

# 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?

<a href="#">draft-ietf-oauth-jwt-bcp</a>	<a href="#">-00</a>	2017-07-19	<a href="#">Active</a>
<a href="#">draft-ietf-oauth-mtls</a>	<a href="#">-04</a>	2017-10-12	<a href="#">Active</a>
<a href="#">draft-ietf-oauth-security-topics</a>	<a href="#">-03</a>	2017-09-10	<a href="#">Active</a>
<a href="#">draft-ietf-oauth-token-binding</a>	<a href="#">-05</a>	2017-10-27	<a href="#">Active</a>
<a href="#">draft-ietf-oauth-token-exchange</a>	<a href="#">-09</a>	2017-07-03	<a href="#">Active</a>

#### *Recently Expired:*

<a href="#">draft-ietf-oauth-pop-key-distribution</a>	<a href="#">-03</a>	2017-02-24	<a href="#">Expired</a>
---	---------------------	------------	-------------------------

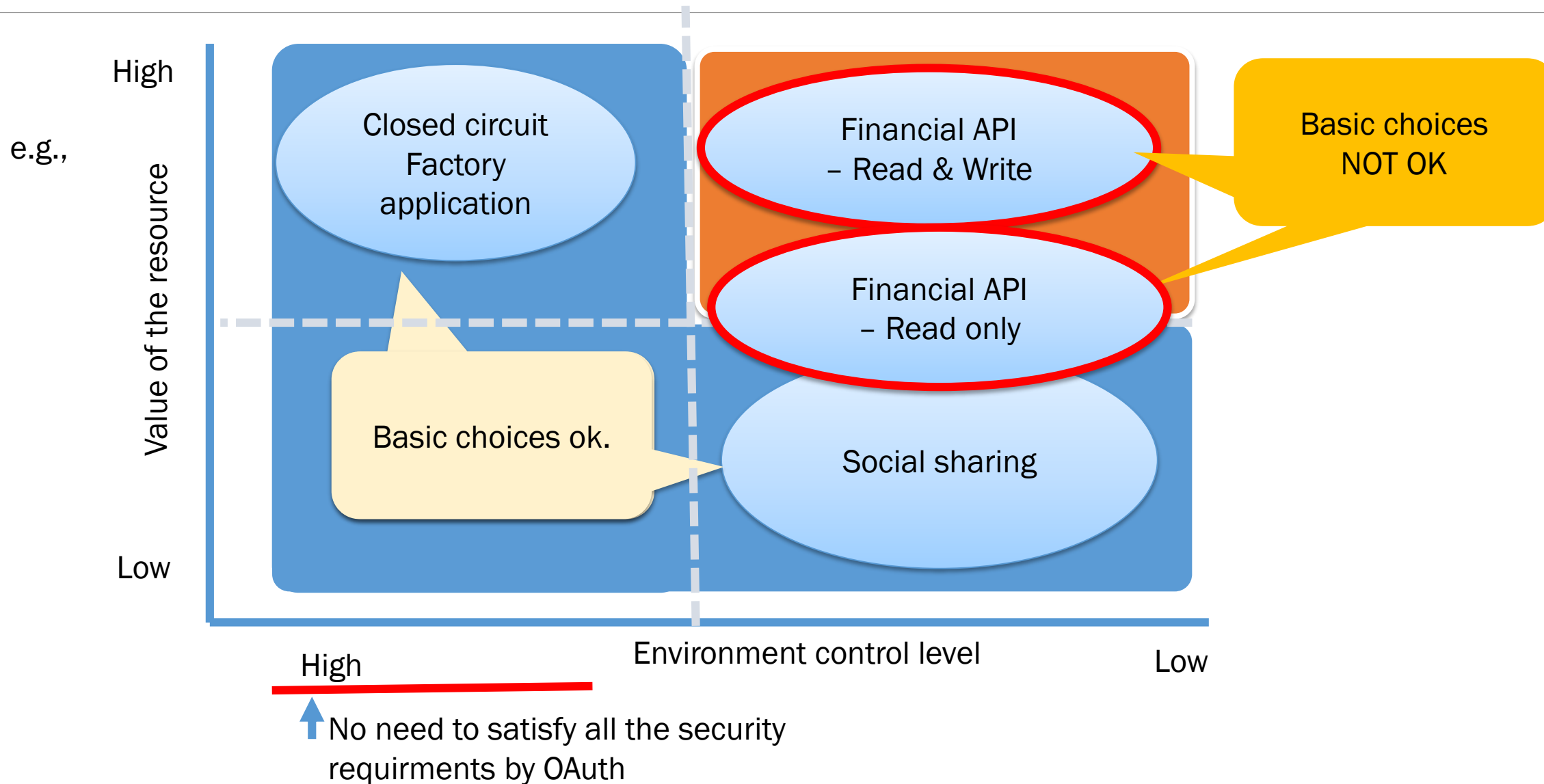
#### *IESG Processing:*

<a href="#">draft-ietf-oauth-discovery</a>	<a href="#">-07</a>	2017-09-07	<a href="#">Waiting for Writeup</a>
<a href="#">draft-ietf-oauth-jwsreq</a>	<a href="#">-15</a>	2017-07-21	<a href="#">IESG Evaluation::AD Followup</a>

#### *Published:*

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

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**

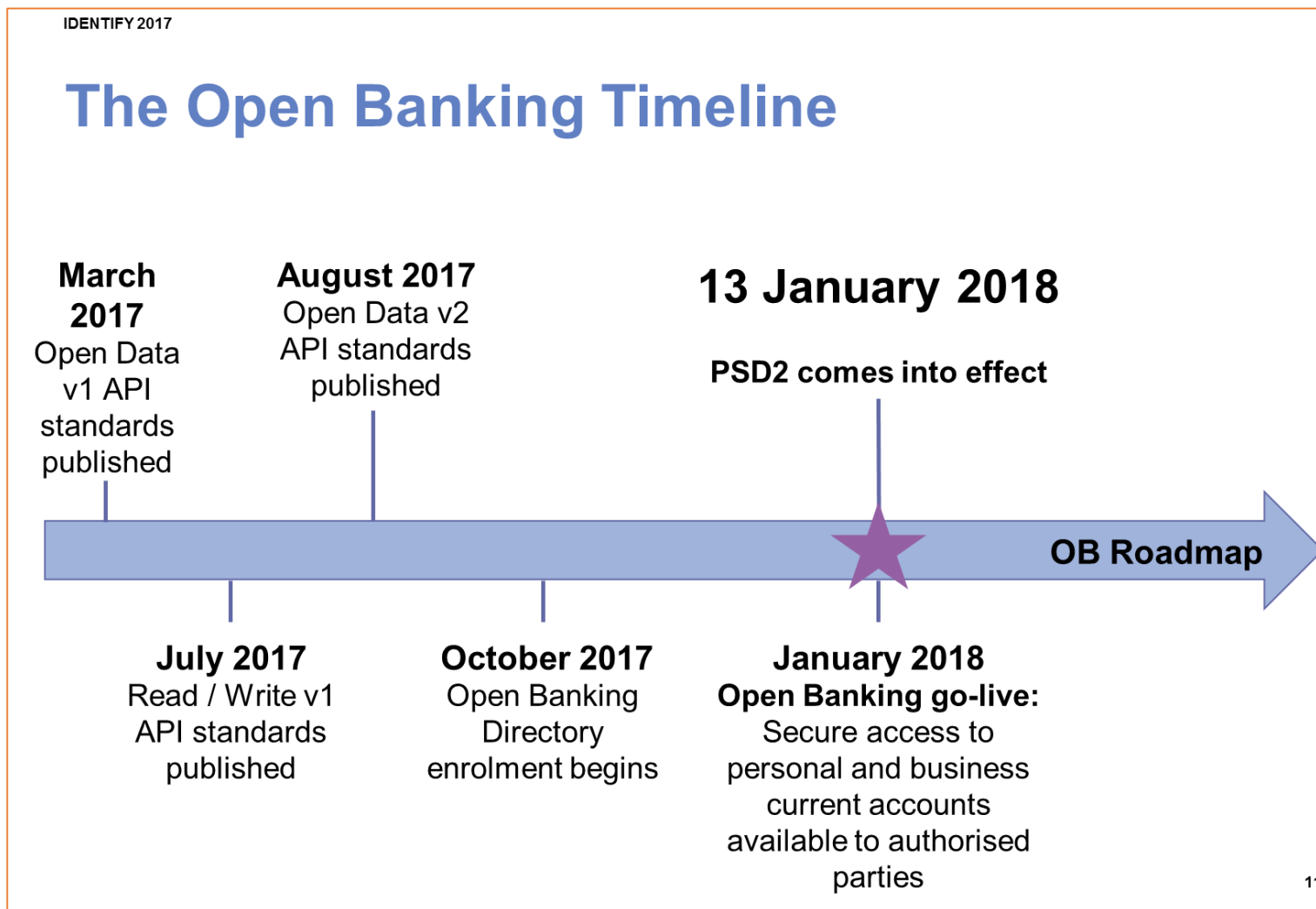
## CMA Appoints New Trustee for Open Banking Implementation Entity

