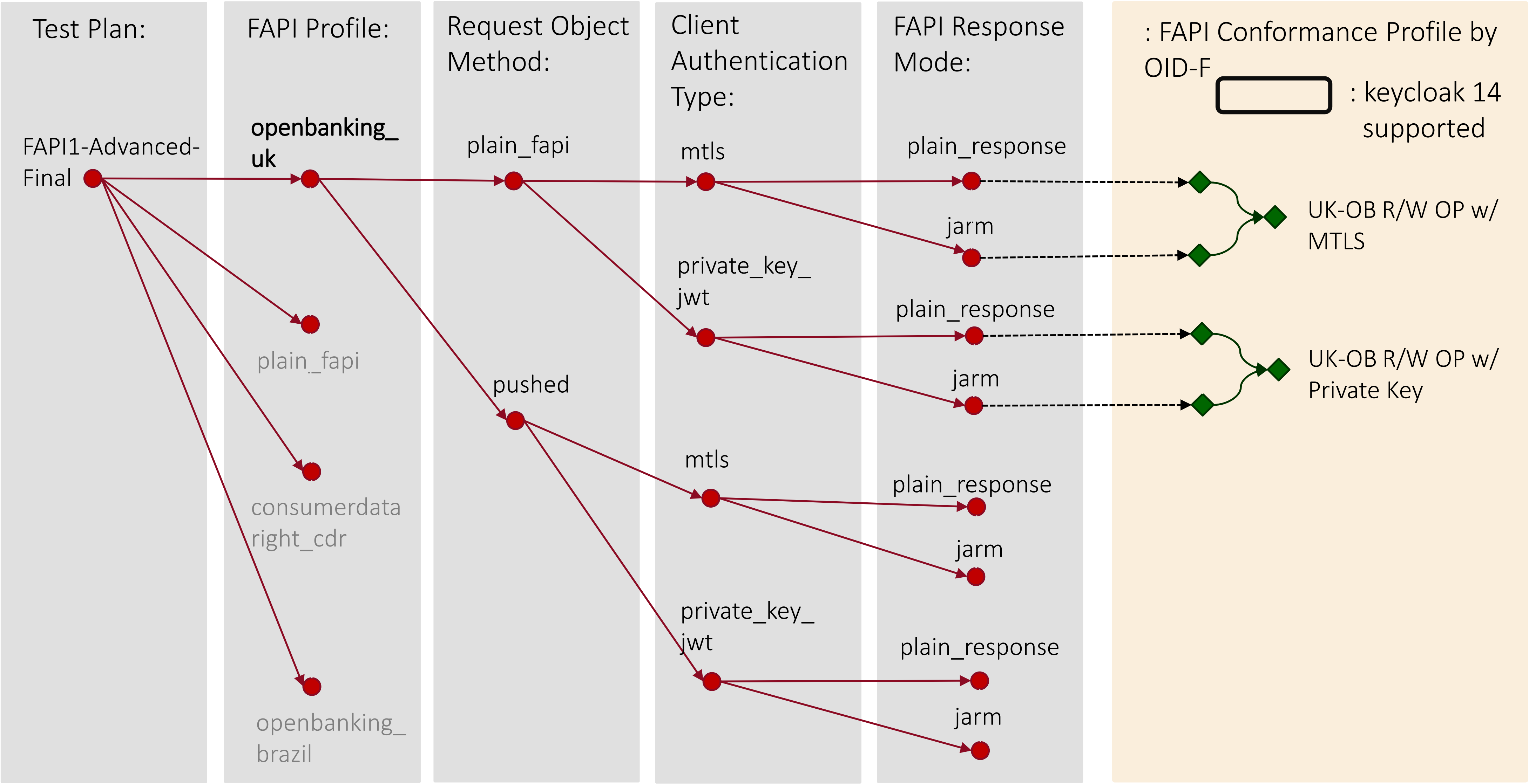
FAPI R/W OP w/ Private Key

FAPI R/W OP w/ MTLS, PAR

FAPI R/W OP w/ Private Key, PAR

FAPI1 Advanced Final : OpenBanking UK

