OpenID Foundation
FAPI WG & Certification Program
Overview for CAMARA

December 20, 2023

OpenID®

Introduction to FAPI

Nat Sakimura
OpenID Foundation Chairman & FAPI WG Co-Chair

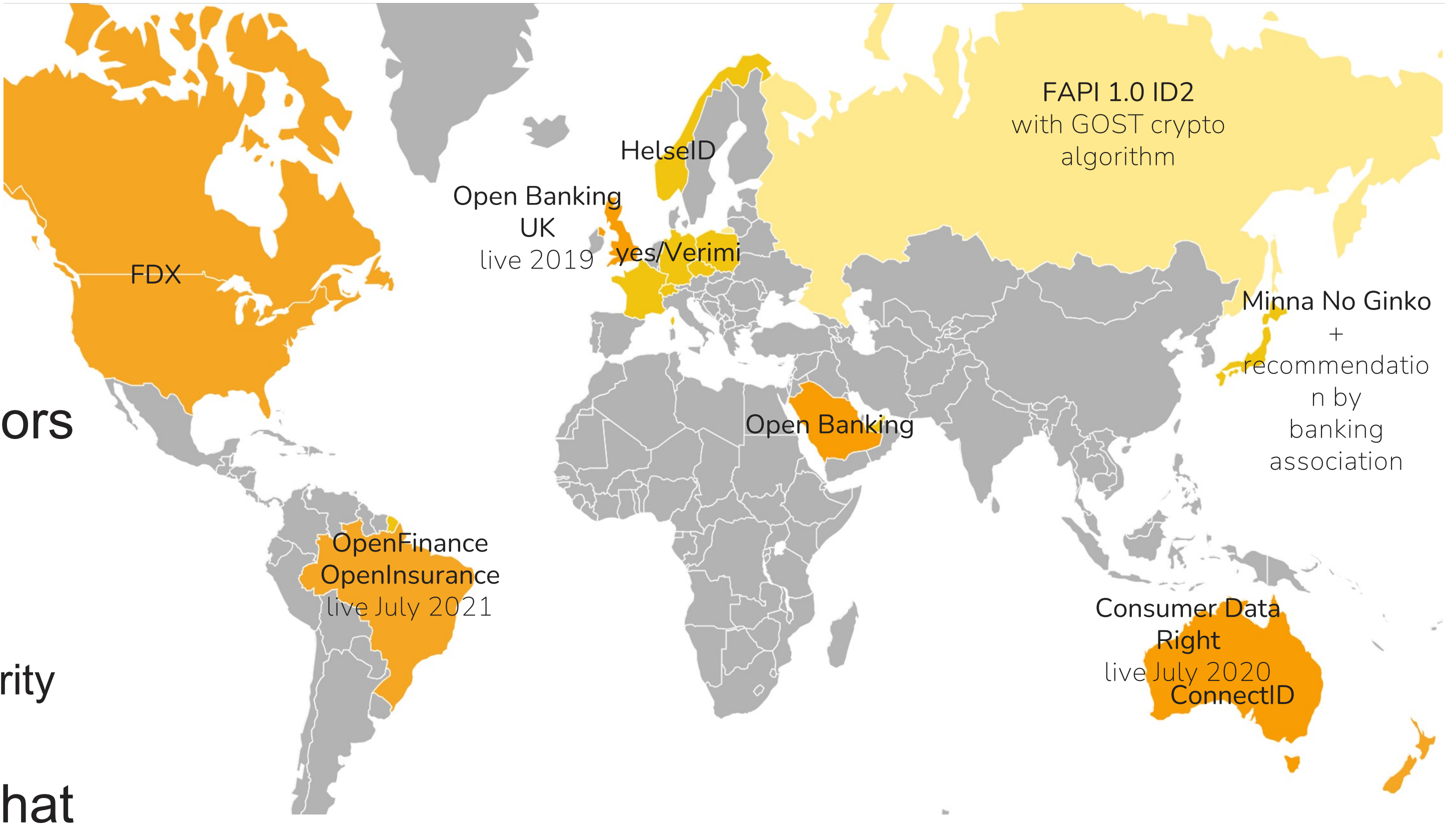
Working Group Overview

Objective of the Working Group

- Create general purpose high-security profiles for OpenID Connect and OAuth

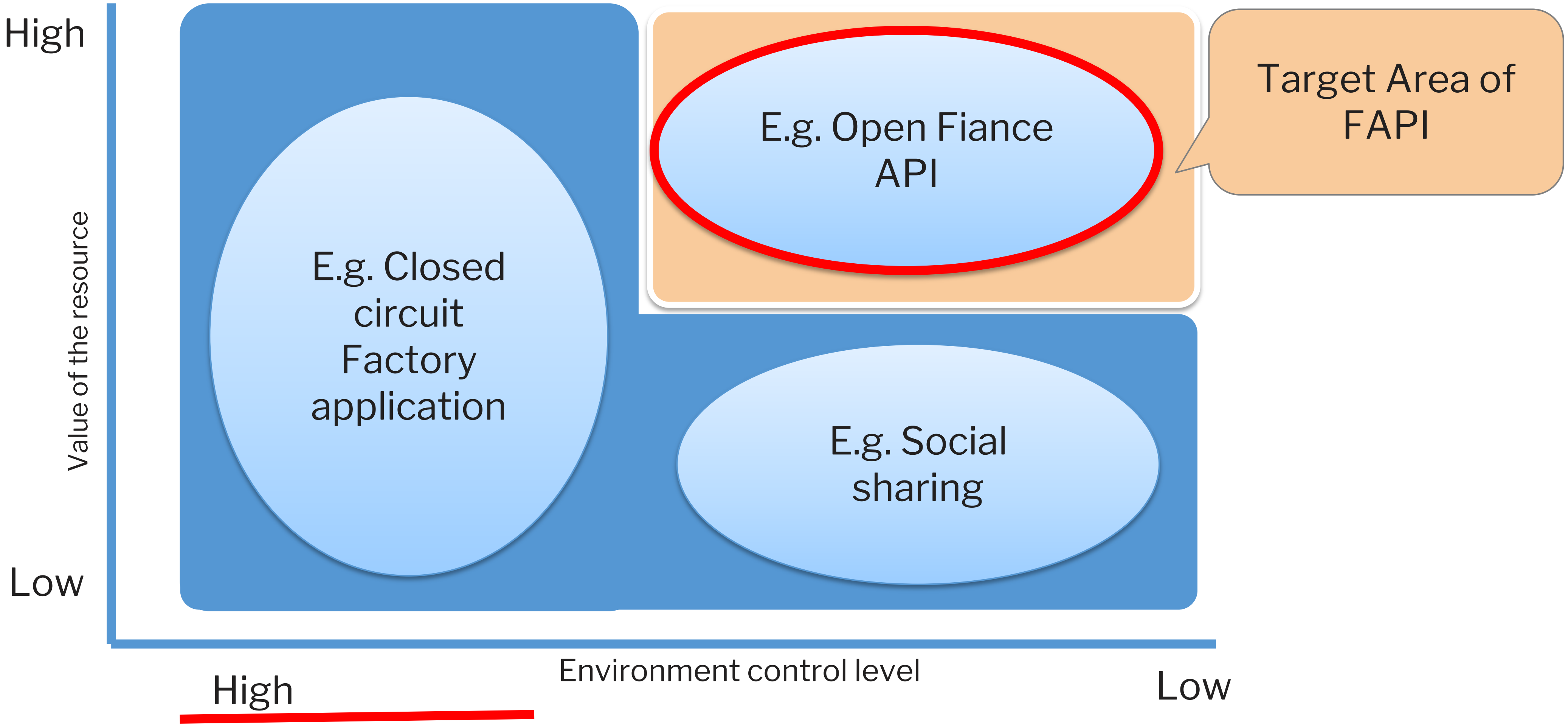
Some notable aspects

- Extensive use of Formal Verification
- Close collaboration with national regulators and associations
  - e.g. Australia, Brazil, UK, FDX, KSA, Canada/US
  - Thanks to Australia sponsoring FAPI2 security analysis!
- Trying to be ISO directive compliant so that translation/adaptation etc. would be easier.
- National level certifications