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 )

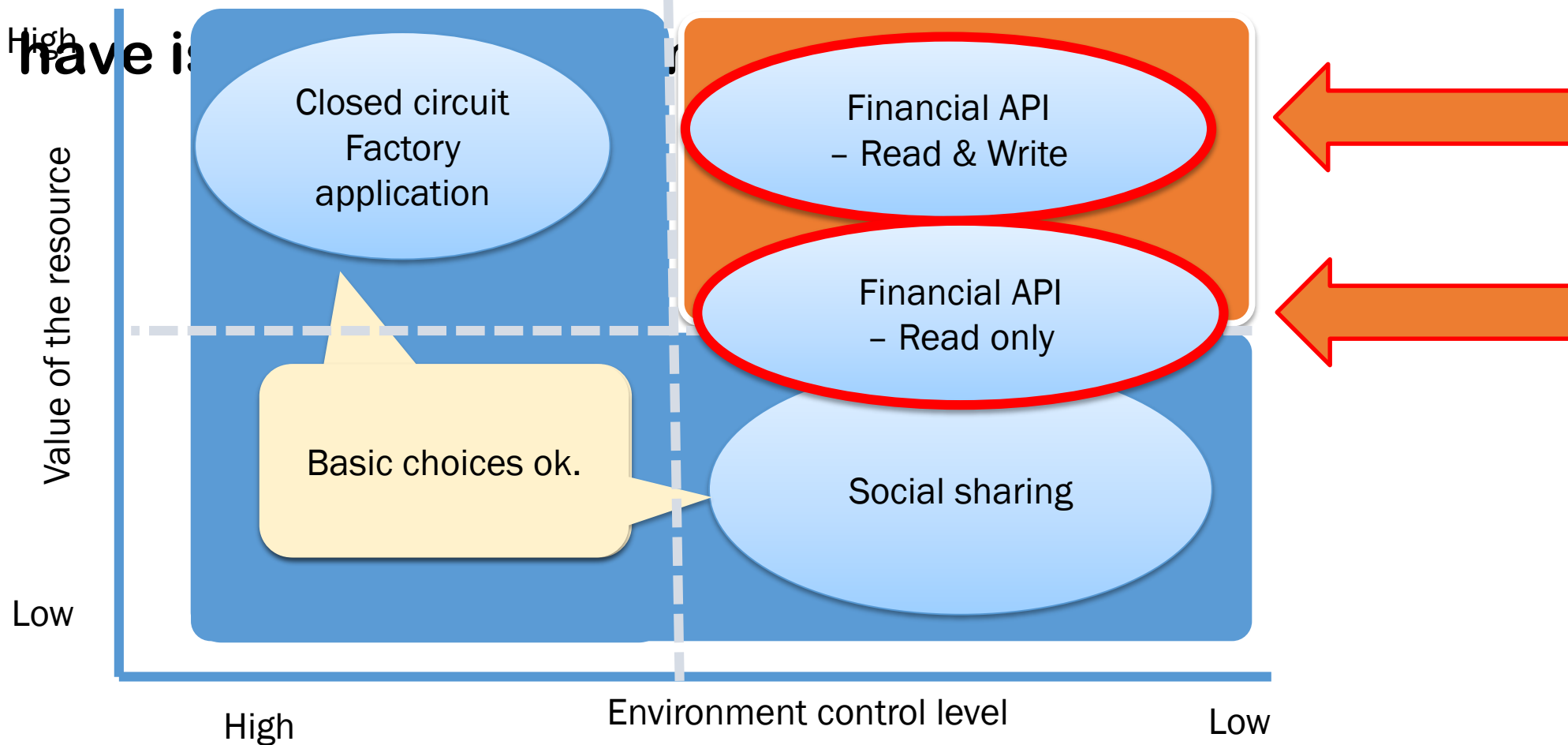
(source) [https://www.zenginkyo.or.jp/fileadmin/res/news/news290713\\_1.pdf](https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_1.pdf)

