

Introduction to the FAPI Read & Write OAuth Profile

2018-05-15

Nat Sakimura(@_nat_en)



Chairman of the board



Research Fellow

- OpenID® is a registered trademark of the OpenID Foundation.
- *Unless otherwise noted, all the photos and vector images are licensed by GraphicStocks.

OAuth is a framework – needs to be profiled

“ This framework was designed with the clear expectation that future work will define prescriptive profiles and extensions necessary to achieve full web-scale interoperability.

[\[Docs\]](#) [\[txt|pdf\]](#) [\[draft-ietf-oauth-v2\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[IPR\]](#) [\[Errata\]](#)

PROPOSED STANDARD
Errata Exist

Internet Engineering Task Force (IETF)
Request for Comments: 6749
Obsoletes: [5849](#)
Category: Standards Track
ISSN: 2070-1721

D. Hardt, Ed.
Microsoft
October 2012

The OAuth 2.0 Authorization Framework

Abstract

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction



Which OAuth?

draft-ietf-oauth-jwt-bcp	-00	2017-07-19	Active
draft-ietf-oauth-mtls	-04	2017-10-12	Active
draft-ietf-oauth-security-topics	-03	2017-09-10	Active
draft-ietf-oauth-token-binding	-05	2017-10-27	Active
draft-ietf-oauth-token-exchange	-09	2017-07-03	Active

Recently Expired:

draft-ietf-oauth-pop-key-distribution	-03	2017-02-24	Expired
---	---------------------	------------	-------------------------

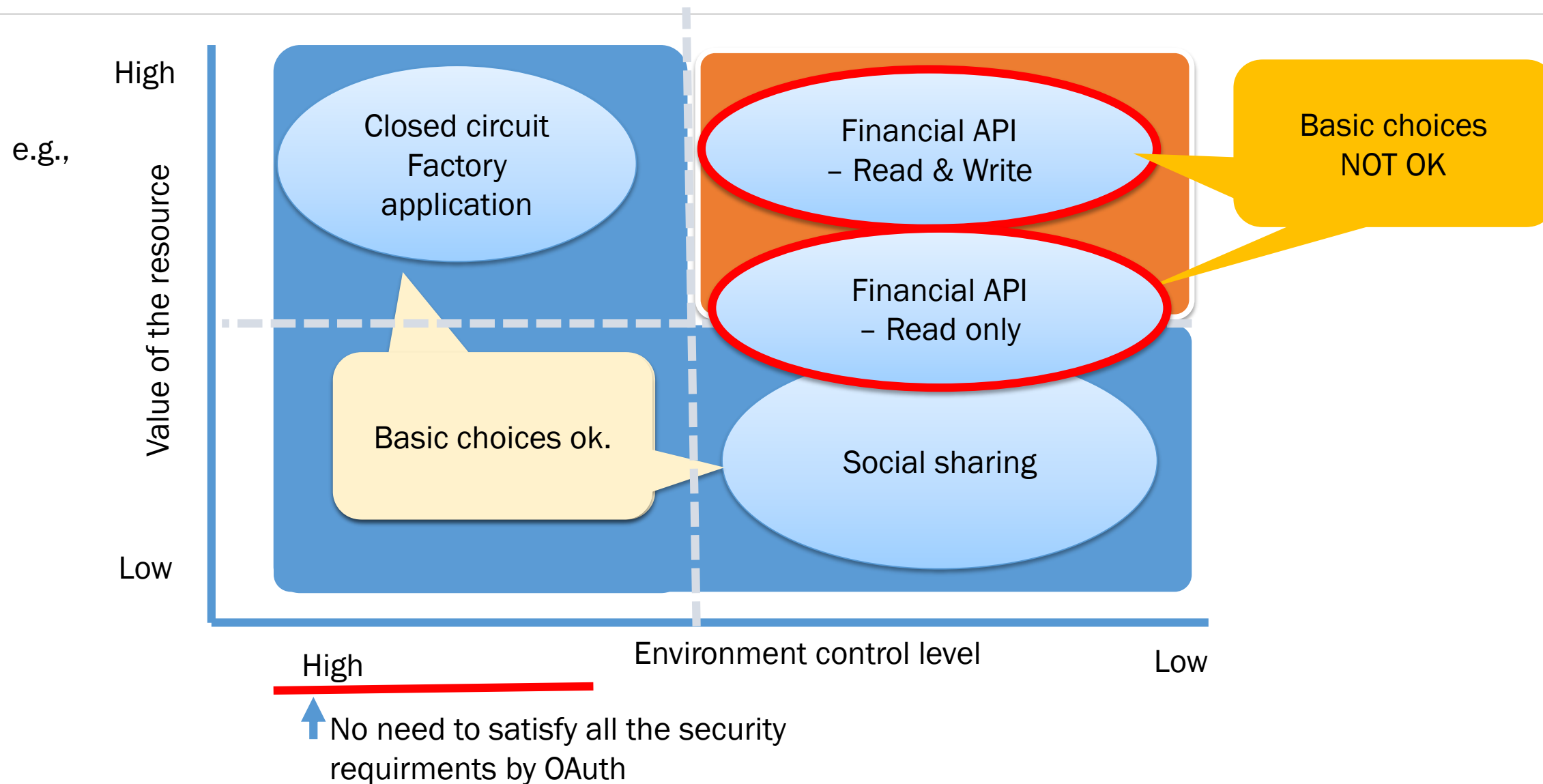
IESG Processing:

draft-ietf-oauth-discovery	-07	2017-09-07	Waiting for Writeup
draft-ietf-oauth-jwsreq	-15	2017-07-21	IESG Evaluation::AD Followup

Published:

Draft name	Rev.	Dated	Status	Obsoleted by/(Updated by)
draft-ietf-oauth-amr-values	-08	2017-03-13	RFC 8176	
draft-ietf-oauth-assertions	-18	2014-10-21	RFC 7521	
draft-ietf-oauth-dyn-reg	-30	2015-05-28	RFC 7591	
draft-ietf-oauth-dyn-reg-management	-15	2015-05-05	RFC 7592	
draft-ietf-oauth-introspection	-11	2015-07-04	RFC 7662	
draft-ietf-oauth-json-web-token	-32 ipr	2014-12-10	RFC 7519	(RFC 7797)
draft-ietf-oauth-jwt-bearer	-12	2014-11-12	RFC 7523	
draft-ietf-oauth-native-apps	-12	2017-06-09	RFC 8252	
draft-ietf-oauth-proof-of-possession	-11	2015-12-19	RFC 7800	
draft-ietf-oauth-revocation	-11	2013-07-13	RFC 7009	
draft-ietf-oauth-saml2-bearer	-23	2014-11-12	RFC 7522	
draft-ietf-oauth-spop	-15	2015-07-10	RFC 7636	
draft-ietf-oauth-urn-sub-ns	-06	2012-07-16	RFC 6755	
draft-ietf-oauth-v2	-31 ipr	2012-08-01	RFC 6749	(RFC 8252)
draft-ietf-oauth-v2-bearer	-23 ipr	2012-08-01	RFC 6750	
draft-ietf-oauth-v2-threatmodel	-08	2012-10-06	RFC 6819	

That creates specification to take care of medium to high risk API access security.



**That can serve all financial transactions
including PSD2,
but not limited to.**

FAPI Security Profile is a general purpose higher security API protection mechanism based on OAuth framework.

It has been adopted by Open Banking UK

BETA
OPEN BANKING

ABOUTCUSTOMERSDEVELOPERSAPI PROVIDERSINDUSTRYCONTACT

**MAY
17
2017**

Open Banking forms collaboration with OpenID Foundation

The Open Banking Implementation Entity (OBIE), the organisation responsible for the open API banking standard, today announces its collaboration with the OpenID Foundation's Financial API Working Group.