FDX
Open Banking UK live 2019
HelseID
yes/Verimi
FAPI 1.0 ID2 with GOST crypto algorithm
Minna No Ginko + recommendation by banking association
Open Banking
OpenFinance OpenInsurance live July 2021
Consumer Data Right live July 2020
ConnectID

FAPI is a set of API Securing Specifications targeted at Mid-High risk scenarios



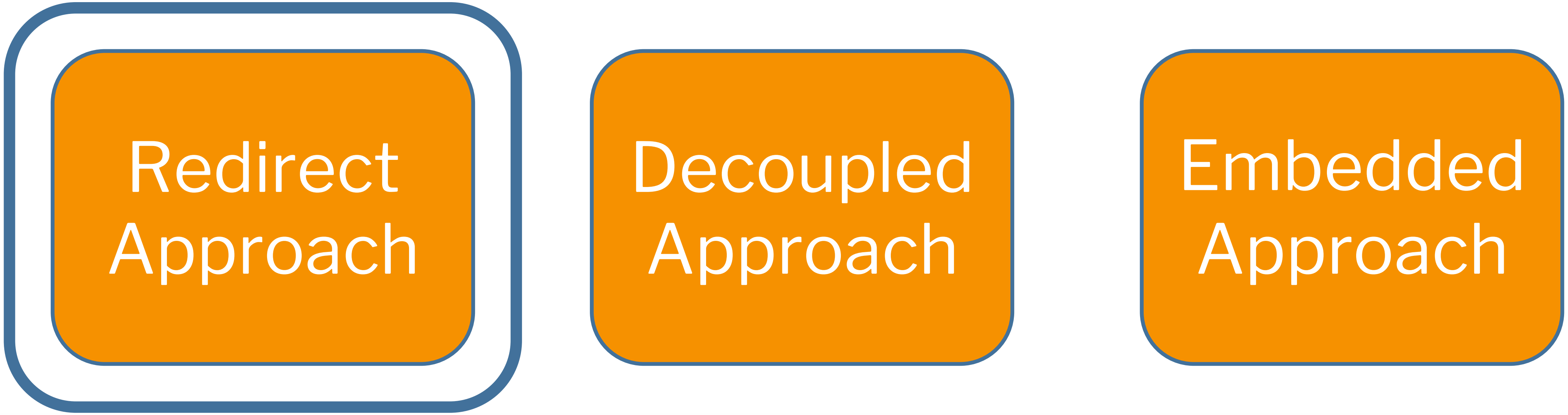
No need to satisfy all the security requirements by OAuth

FAPI 1 – Redirect Approach – FINAL (2021)

Traditional OAuth (RFC6749) Approach where user is redirected to the Authorization Server to provide his grant.

- Part 1: FAPI Security Profile (FAPI) 1.0 – Part 1: Baseline
- Part 2: FAPI Security Profile (FAPI) 1.0 – Part 2: Advanced*

*** Uses JARM**



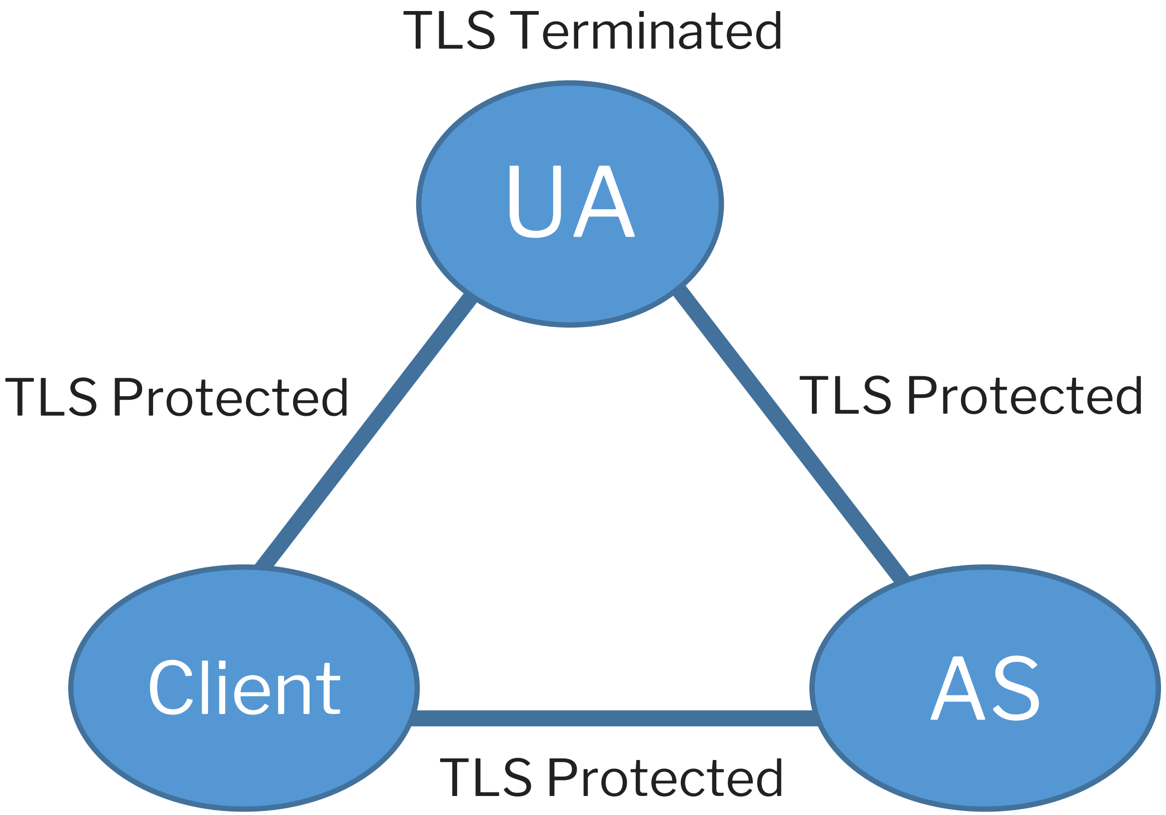
Redirect Approach

Decoupled Approach

Embedded Approach

RFC6749 is not complete with source, destination, and message authentication,

	Sender AuthN	Receiver AuthN	Message AuthN
AuthZ Req	Indirect	None	None
AuthZ Res	None	None	None
Token Req	Weak	Good	Good
Token Res	Good	Good	Good



FAPI Part 2 is complete with source, destination, and message authentication.