# **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**



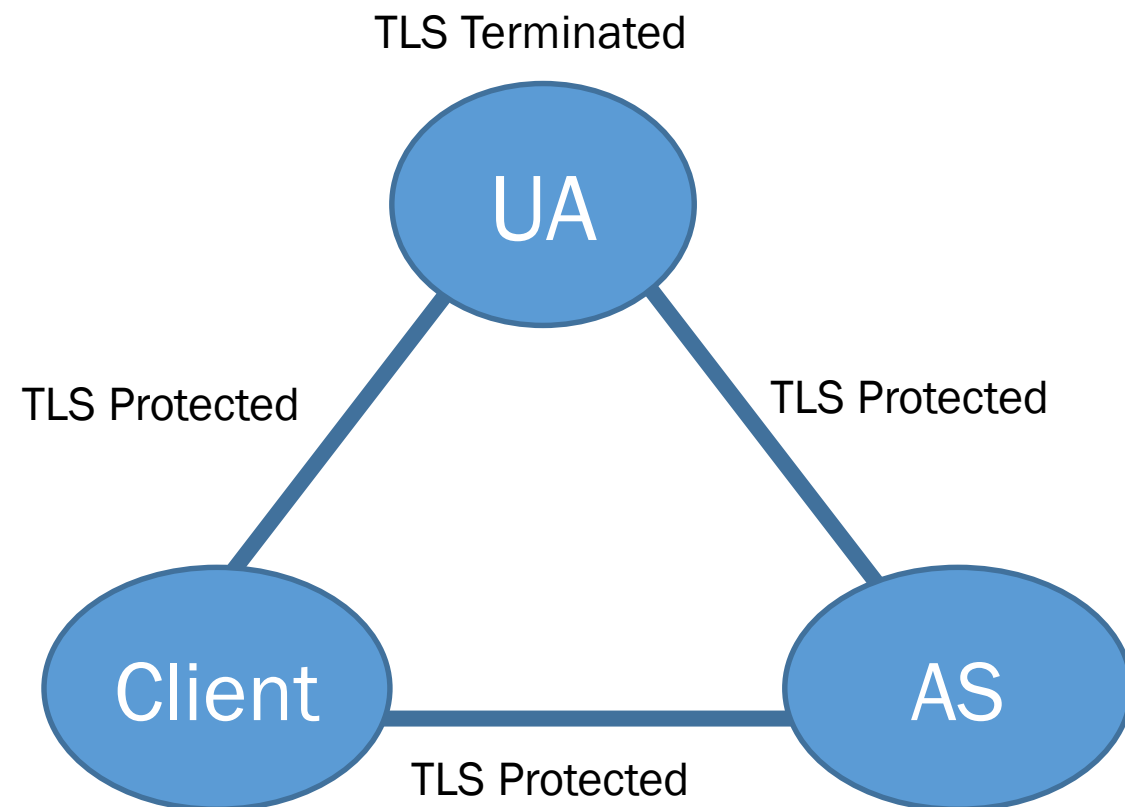
Redirect  
Approach

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



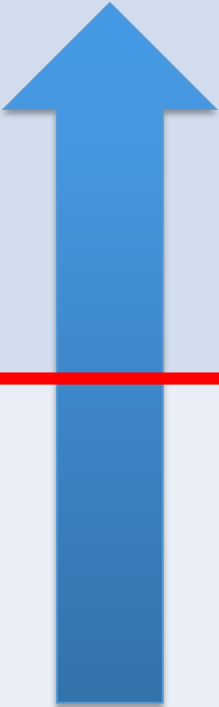




## FAPI Part 2 is complete with source, destination, and message authentication.

- 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](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](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](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