[Read More](#)

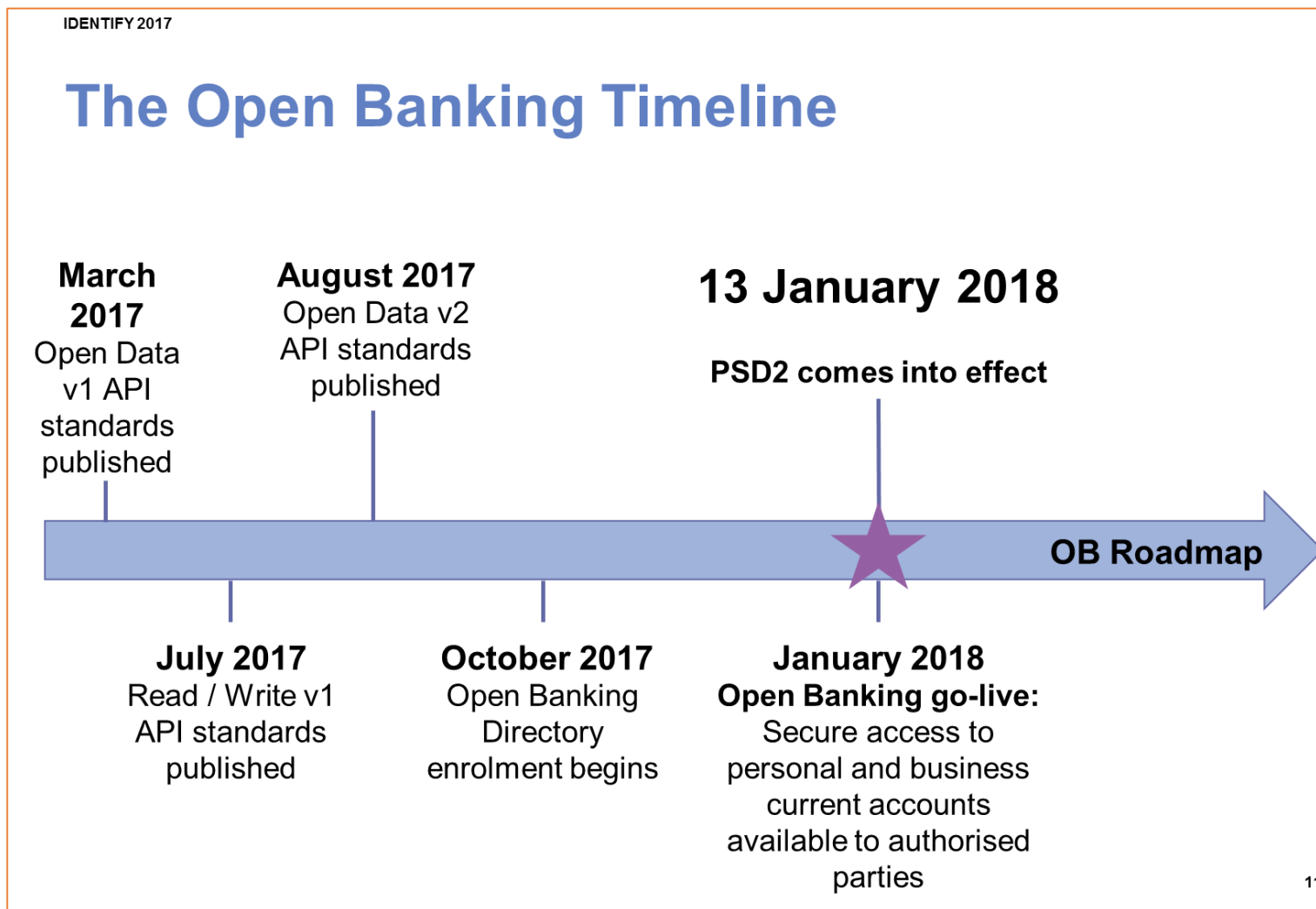
**APR
13
2017**

CMA Appoints New Trustee for Open Banking Implementation Entity

The Competition & Markets Authority ('CMA') has, today, announced that Imran Gulamhuseinwala will become the new trustee for the Open Banking Implementation Entity (the 'IE').