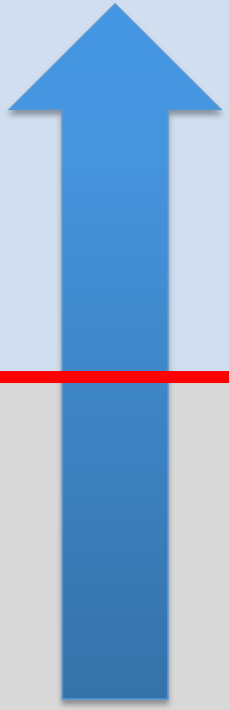
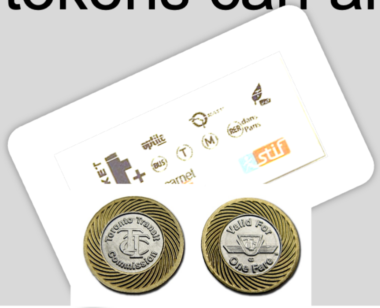
- **Following BCM principles* as the design guidance.**
- **By using OpenID Connect's Hybrid Flow and Request Object, you are pretty well covered.**

	Sender AuthN	Receiver AuthN	Message AuthN
AuthZ Req	Request Object	Request Object	Request object
AuthZ Res	Hybrid Flow/JARM	Hybrid Flow/JARM	Hybrid Flow/JARM
Token Req	Good	Good	Good
Token Res	Good	Good	Good

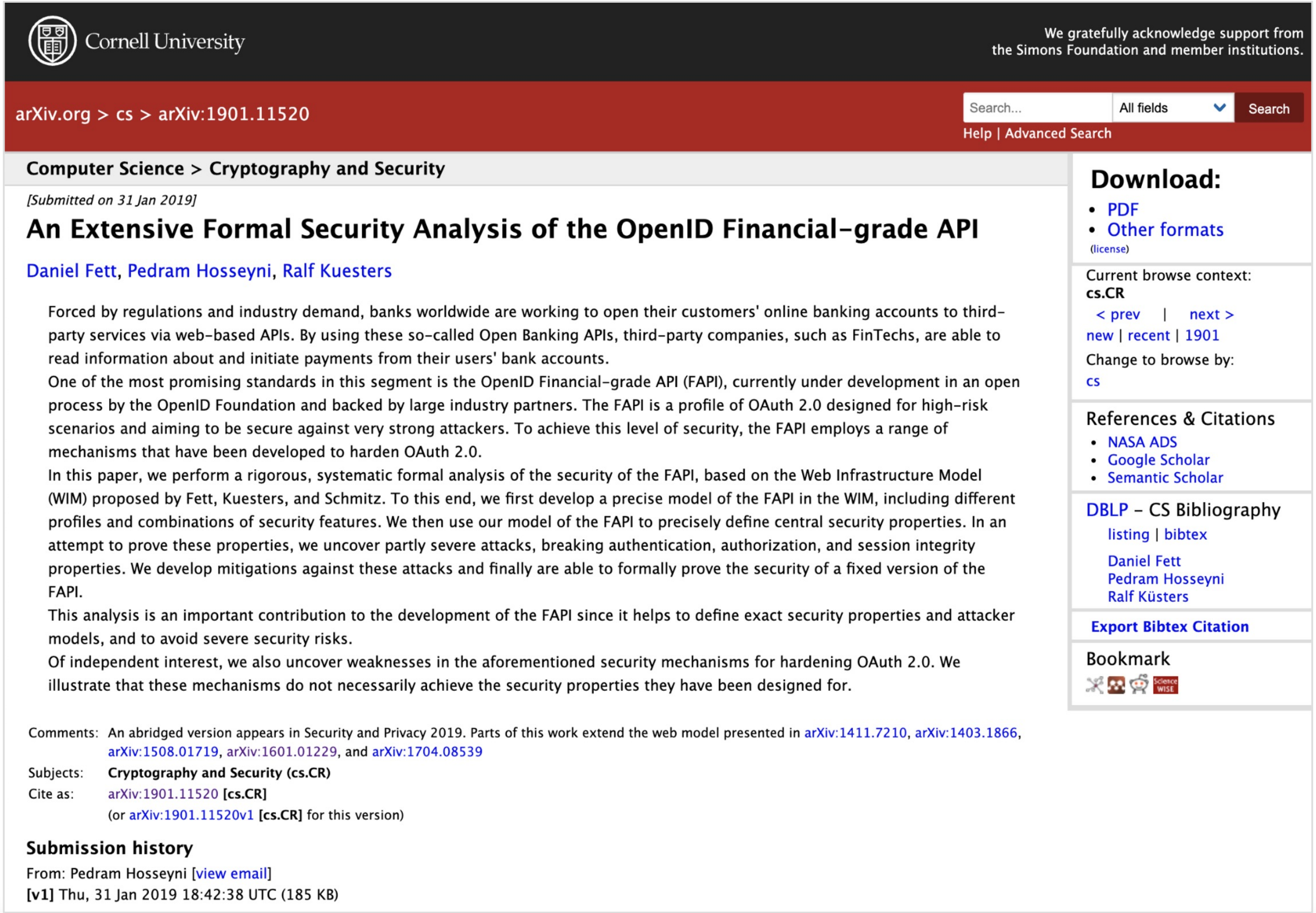
The principles proposed in Basin, D., Cremers, C., Meier, S.: Provably Repairing the ISO/IEC 9798 Standard for Entity Authentication. Journal of Computer Security -Security and Trust Principles archive Volume 21 Issue 6, 817-846 (2013)
https://www.cs.ox.ac.uk/people/cas.cremers/downloads/papers/BCM2012iso9798.pdf

All Tokens are Sender Constrained instead of being bearer

so that even if tokens are intercepted, the user is still protected.

Security Levels	Token Types	Notes
	Sender Constrained Token	Only the entity that was issued can used the token.
	Bearer Token	Stolen tokens can also be used 

Formal Analysis of FAPI 1.0 is completed in 2019 and its security property is well understood


Cornell University
We gratefully acknowledge support from the Simons Foundation and member institutions.
Search...
All fields
Search
Help | Advanced Search

arXiv.org > cs > arXiv:1901.11520

Computer Science > Cryptography and Security

[Submitted on 31 Jan 2019]

An Extensive Formal Security Analysis of the OpenID Financial-grade API

Daniel Fett, Pedram Hosseyni, Ralf Kuesters

Forced by regulations and industry demand, banks worldwide are working to open their customers' online banking accounts to third-party services via web-based APIs. By using these so-called Open Banking APIs, third-party companies, such as FinTechs, are able to read information about and initiate payments from their users' bank accounts.
One of the most promising standards in this segment is the OpenID Financial-grade API (FAPI), currently under development in an open process by the OpenID Foundation and backed by large industry partners. The FAPI is a profile of OAuth 2.0 designed for high-risk scenarios and aiming to be secure against very strong attackers. To achieve this level of security, the FAPI employs a range of mechanisms that have been developed to harden OAuth 2.0.
In this paper, we perform a rigorous, systematic formal analysis of the security of the FAPI, based on the Web Infrastructure Model (WIM) proposed by Fett, Kuesters, and Schmitz. To this end, we first develop a precise model of the FAPI in the WIM, including different profiles and combinations of security features. We then use our model of the FAPI to precisely define central security properties. In an attempt to prove these properties, we uncover partly severe attacks, breaking authentication, authorization, and session integrity properties. We develop mitigations against these attacks and finally are able to formally prove the security of a fixed version of the FAPI.
This analysis is an important contribution to the development of the FAPI since it helps to define exact security properties and attacker models, and to avoid severe security risks.
Of independent interest, we also uncover weaknesses in the aforementioned security mechanisms for hardening OAuth 2.0. We illustrate that these mechanisms do not necessarily achieve the security properties they have been designed for.