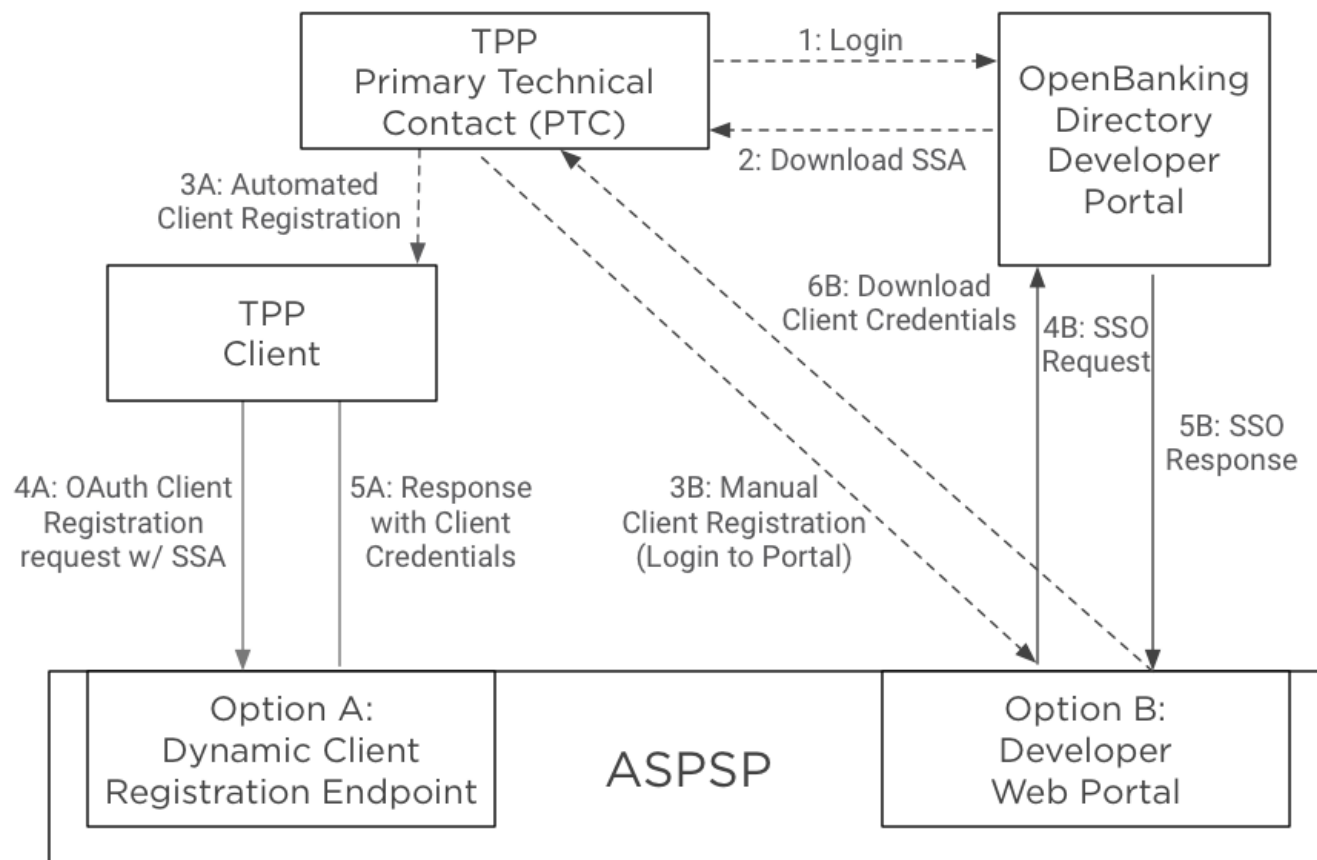
Decoupled  
Approach

Embedded  
Approach

We have other works as well...