[Read More](#)

9 Major banks in UK went live on January, 2018



Australia adopting the same profile

(Source) Chris Mitchel, "Banking is now more open", Identify 2017

It is also recommended by the Japanese Banker's association

オープン API のあり方に関する検討会報告書
－ オープン・イノベーションの活性化に向けて －

2017 年 7 月 13 日
オープン API のあり方に関する検討会
(事務局：一般社団法人 全国銀行協会)

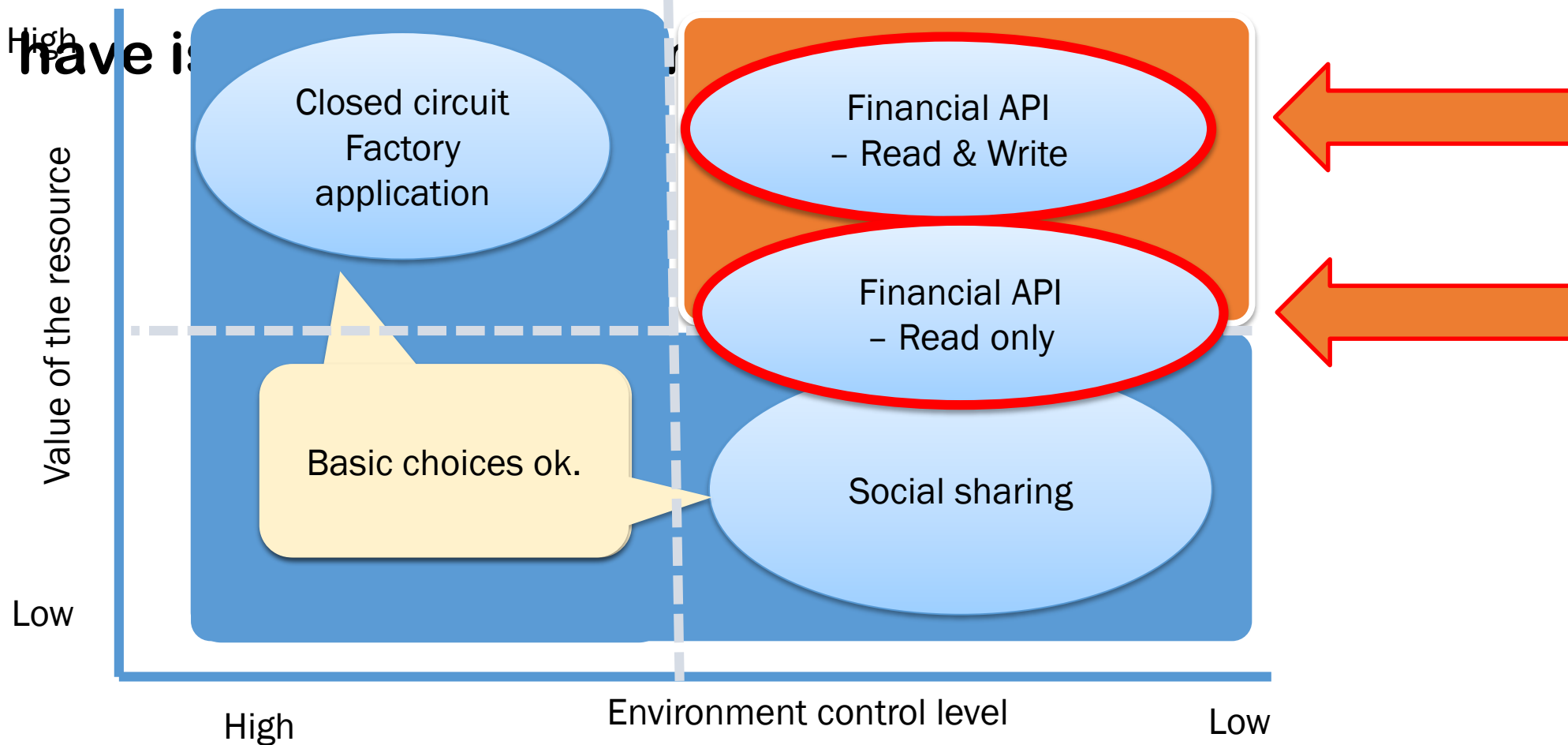
(source) https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_1.pdf