Comments: An abridged version appears in Security and Privacy 2019. Parts of this work extend the web model presented in arXiv:1411.7210, arXiv:1403.1866, arXiv:1508.01719, arXiv:1601.01229, and arXiv:1704.08539
Subjects: **Cryptography and Security (cs.CR)**
Cite as: arXiv:1901.11520 **[cs.CR]**
(or arXiv:1901.11520v1 **[cs.CR]** for this version)

Submission history

From: Pedram Hosseyni [view email]
[v1] Thu, 31 Jan 2019 18:42:38 UTC (185 KB)

Download:

- PDF
- Other formats

(license)

Current browse context:
cs.CR
< prev | next >
new | recent | 1901
Change to browse by:
cs

References & Citations

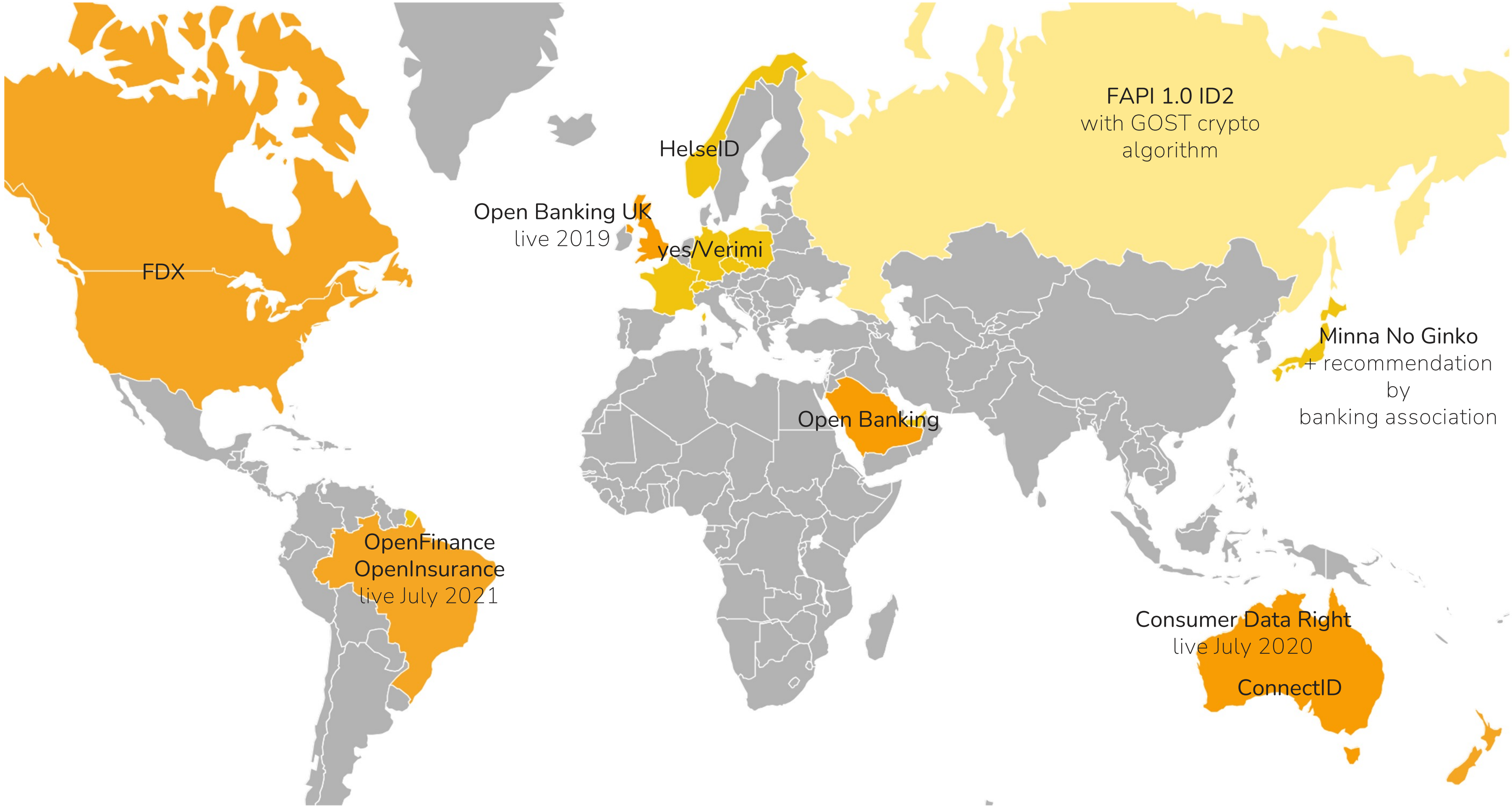
- NASA ADS
- Google Scholar
- Semantic Scholar

DBLP - CS Bibliography
listing | bibtex
Daniel Fett
Pedram Hosseyni
Ralf Küsters

Export Bibtex Citation

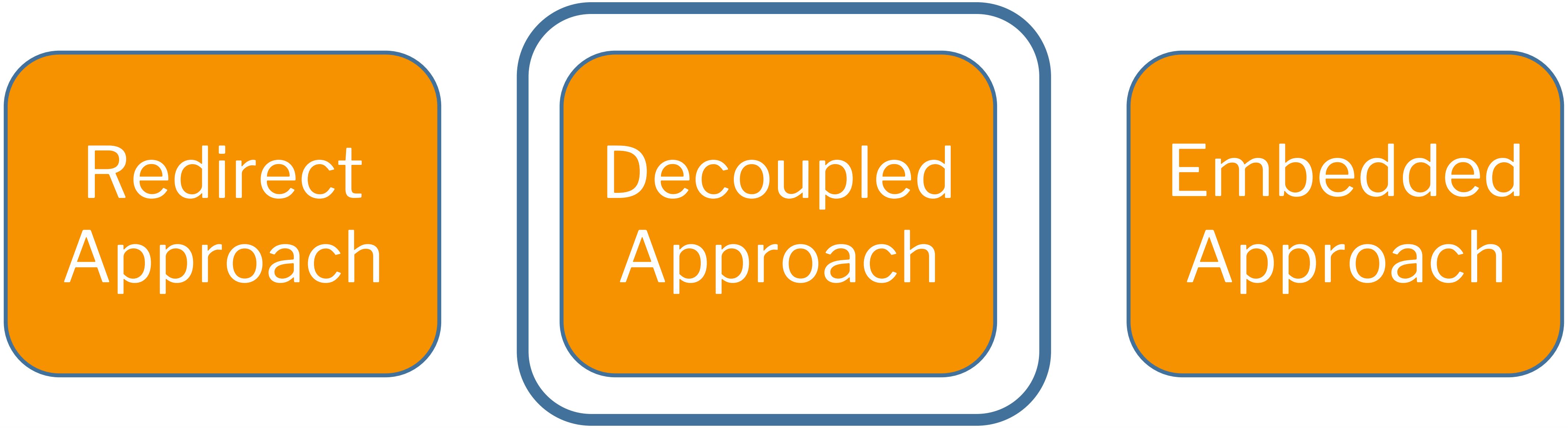
Bookmark

FAPI 1.0 Adoption



FAPI is not complete with only one “Approach”

- FAPI: CIBA Profile
  - A profile of Client Initiated Backchannel Authentication Core Final (2021)