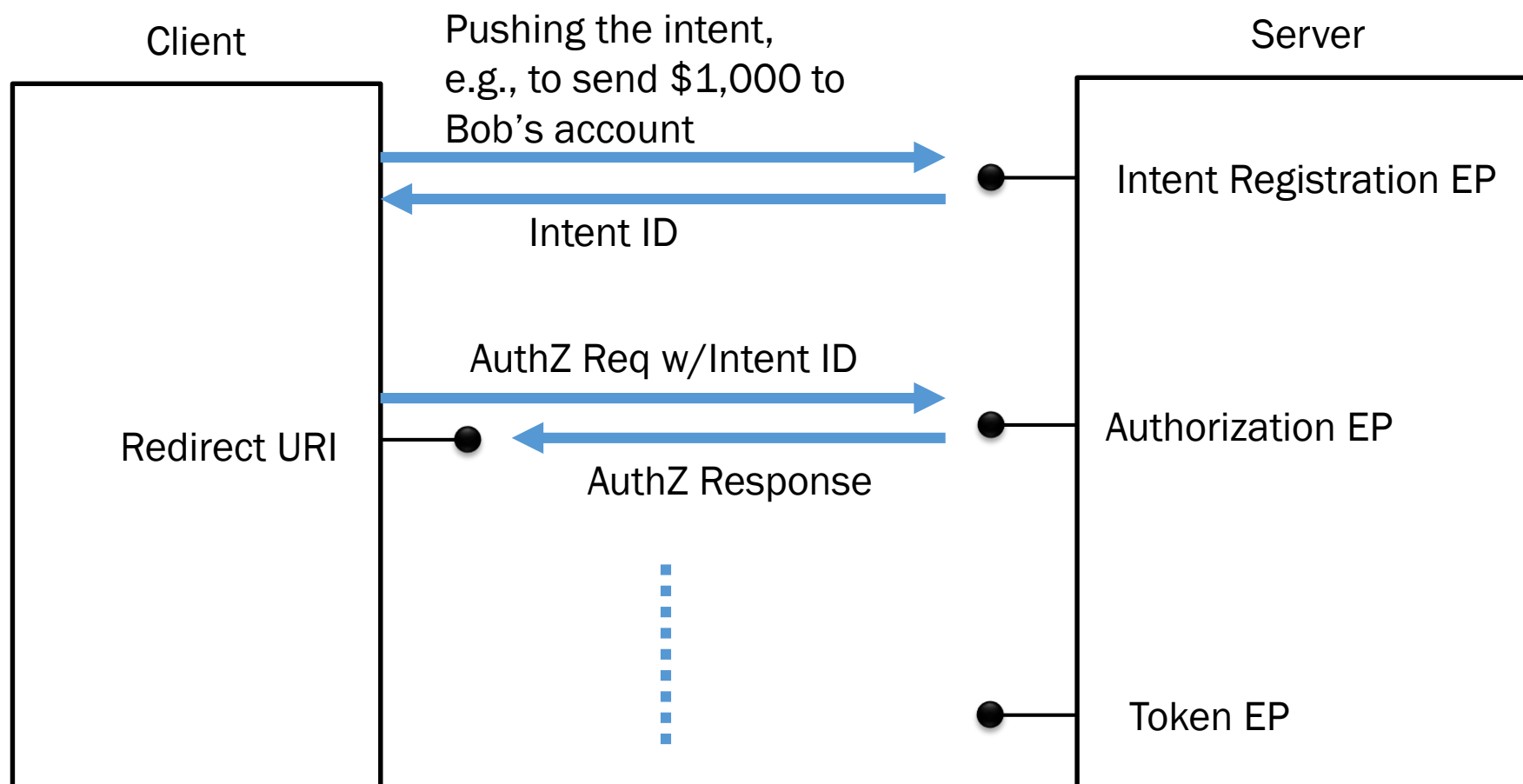
## ■ E.g. The OpenBanking OpenID Dynamic Client Registration Specification

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 ...**

# Introduction to OpenID Connect Self Issued Provider

2018-05-15

Nat Sakimura(@\_nat\_en)



Chairman of the board



Research Fellow

- OpenID® is a registered trademark of the OpenID Foundation.