US FS-ISAC aligning their security requirements

**... and major IAM vendors are
implementing it**

**Submit to ISO/TC 68 and is a part of the
forthcoming technical specification**

e.g. We have is



Which are redirect approach

- **Part 1: Read Only Security Profile**
- **Part 2: Read and Write Security Profile**



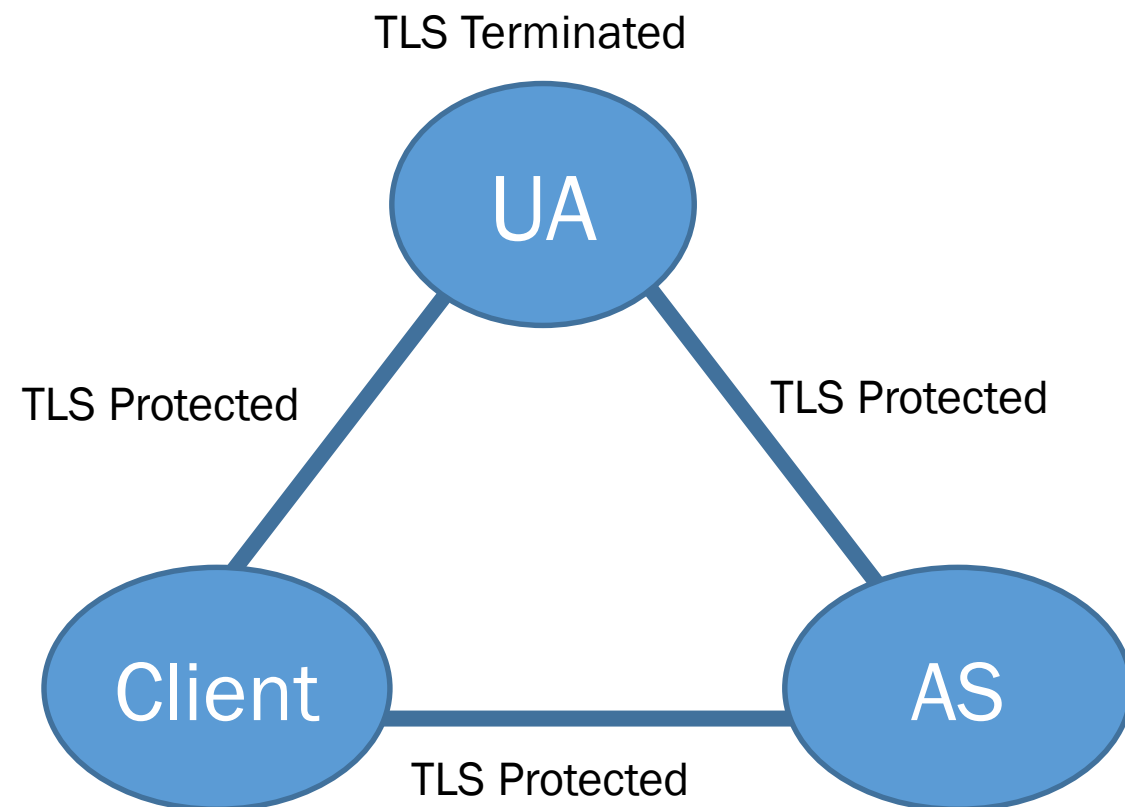
Redirect
Approach

Decoupled
Approach

Embedded
Approach

While 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

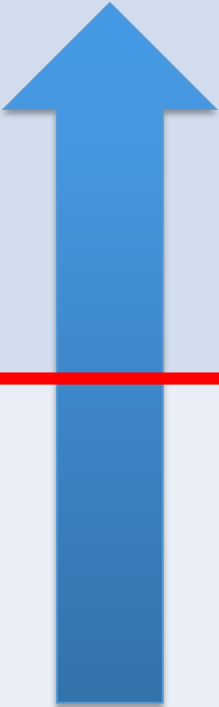




FAPI Part 2 is complete with source, destination, and message authentication.

- 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	Hybrid Flow	Hybrid Flow
Token Req	Good	Good	Good
Token Res	Good	Good	Good

Tokens are Sender Constrained instead of being bearer

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

These are in the form of check lists.

5.2 Read and Write API Security Provisions

5.2.1 Introduction

Read and Write access carries higher financial risk; therefore the protection level required is higher than Read-Only access.

As a profile of The OAuth 2.0 Authorization Framework, this document mandates the following for the Read and Write API of the FAPI.

5.2.2 Authorization Server

The authorization server shall support the provisions specified in clause 5.2.2 of Financial API - Part 1: Read-Only API Security Profile.

In addition, the authorization server, for the Write operation,

1. shall require the `request` or `request_uri` parameter to be passed as a JWS signed JWT as in clause 6 of [OIDC](#);
2. shall require the `response_type` values `code id_token` or `code id_token token`;