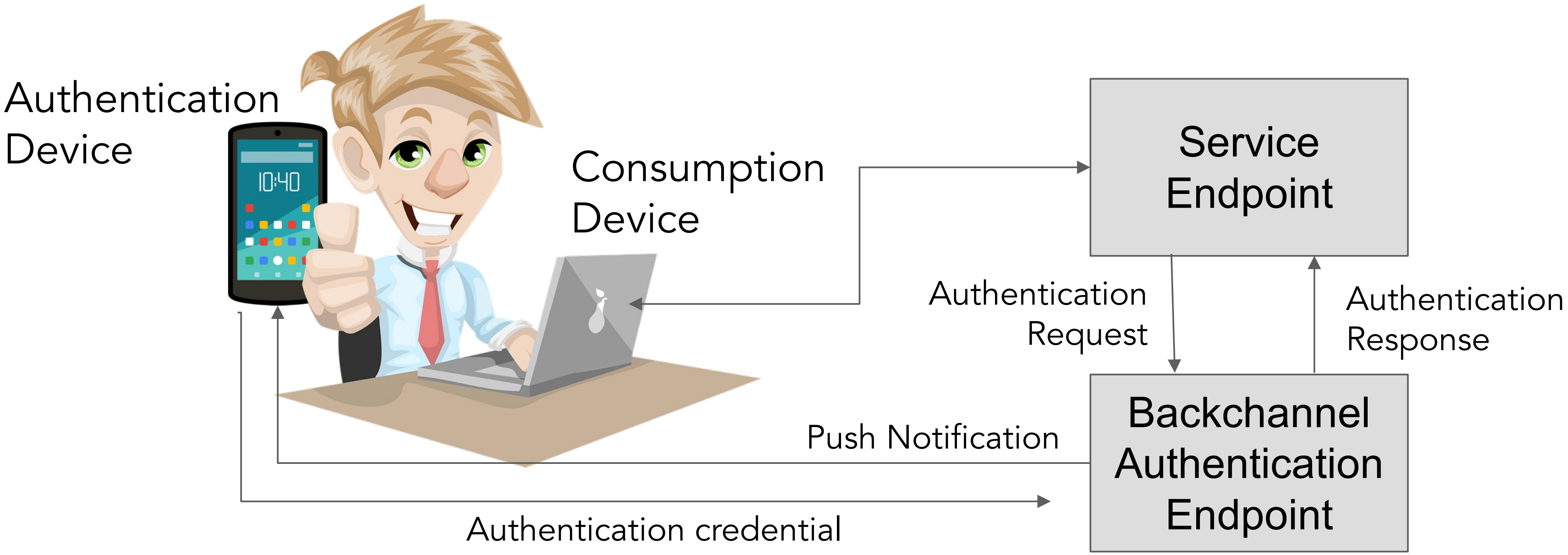
Redirect Approach

Decoupled Approach

Embedded Approach

FAPI: CIBA Profile

- Allows individuals to provide authorization from a second device.
  - ⇒ No need to move out of RP/Service context on the consumption device



Working Group Progress & Opportunities

Published Specifications

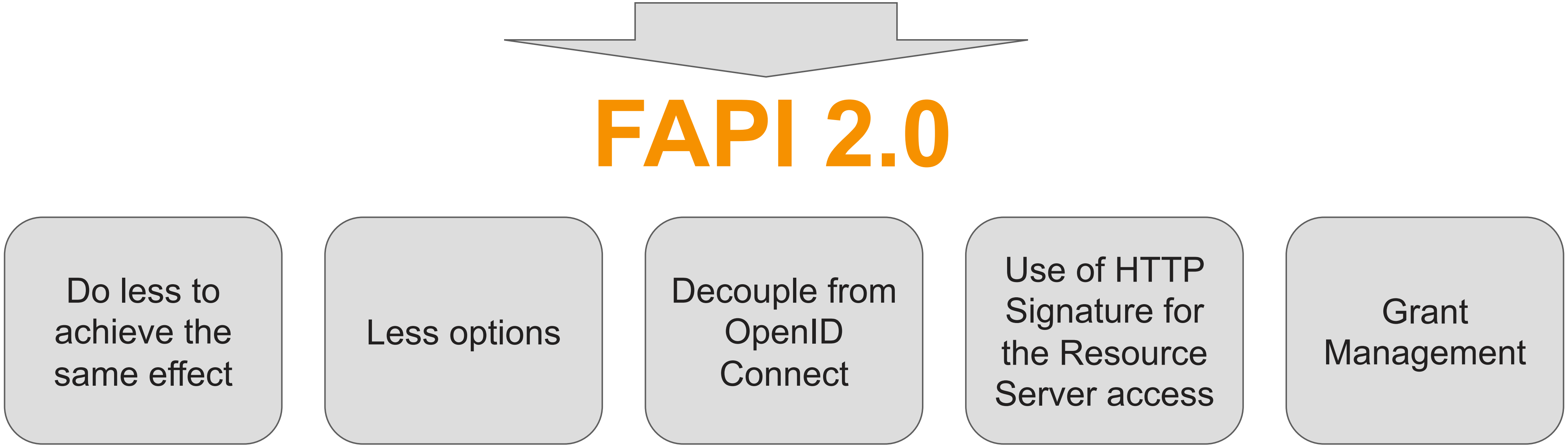
- FAPI Security Profile (FAPI) 1.0 – Part 1: Baseline – A secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability.
- FAPI Security Profile (FAPI) 1.0 – Part 2: Advanced – A highly secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability.
- JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) – This specification was created to bring some of the security features defined as part of OpenID Connect to OAuth 2.0

FAPI 1.0 is complete with Conformance Suites

- It tests not only the functional side but also performs negative tests so that some of the common security problems are spotted automatically.
- Some companies use the conformance suites in their development cycle as well.
- There are base tests as well as regional standards specific profile testings.
  - UK
  - Australia
  - Brasil
- There now are over 800 certified FAPI 1.0 server implementations.

What are FAPI 1.0 shortcomings?

- Probably, it has done too much to secure, making implementations complex.
- Too many options.
- Quite tied to OpenID Connect 1.0.
- The communication between clients and resource servers are out of scope and has not provided a way to provide “non-repudiation”.
- No Standard Mechanism for Grant Management



FAPI 2.0

Do less to achieve the same effect

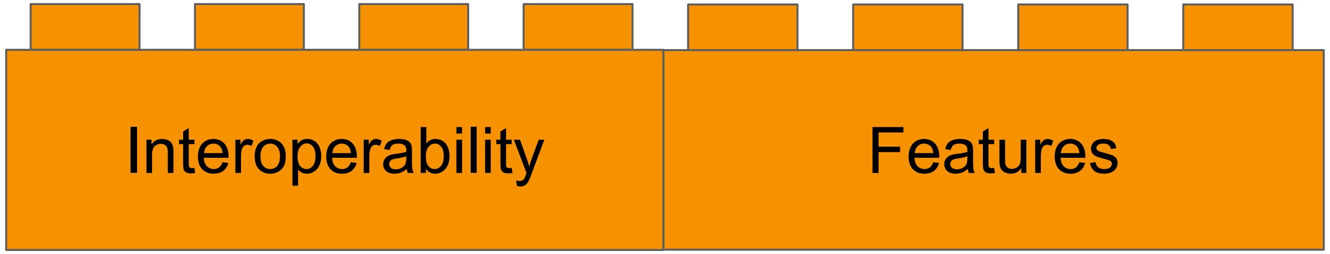
Less options

Decouple from OpenID Connect

Use of HTTP Signature for the Resource Server access

Grant Management

FAPI 2.0



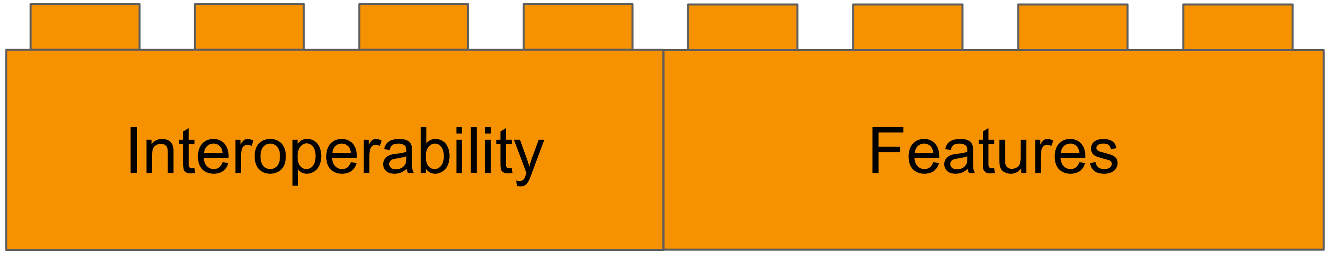
Pushed Authorization Requests (PAR)