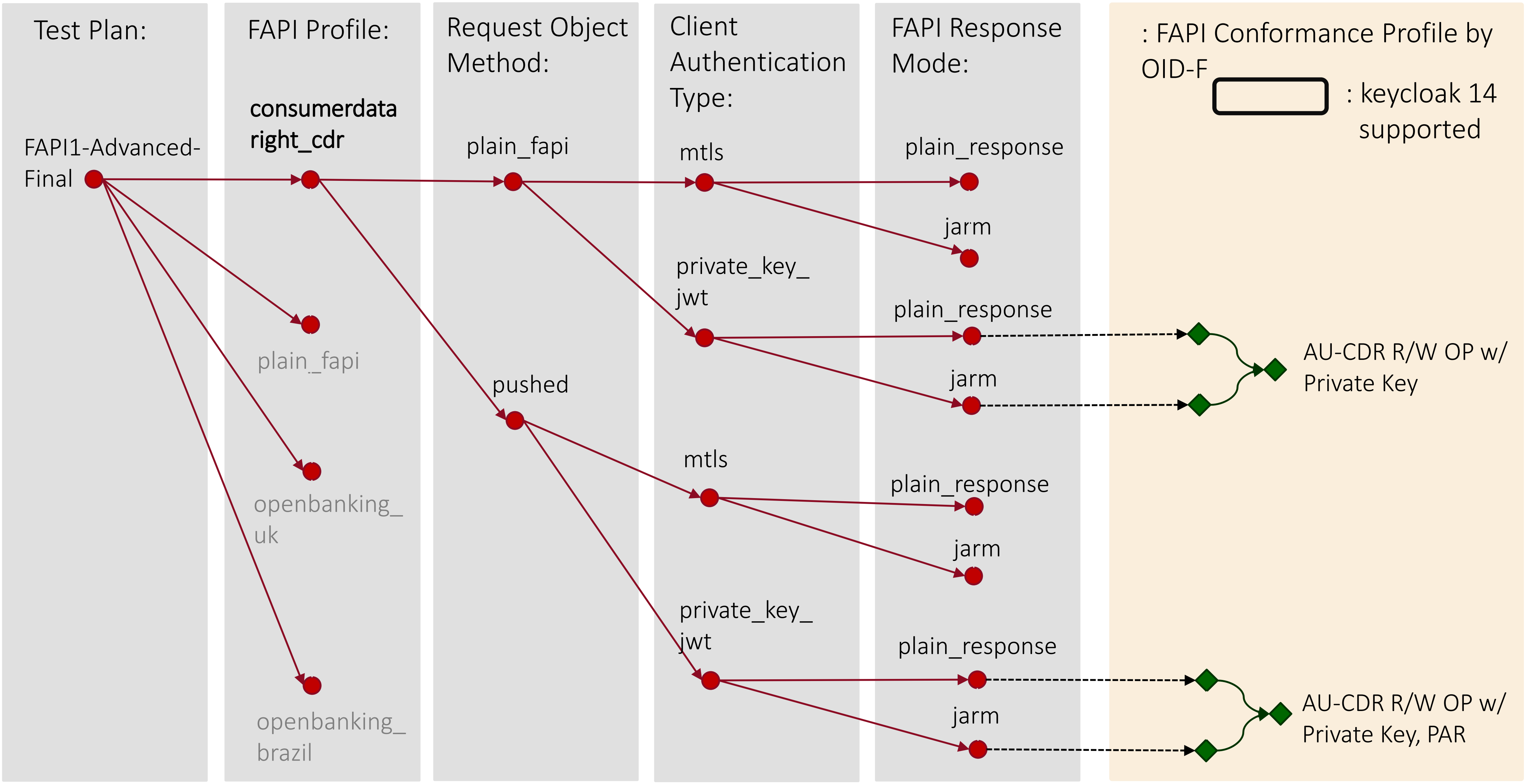
conformance-suite ver : release-4.1.12



PROPOSED DRAFT

FAPI1 Advanced Final : Consumer Data Right Australia

conformance-suite ver : release-4.1.12



Test Plan:

FAPI1-Advanced-Final

FAPI Profile:

consumerdata right_cdr

plain_fapi

openbanking_uk

openbanking_brazil

Request Object Method:

plain_fapi

pushed

Client Authentication Type:

mtls

private_key_jwt

mtls

private_key_jwt

FAPI Response Mode:

plain_response

jarm

plain_response

jarm

plain_response

jarm

plain_response

jarm

: FAPI Conformance Profile by OID-F

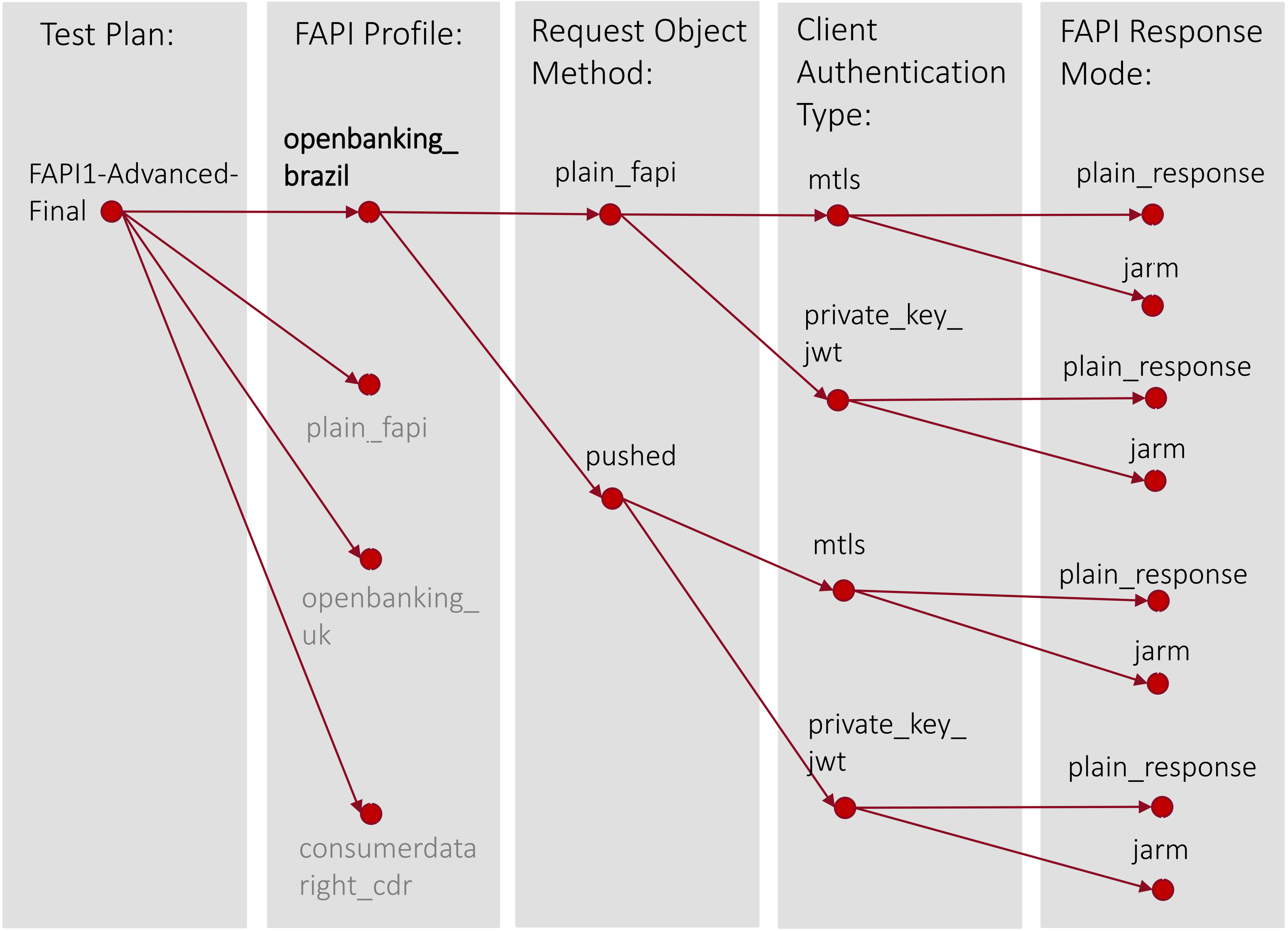
: keycloak 14 supported

AU-CDR R/W OP w/ Private Key

AU-CDR R/W OP w/ Private Key, PAR

FAPI1 Advanced Final : OpenBanking Brazil

conformance-suite ver : release-4.1.12



Test Plan:

FAPI1-Advanced-Final

FAPI Profile:

openbanking_brazil

plain_fapi

openbanking_uk

consumerdataright_cdr

Request Object Method:

plain_fapi

pushed

Client Authentication Type:

mtls

private_key_jwt

mtls

private_key_jwt

FAPI Response Mode:

plain_response

jarm

plain_response

jarm

plain_response

jarm

plain_response

jarm

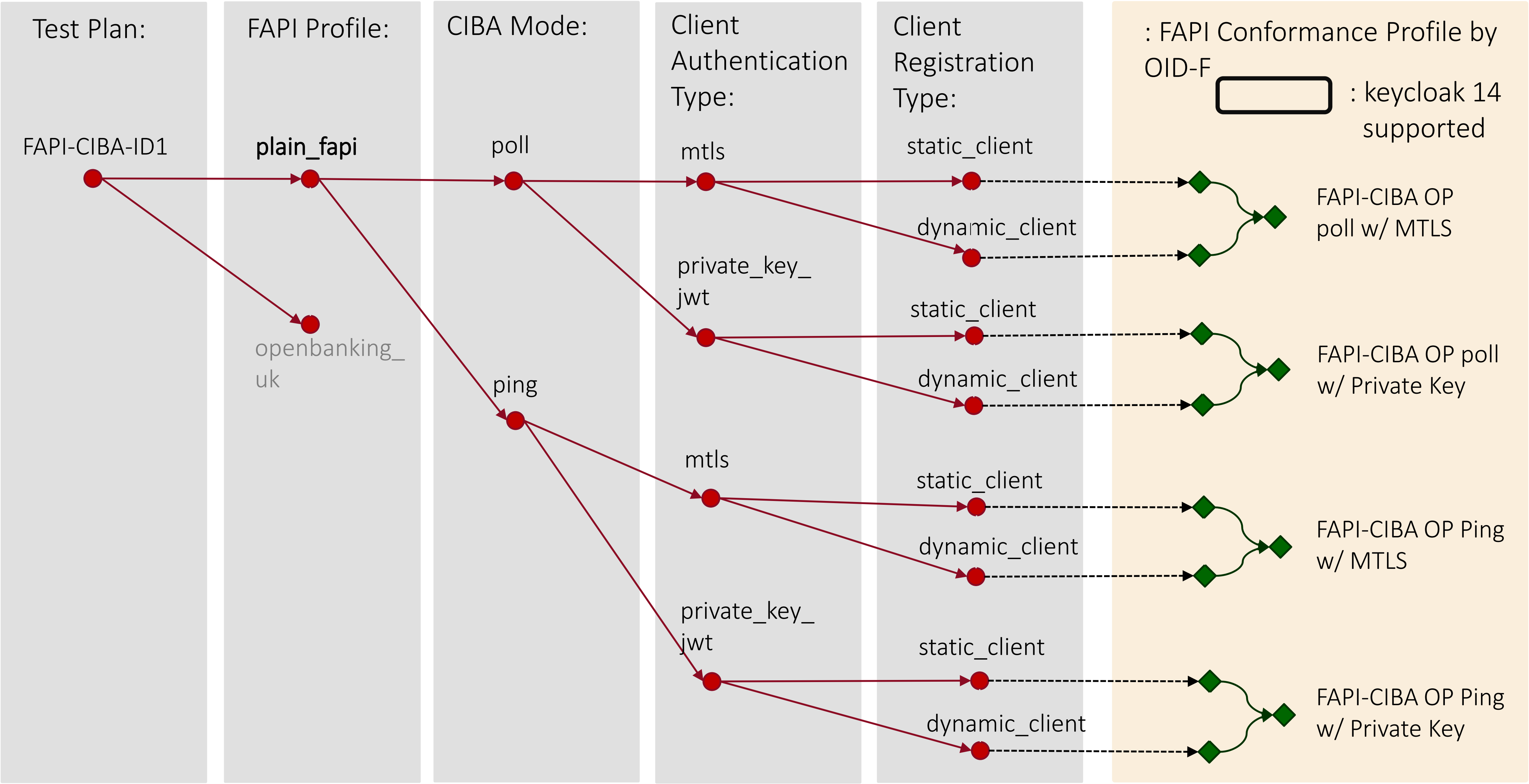
: FAPI Conformance Profile by OID-F

□ : keycloak 14 supported

PROPOSED DRAFT

FAPI CIBA ID1 : Plain FAPI

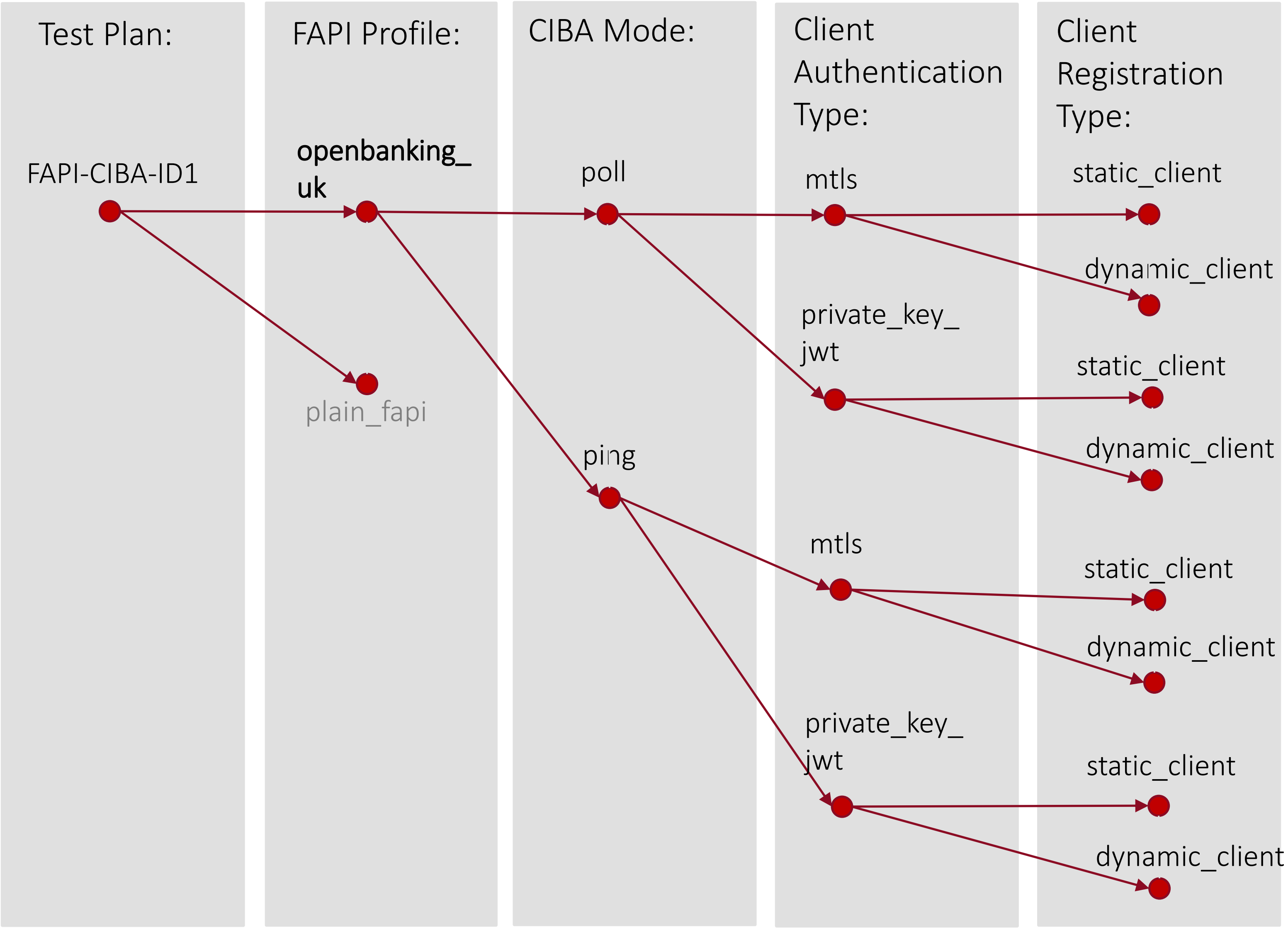
conformance-suite ver : release-4.1.12



PROPOSED DRAFT

FAPI CIBA ID1 : OpenBanking UK

conformance-suite ver : release-4.1.12



: FAPI Conformance Profile by OID-F

□ : keycloak 14 supported

PROPOSED DRAFT

Proposals for Supporting FAPI conformance profiles

FAPI conformance Profile by OID-F

Specification: https://standards.openbanking.org.uk/security-profiles/

- Financial Grade API (FAPI) Security Profile

  [Specification]

  same as FAPI 1.0 Advanced Security Profile.

  [Conformance Test]

  Test Plan :

  FAPI1-Advanced-Final: Authorization server test

  FAPI Profile :

  openbanking_uk

  [FAPI Conformance Profile (Certificate)]

  UK-OB R/W OP w/ MTLS

  UK-OB R/W OP w/ Private Key