3. shall return ID Token as a detached signature to the authorization response;
4. shall include state hash, `s_hash`, in the ID Token to protect the `state` value;
5. shall only issue holder of key authorization code, access token, and refresh token for write operations;
6. shall support [OAUTH](#) or [MTLS](#) as a holder of key mechanism;
7. shall support user authentication at LoA 3 or greater as defined in [X.1254](#);
8. shall support signed ID Tokens; and
9. should support signed and encrypted ID Token.

(source) https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_002.md

Crypto Requirements are tightened for interoperability and security

8.5 TLS Considerations

As confidential information is being exchanged, all interactions shall be encrypted with TLS (HTTPS).

Section 7.1 of Financial API - Part 1: Read Only API Security Profile shall apply, with the following additional requirements:

1. Only the following 4 cipher suites shall be permitted:

- `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`

8.6 JWS Algorithm Considerations

JWS signatures shall use the `PS256` or `ES256` algorithms for signing.

(source) https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_002.md

And now working on the decoupled approach ...

■ CIBA (client initiated backchannel authentication) profile.

https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_CIBA.md

Redirect
Approach

Decoupled
Approach

Embedded
Approach

Embedded Approach

- **Giving bearer credentials to a third party is a bad idea.**
- **GDPR explicit consent for third party data transfer?**
 - What would be the liability implications?
- **Perhaps per app “password”?**