replace bespoke solutions like external resources with references in scope/claims, custom authorization request parameters, …

→ Simplified development through vendor support (expected)

→ Minimize data in front-channel to improve security

FAPI 2.0

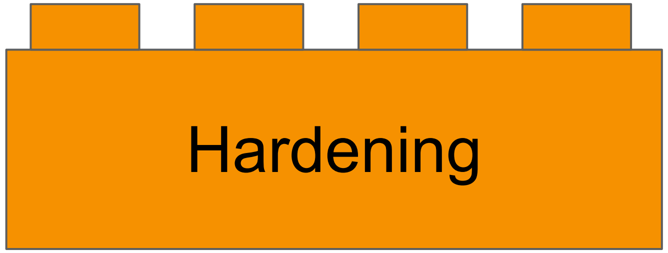


Rich Authorization Requests (RAR)

enable fine-grained and complex consents.

```
[
  {
    "type": "payment_initiation",
    "actions": [
      "initiate", "status", "cancel"
    ],
    "locations": [
      "https://example.com/payments"
    ],
    "instructedAmount": {
      "currency": "EUR",
      "amount": "123.50"
    },
    "creditorName": "Merchant123",
    "creditorAccount": {
      "iban": "DE02100100109307118603"
    },
    "remittanceInformationUnstructured": "Ref Number"
  }
]
```

FAPI 2.0



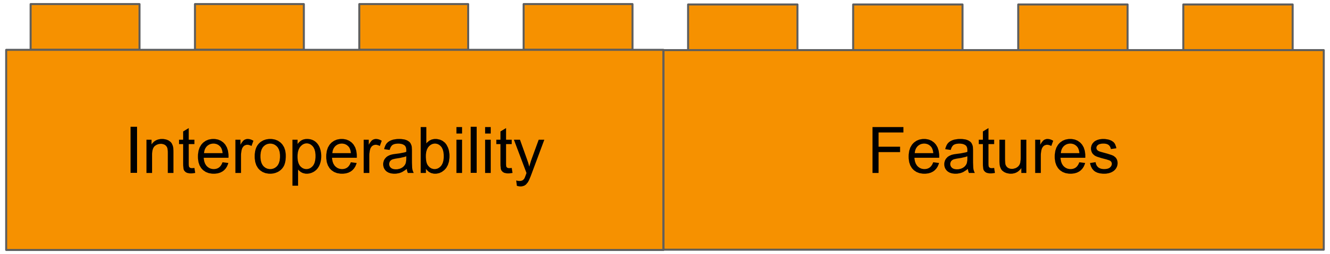
Hardening

OAuth Security Best Current Practice RFC draft incorporated for latest OAuth security recommendations.

OAuth Mutual TLS for client authentication and sender-constrained access tokens. (as in FAPI 1.0)

→ Protect against code replay, mix-up attacks, etc.

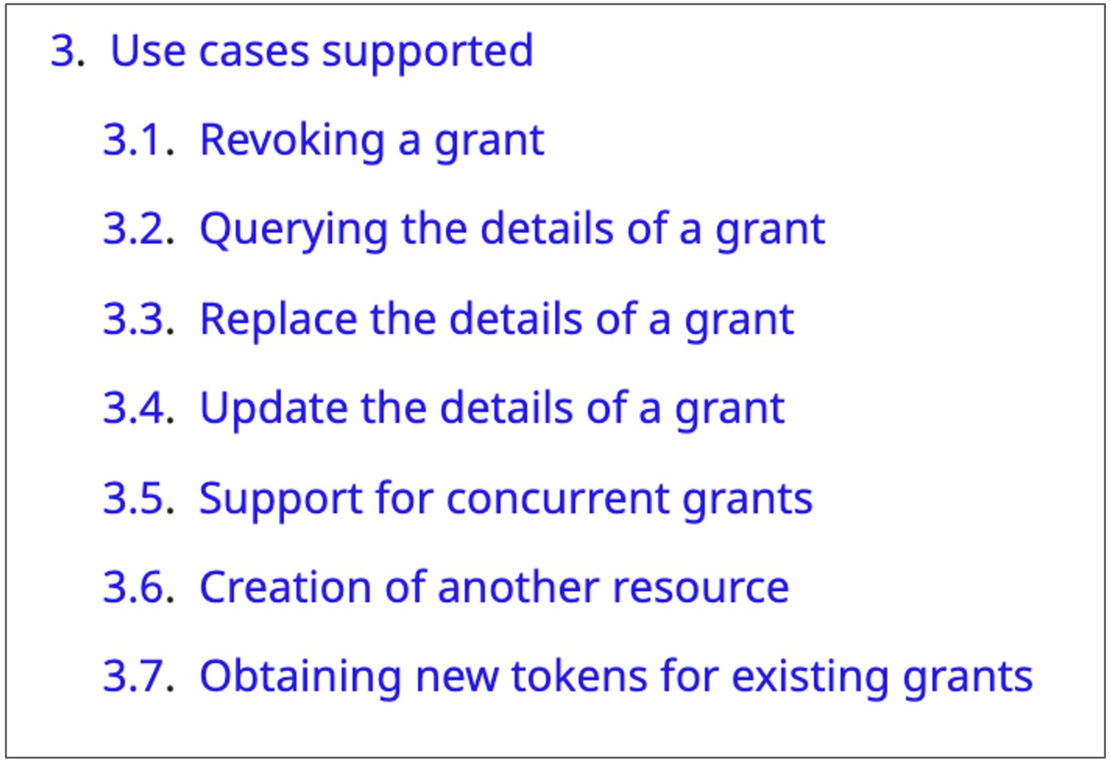
FAPI 2.0



Grant Management API

enables support for

- consent state synchronization
- consent revocation
- concurrent consents
- dashboards



3. Use cases supported
   - 3.1. Revoking a grant
   - 3.2. Querying the details of a grant
   - 3.3. Replace the details of a grant
   - 3.4. Update the details of a grant
   - 3.5. Support for concurrent grants
   - 3.6. Creation of another resource
   - 3.7. Obtaining new tokens for existing grants

Working Group Progress & Opportunities

Implementer's Drafts

- FAPI: Client Initiated Backchannel Authentication (CIBA) Profile – FAPI CIBA is a profile of the OpenID Connect's CIBA specification that supports the decoupled flow
- FAPI 2.0 Security Profile and Attacker Model – FAPI 2.0 has a broader scope than FAPI 1.0 as it aims for complete interoperability at the interface between client and authorization server as well as interoperable security mechanisms at the interface between client and resource server
- FAPI 2.0 Message Signing – an extension of the baseline profile that provides non-repudiation for all exchanges including responses from resource servers
- Grant Management for OAuth 2.0 – This profile specifies a standards based approach to managing "grants" that represent the consent a data subject has given. It was born out of experience with the roll out of PSD2 and requirements in Australia