  [Contribution]

  No contribution ongoing

- CIBA Profile

  [Specification]

  same as FAPI CIBA Security Profile.

  [Conformance Test]

  Test Plan :

  FAPI-CIBA-ID1: Authorization server test

  FAPI Profile :

  openbanking_uk

  [FAPI Conformance Profile (Certificate)]

  Nothing

  [Contribution]

  No contribution ongoing

UK OpenBanking Security Profile

Specification: https://standards.openbanking.org.uk/security-profiles/

- Financial Grade API (FAPI) Security Profile

  [Specification]

  same as FAPI 1.0 Advanced Security Profile.

  [Conformance Test]

  Test Plan :

  FAPI1-Advanced-Final: Authorization server test

  FAPI Profile :

  openbanking_uk

  [FAPI Conformance Profile (Certificate)]

  UK-OB R/W OP w/ MTLS

  UK-OB R/W OP w/ Private Key

  [Contribution]

  No contribution ongoing

- CIBA Profile

  [Specification]

  same as FAPI CIBA Security Profile.

  [Conformance Test]

  Test Plan :

  FAPI-CIBA-ID1: Authorization server test

  FAPI Profile :

  openbanking_uk

  [FAPI Conformance Profile (Certificate)]

  Nothing

  [Contribution]

  No contribution ongoing

Open Banking Brazil Financial-grade API Security Profile

[Specification]