Redirect
Approach

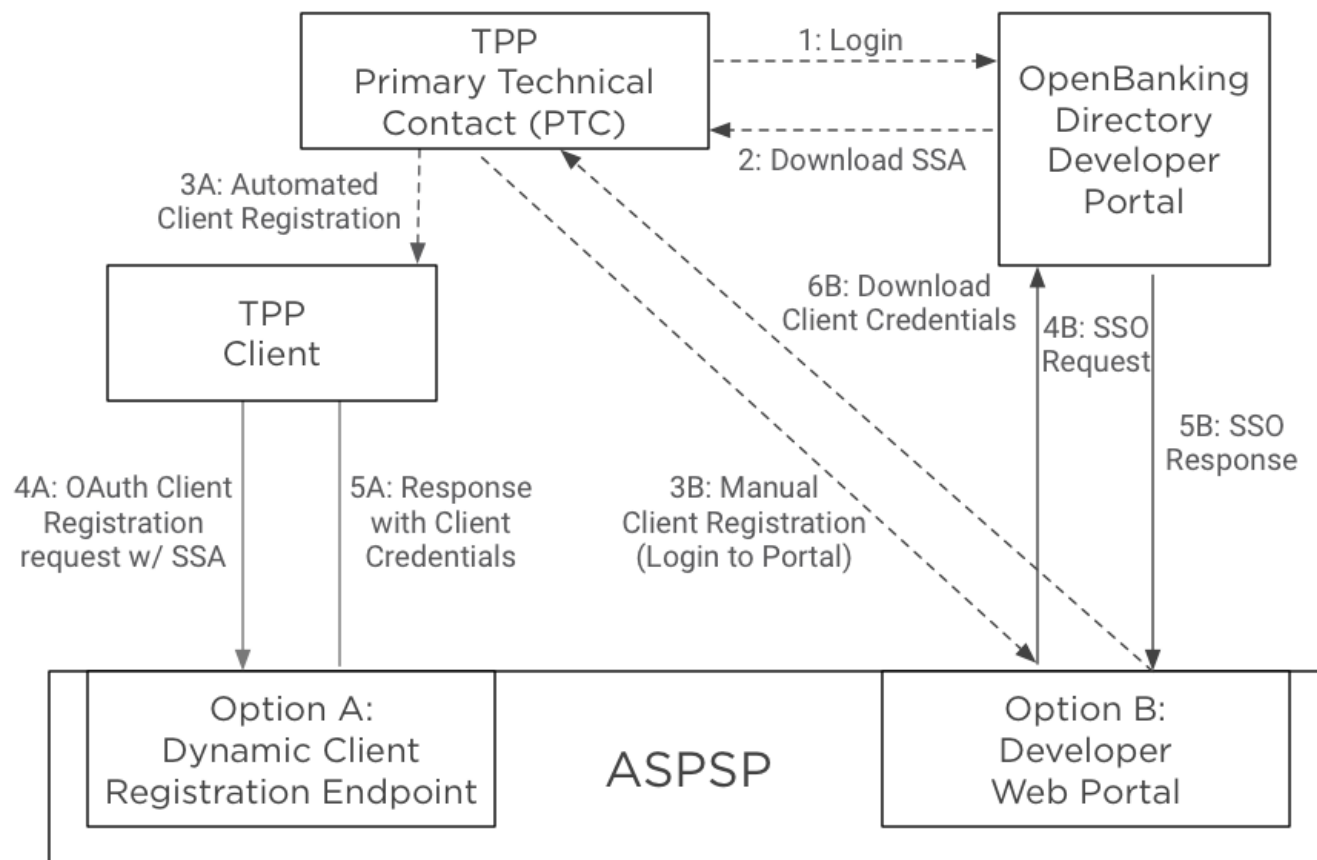
Decoupled
Approach

Embedded
Approach

We have other works as well...