Working Group Progress & Opportunities

White Papers

- "Open Banking, Open Data, and the Financial Grade API” - 2022
- “Open Banking and Open Data: Ready to Cross Borders?” - 2023

Formal Analysis

- FAPI 2.0 Security Profile analysis complete
- FAPI 2.0 Message Signing, CIBA, DCR / DCM (Dynamic Client Registration/Management). Draft shared with WG. Action: WG Sign off by end of October

Certification

- Thriving for FAPI 1.0.
- FAPI 2.0 tests delivered, certification gaining momentum
  - Multiple vendors / banks / fintechs certified
  - Existing and prospective implementors encouraged to consider FAPI 2.0 in roadmap

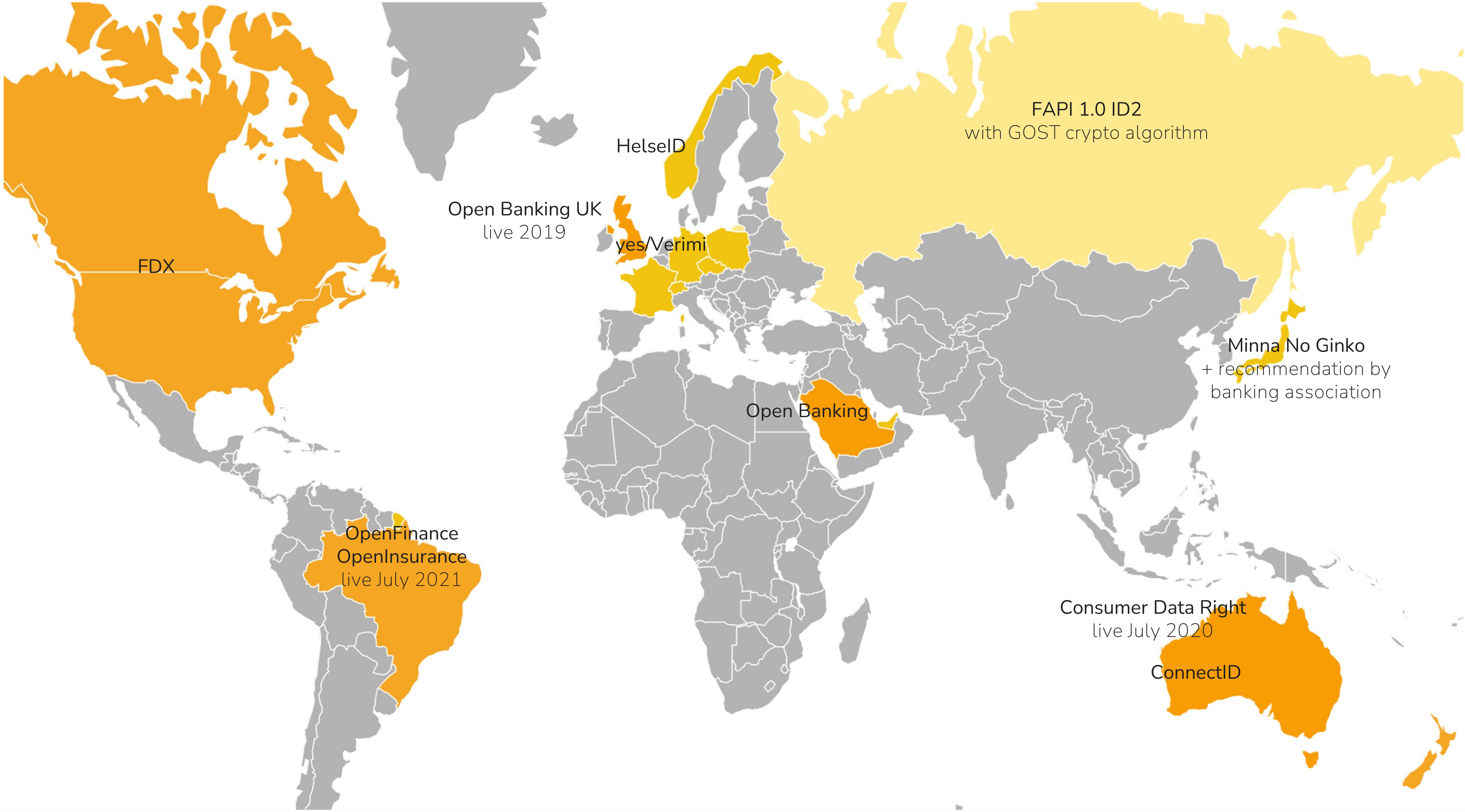
Working Group Roadmap

DATE	DELIVERABLES	ASPIRATIONS	NOTES
Q4 2023	Formal Verification for FAPI 2.0 Message Signing, DCR, and CIBA	End Oct WG Signoff Australian Gov't notification of WG sign-off	
	FAPI 2.0 Message Signing - - 2nd Implementer's draft		
Q1 2024		FINAL for FAPI 2.0 specs.	

FAPI Landscape Update

Mike Leszcz
OpenID Foundation Program Manager

The Evolving Landscape



FAPI Landscape Update

OBIE (Gov't)

- OIDF Certification (partial mandatory CMA9, annual)
- Local profile
- 64 IdP entities certified

Open Finance (Gov't)

- OIDF Certification (mandatory, annual)
- Local profile
- Board member
- Community group pilot
- Hundreds of IdP & RP entities certified
- 2024 recertification in Q1

Open Insurance (Gov't)

- OIDF Certification (mandatory)
- Local profile
- 47 IdP and 45 RP entities certified

CDR (Gov't)

- Selected FAPI 1.0, moving to FAPI 2.0
- Co-funded mathematical Security Analysis by Stuttgart University FAPI 2.0 Baseline complete
- FAPI Message Signing and CIBA completed - awaiting FAPI WG feedback

ConnectID (Private)

- ConnectID, co-funded conformance tests via directed funding
- OIDF pilot to bundle specifications
- Board member
- 5 IdP and 9 RP entities certified to ***FAPI 2.0***

SAMA (Gov't)

- OIDF Certs. (Mandatory)
- Local KSA profile
- 17 IdP and 12 RP entities certified

Note: Local entities in New Zealand (live, small scale) and Nigeria also selected FAPI.

FAPI Landscape Update

Open Banking Canada (Gov't)

- Open Banking Canada Feedback
- FDX selected FAPI 1.0
- Report completed and is under review. Will be released before end of year.
- FDX discussions renewed on combined certification to streamline FDX member journey

Norway Norsk Helsenett (Gov't)

- Selected FAPI 2.0
- Deployed in to nearly all healthcare personel (250k) and providers (7.5k)
- OIDF Workshop presentation @ EIC & OAuth Workshop

Japan Minna Bank (Private)

- Selected FAPI for Minna Bank to x-sell of Insurance with partners

Germany (Private)

- yes.com - private-sector open banking ecosystem
- Selected FAPI 2.0

CFPB / FDX (Gov't / Private)

- CFPB feedback
- FDX selected FAPI 1.0 Advanced, considering path to FAPI 2.0
- FDX discussions renewed on combined certification to streamline FDX member journey
- Awaiting initial rulemaking to review and comment – anticipated this week

Note: Local entities in New Zealand (live, small scale) and Nigeria also selected FAPI.