**Have you read the Chapter 7 of  
OpenID Connect?**

**6.2.4.** request\_uri Rationale

## **6.3.** Validating JWT-Based Requests

**6.3.1.** Encrypted Request Object

**6.3.2.** Signed Request Object

**6.3.3.** Request Parameter Assembly and Validation

## **7.** Self-Issued OpenID Provider

**7.1.** Self-Issued OpenID Provider Discovery

**7.2.** Self-Issued OpenID Provider Registration

**7.2.1.** Providing Information with the "registration" Request Parameter

**7.3.** Self-Issued OpenID Provider Request

**7.4.** Self-Issued OpenID Provider Response

**7.5.** Self-Issued ID Token Validation

## **8.** Subject Identifier Types

**8.1.** Pairwise Identifier Algorithm

## **9.** Client Authentication

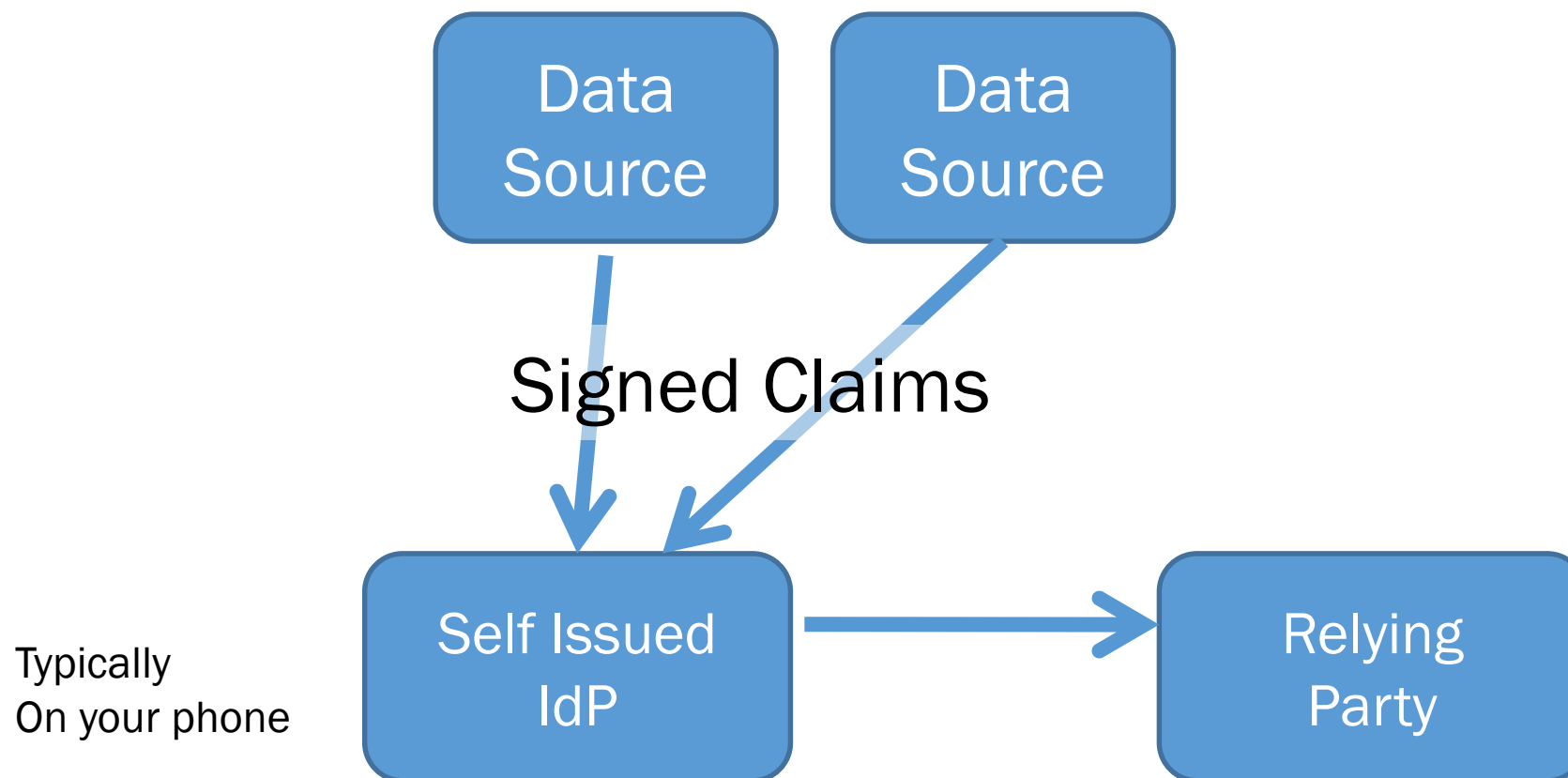
## **10.** Signatures and Encryption

**10.1.** Signing

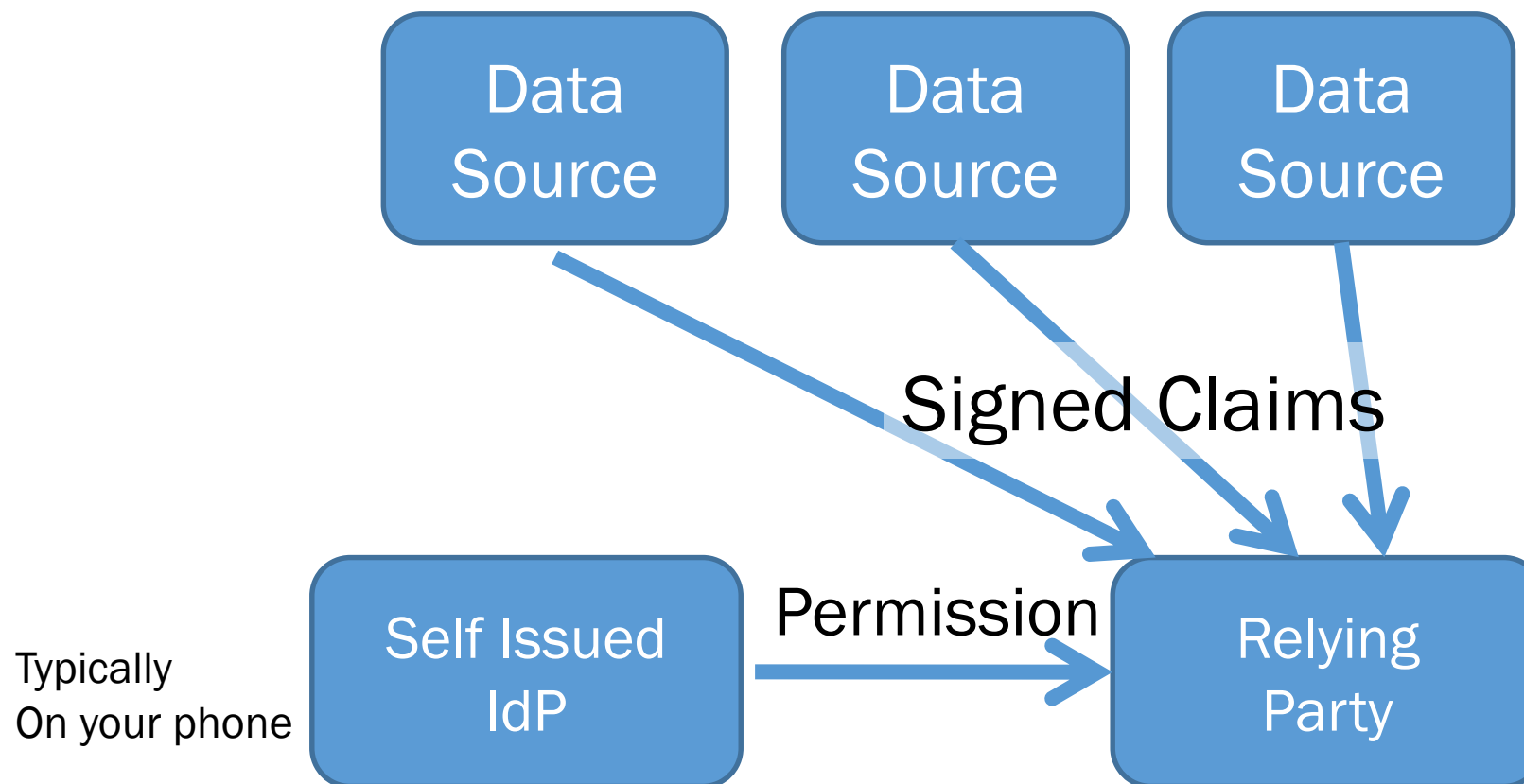
**It is an IdP on your local machine**

- **I am the issuer of my “identity” therefor it will not be taken away**
- **Sounds a lot like “Self Sovereign Identity”, is it not?**
- **It does not need Blockchain, and does not leak information like current proposals that uses Blockchain.**
- **Wire-protocol-wise, it is OpenID Connect with a little twist.**