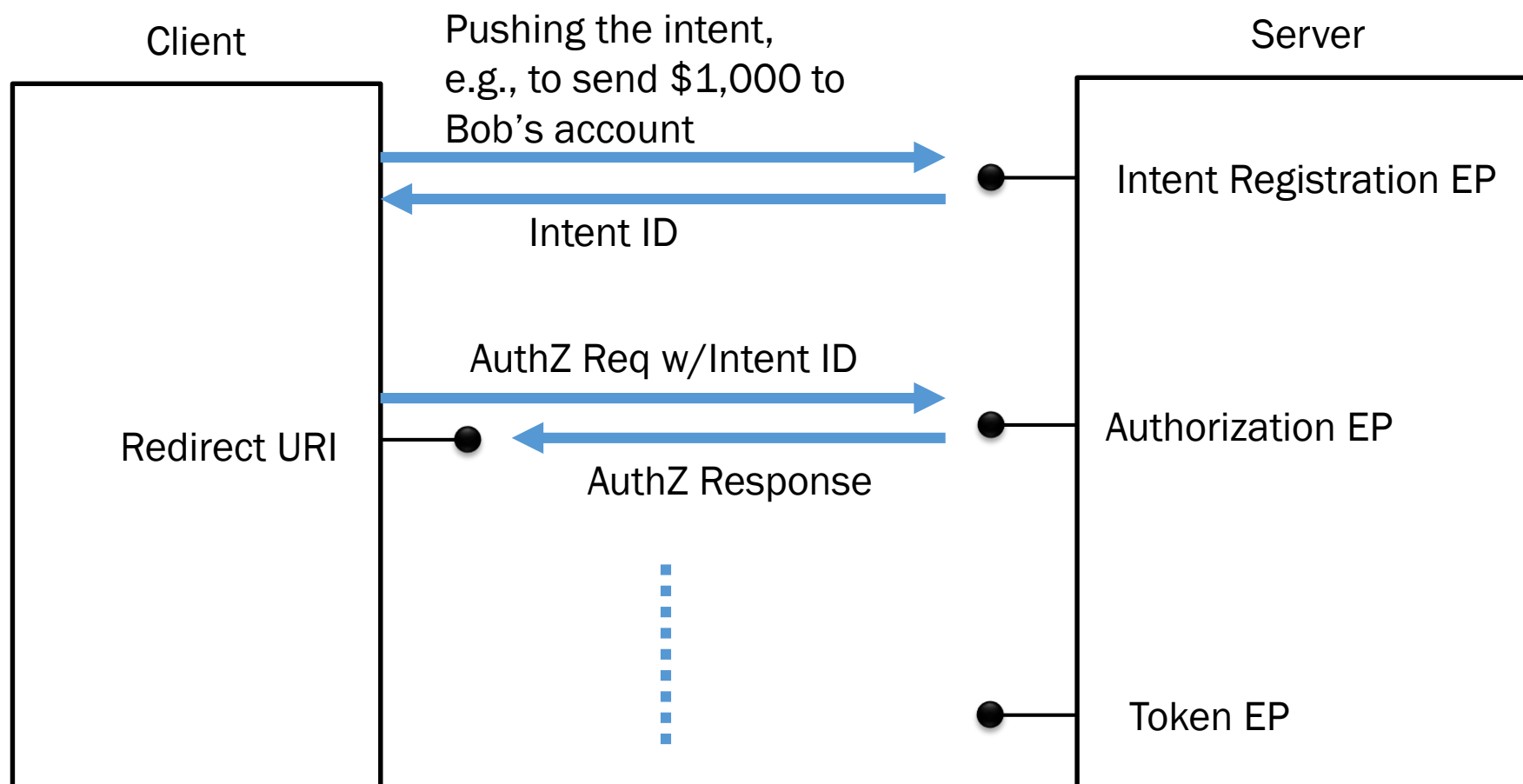
■ E.g. The OpenBanking OpenID Dynamic Client Registration Specification

OpenBanking Client Registration Overview (Options A, B)



... and perhaps

■ Intent registration endpoint





**How can we tell that the implementation
conforms to the specification?**

Once it passes the test, the implementer can self-certify and publish.

- That gets the implementers under the premise of the article 5 of the FTC Act.
- The log will be openly available so others can also find out false claims.

See <http://openid.net/certification/> for details

enters to test their conformance.



By the way



New Name for WG?

**After all, there is nothing specifically
“Financial”**

**It is a general purpose High Security API
protection protocol**

Some of the candidates ...

- **Fully Assured Protection Interoperable**
- **Fair Assurance Protection Interface**
- **Full Assurance Protection Interface**
- **Full Assurance Profile Interface (FAPI) WG**
- **Plus ...**