Certification Program Overview

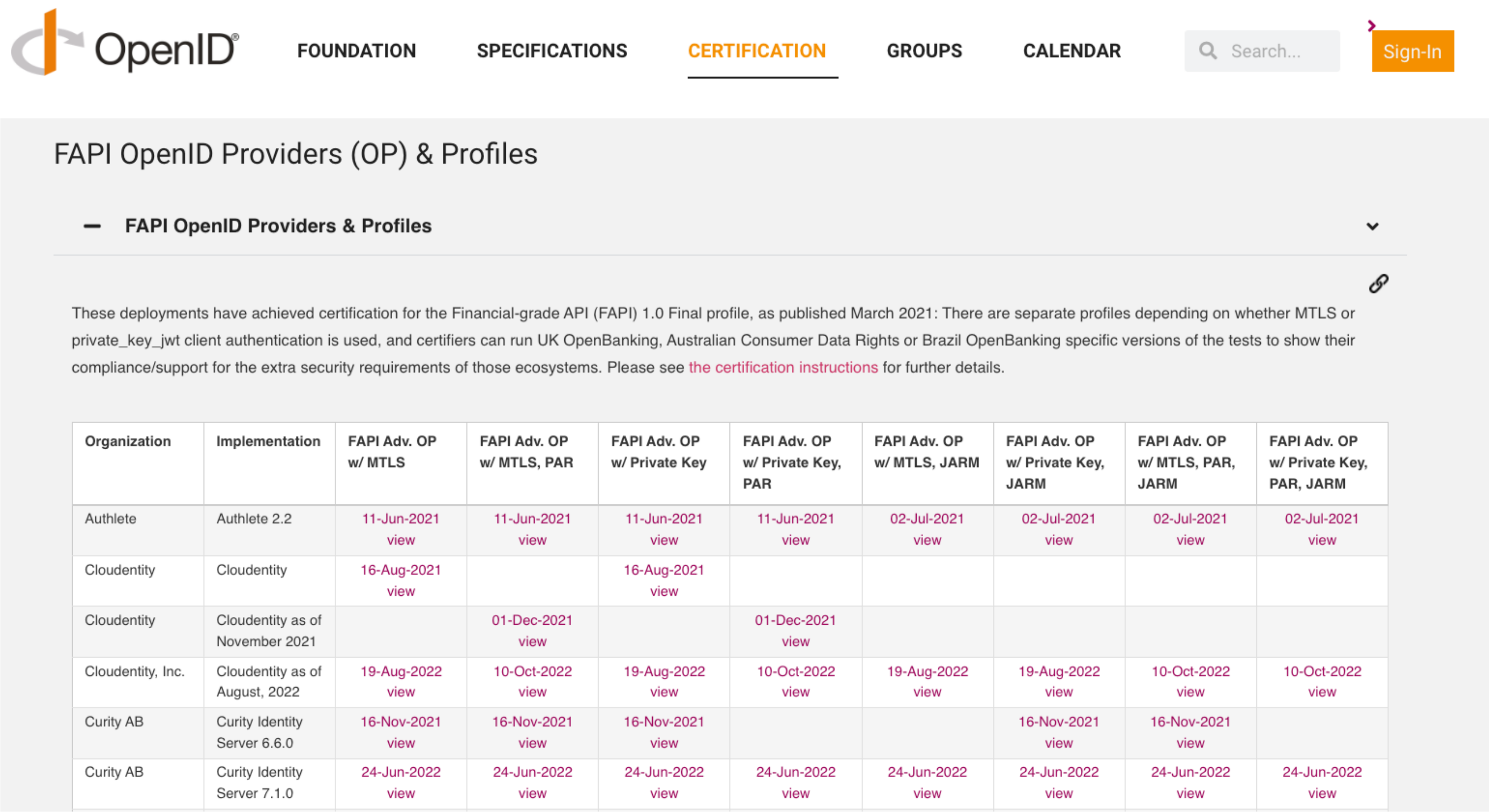
Mike Leszcz
OpenID Foundation Program Manager

OpenID Certification Program

- A light-weight, low-cost, self-certification program to serve members, drive adoption and promote high-quality implementations
    - Identity Providers launched in early 2015
    - Relying Parties launched in late 2016
    - Financial-grade profiles launched in 2019
- Each certification makes it easier for those that follow and helps make subsequent deployments more trustworthy, interoperable and secure
- All certified implementations are openly listed at https://openid.net/developers/certified/

FAPI Certifications

https://openid.net/certification/#FAPI_OPs



FAPI OpenID Providers (OP) & Profiles

FAPI OpenID Providers & Profiles

These deployments have achieved certification for the Financial-grade API (FAPI) 1.0 Final profile, as published March 2021: There are separate profiles depending on whether MTLS or private_key_jwt client authentication is used, and certifiers can run UK OpenBanking, Australian Consumer Data Rights or Brazil OpenBanking specific versions of the tests to show their compliance/support for the extra security requirements of those ecosystems. Please see the certification instructions for further details.

Organization	Implementation	FAPI Adv. OP w/ MTLS	FAPI Adv. OP w/ MTLS, PAR	FAPI Adv. OP w/ Private Key	FAPI Adv. OP w/ Private Key, PAR	FAPI Adv. OP w/ MTLS, JARM	FAPI Adv. OP w/ Private Key, JARM	FAPI Adv. OP w/ MTLS, PAR, JARM	FAPI Adv. OP w/ Private Key, PAR, JARM
Authlete	Authlete 2.2	11-Jun-2021 view	11-Jun-2021 view	11-Jun-2021 view	11-Jun-2021 view	02-Jul-2021 view	02-Jul-2021 view	02-Jul-2021 view	02-Jul-2021 view
Cloudentity	Cloudentity	16-Aug-2021 view		16-Aug-2021 view					
Cloudentity	Cloudentity as of November 2021		01-Dec-2021 view		01-Dec-2021 view				
Cloudentity, Inc.	Cloudentity as of August, 2022	19-Aug-2022 view	10-Oct-2022 view	19-Aug-2022 view	10-Oct-2022 view	19-Aug-2022 view	19-Aug-2022 view	10-Oct-2022 view	10-Oct-2022 view
Curity AB	Curity Identity Server 6.6.0	16-Nov-2021 view	16-Nov-2021 view	16-Nov-2021 view			16-Nov-2021 view	16-Nov-2021 view	
Curity AB	Curity Identity Server 7.1.0	24-Jun-2022 view	24-Jun-2022 view	24-Jun-2022 view	24-Jun-2022 view	24-Jun-2022 view	24-Jun-2022 view	24-Jun-2022 view	24-Jun-2022 view

OpenID CERTIFIED

2,400+ total certifications to date!

Conformance Tests Update

Current Certification Programs

- OpenID Connect, OpenID Connect Logout, FAPI1-Advanced, FAPI2 Security Profile ID2, FAPI2 Message Signing ID1 (partial), FAPI-CIBA ID1

Tests Under Development

- OpenID For Verifiable Presentations
- OpenID Connect for Identity Assurance
- FAPI2 DPoP, HTTP Signatures

Future Roadmap

- OpenID For Verifiable Credential Issuance
- OpenID Federation (directed funding received from ConnectID, thank you!)
- FAPI2-CIBA
- OIDF-J/ Japan Gov collaboration (directed funding anticipated for OID4VC tests)

Thank you.

OpenID®

Visit: www.OpenID.net