- **It can obviously use the platform supported Authenticator,**
  - **e.g. FIDO/WebAuthn supporting TEE through biometric unlocking.**

# Aggregated Claims



# Distributed Claims



# E-SHOP LOGIN

## LOGIN

USERNAME

Username

PASSWORD

Password

Forgot Password ?

LOGIN

Social Logins



Self Issued Provider

Tap on it.

# E-SHOP LOGIN

LOGIN

USERNAME

Username

Open in "SldP"?

Cancel

Open

Forgot Password ?

LOGIN



Hello vrv-X0e69uJD3jvFtAFKgn-tF1fmSggJknN5v34AJkI

```
{
  "gender": "M",
  "iat": "2018-05-15T19:49:37.000Z",
  "family_name": "Sakimura ",
  "nonce": "12p29on",
  "sub": "vrv-X0e69uJD3jvFtAFKgn-tF1fmS
  ggJknN5v34AJkI",
  "sub_jwk": {
    "kty": "RSA",
    "n": "AN8Yh9JyU1AnHpx01TKsv6AEqlx
    yxjHdH-ve1J3p-YfNVBw7az7zyAlftX_3l380HGNa
    hQ_fypsAUMIK8AAUp5f843BRm4i35d8mJBkGwNsPo
    LpDY2aM6cYRrwTttBs4gaBLFI4wJo8r2jMRiLIrwp
    yxPZEtWIyztlH1scDuU5orx8DR_lKffvEgA4iktRQ
    3CU0VarYtoDoPRrls90JxUxHSpqtTn7tezK0LKY6V
    LrWB-c0D13XPsbPTsaJguyt1jvtrx1Gxsjs2MGktg
    iYg-KqvTE0EsZAIxjVqdySWjtgqC0yLphXgyBdTC5
    FyzxU9svNB4wyWVUYey6BrEmuFT50",
    "e": "AQAB"
  },
  "aud": "http://connect.openid4.us/esh
  op/sicallback.html",
  "exp": "2018-05-15T19:54:37.000Z",
  "updated_at": 1526413732,
  "iss": "https://self-issued.me"
}
```