https://openbanking-brasil.github.io/specs-seguranca/open-banking-brasil-financial-api-1_ID1.html

Based on FAPI 1.0 Security Profile.

[Conformance Test]

Test Plan : FAPI1-Advanced-Final: Authorization server test

FAPI Profile : openbanking_brazil

[FAPI Conformance Profile (Certificate)]

Nothing

[Contribution]

PR sent for FAPI-JARM that is required by Open Banking Brazil.

In Progress Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0

🔥 KEYCLOAK-18452 FAPI JARM: JWT Secured Authorization Response Mode for OAuth 2.0

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18452

GH PR: https://github.com/keycloak/keycloak/pull/8158

FAPI 1.0 + PAR

[Specification]

https://openid.net/specs/openid-financial-api-part-2-1_0.html : **5.2.2.18**

[Conformance Test]

Test Plan : FAPI1-Advanced-Final: Authorization server test

FAPI Profile : plain_fapi

[FAPI Conformance Profile (Certificate)]

FAPI R/W OP w/ MTLS, PAR

FAPI R/W OP w/ Private Key, PAR

[Contribution]

PR sent for PAR.

In Progress OAuth 2.0 Pushed Authorization Requests (PAR)

🔥 KEYCLOAK-18353 Implement Pushed Authorization Request inside the Keycloak

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18353

GH PR: https://github.com/keycloak/keycloak/pull/8144

END