Global Adoption of FAPI Among Open Banking Standards... And Beyond

Nat Sakimura, Chairman, OpenID Foundation
2020-09-22
Signed Claims Passing Protocol(s)

(aka Selective Claims Disclosure Protocol)
Claims can come from many sources

Which also forms Basis for ABAC.
Current base protocol is OpenID Connect (OIDC)
It is being used everywhere
You probably are using it ...

- Sign in with Apple
- Google Sign-in
- Microsoft Azure AD
- Zenkey
- itsme (Belgium)
- BankID (Norway)
- France Connect (France)
- Myna Portal (Japan)
- Etc.
Current Working Groups

There are 10 active working groups (WGs) tackling on the topics that are defined in their charters. (As of 2020-04-27)

WGs meet mostly online to share information and develop documents using issue tracking systems and git repositories and mailing lists.
OpenID Foundation Members

Members spread over 36 countries.
Supporting three types of Scalability

1. Performance
2. Deployment Pattern
3. Security
Battle Proven
Scalable
Performance

Over 90% of Azure AD App Authentications are through OpenID Connect as of April 2018.
Spanning from Centralized to Decentralized
Security Scalability

FAPI

OAuth 2.0 (RFC6749 & RFC6750)
+ ID Token (JWS/JWT)
+ Hybrid Flow
+ JAR

OpenID Connect
+ mTLS
+ PKCE
+ JARM
+ CIBA etc.
FAPI - Financial-grade API Security Profile

Designed for higher security

For transactions with higher values at stake or to exchange sensitive data.

Formally Verified

Security Properties Formally verified against Web Attacker Model.
... but how do you know if it was implemented correctly?
Conformance Test
OpenID Certification Program

Easy to use, semi-automated testing of your implementations.

Ensures that the implementations correctly implement the specification so that the interoperability improves substantially.

"Time it took for a bank and a fintech to connect via API literally went down from weeks to minutes."

-- Gavin Littlejohn, Chairman, FDATA Global
## Verified by Conformance Test Suites

<table>
<thead>
<tr>
<th>Entity</th>
<th>System/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oxyliom</td>
<td>GAïA Trust Platform 4.4</td>
</tr>
<tr>
<td>Ozone</td>
<td>Ozone Sandbox v3.1</td>
</tr>
<tr>
<td>Ping Identity</td>
<td>Consumer Data Rights SandBox for OpenBanking v1.4</td>
</tr>
<tr>
<td>Ping Identity</td>
<td>PingFederate 9.2.3</td>
</tr>
<tr>
<td>Sainsbury’s Bank PLC</td>
<td>Sainsbury’s Bank OpenID v1.1</td>
</tr>
<tr>
<td>Filip Skokan</td>
<td></td>
</tr>
<tr>
<td>TSB Bank PLC</td>
<td>CA API OpenID v1.1</td>
</tr>
<tr>
<td>Vanquis Bank Ltd</td>
<td></td>
</tr>
<tr>
<td>WSO2 (UK) Limited</td>
<td>OpenID v1.1</td>
</tr>
</tbody>
</table>

Global names like **HSBC** and **BARCLAYS** leading the way.
FAPI
API Security Profile

General Purpose High Security Level API Protection Protocol based on OAuth 2.0 Family of specifications.

Co-chairs:
Nat Sakimura (Japan)
Dave Tonge (UK)
Anoop Saxena (US)
Anthony Nadalin (US)
FAPI Projected Schedule

FAPI 1.0

2016-06
RO
RW
MTLS
ID 1
ID 2
2017-07
2018-10
2019-08
2020-02
2020-09
2020-12*

FAPI 2.0

2020-09
ID 1

Grant Management

Advanced

Baseline=JAR+PAR+RAR+JARM

"Public" Client Prof.

PAR&RAR

JARM
ID 1

FAPI-CIBA
ID 1

RFC8705

* Projection Only
FAPI Projected Schedule

**FAPI 1.0**
- 2016-06: RO ID 1
- 2017-07: MTLS
- 2018-10: ID 2
- 2019-08: JARM ID 1
- 2020-02: FAPI-CIBA ID 1
- 2020-09: RFC8705

**FAPI 2.0**
- 2020-09: PAR&RAR
- 2020-09: Grant Management

**Baseline**
- Baseline = JAR + PAR + RAR + JARM

**Advanced**
- "Public" Client Prof.

* Projection Only
Projected FAPI Adoption

- Live.
  CMA9+ are going through the Certification

- Working towards adoption

- Banking association guideline recommends FAPI

- Soft launched on July 1.

- Working towards adoption. Cryptographic algorithm may need to be changed.
Projected FAPI Adoption (with FDX)

- **Live.**
  - CMA9+ are going through the Certification

- **Working towards adoption**
  - Banking association guideline recommends FAPI

- **Soft launched on July 1.**

- **Working towards adoption.**
  - Cryptographic algorithm may need to be changed.
There are more works going on top of it

eKYE/IDA for OIDC

FAPI

Modrna  Heart  …

OpenID Connect

OAuth 2.0  JWx
eKYC & IDA
Verified Claims

Verified Claims representation to be sent over FAPI etc.

Co-chairs:
Mark Haine (UK)
Naohiro Fujie (Japan)
Anthony Nadalin (US)
Passing verified claims

Assumptions
- Verification rules
  (Laws, regulations and contracts)
- Verification status
- Verification methods

→ Implicit Trust

Alice Mirror
DoB: July, 1, 1970
DL: 12345678
A/C Bal: 880,035 USD
Passing verified claims

**verification**: {
    "trust_framework": "de_aml",
    "time": "2012-04-23T18:25Z",
    "verification_process": "f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
    "evidence": [
        {
            "type": "id_document",
            "method": "pipp",
            "verifier": {
                "organization": "Deutsche Post",
                "txn": "1aa05779-0775-470f-a5c4-9f1f5e56cf06"
            },
            "time": "2012-04-22T11:30Z",
            "document": {
                "type": "idcard",
                "issuer": {
                    "name": "Stadt Augsburg",
                    "country": "DE"
                },
                "number": "53554554",
                "date_of_issuance": "2010-03-23",
                "date_of_expiry": "2020-03-22"
            }
        }
    ]
}
International Standard

··• Identifiers for…

<table>
<thead>
<tr>
<th>Trust Frameworks</th>
<th>Identity Documents</th>
<th>Verification Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>eIDAS &amp; NIST 800-63A</td>
<td>ID Card &amp; Passport</td>
<td>Physical In-Person Proofing</td>
</tr>
<tr>
<td>Japanese &amp; German AML</td>
<td>Driver’s License</td>
<td>Supervised remote In-Person Proofing</td>
</tr>
</tbody>
</table>

··• Extensible

··• Contributions welcome!

Full list: https://bitbucket.org/openid/ekyc-ida/wiki/identifiers
eKYC/IDA Outlook

- Expression Language
- New Claims
  - e.g., age verifications
- Support for Legal Entities
- Conformance Tests
- Work with potential adopters
  - TISA
  - European Commission
  - ETSi
“Expression Language” initial draft contributed by Santander

3. Expression Language

The assertion member contains the expression (a JSON object) that will be evaluated as a boolean depending on the actual value of the named claim.

This language SHOULD be defined by the OP and it MUST be discoverable at the well-known endpoint, see section OP Metadata.

Recommended operations (if applicable):

- eq: The value is equal to the given value.
- gt: The value should be greater than the given value.
- lt: The value should be lower than the given value.
- gte: The value is equal or greater than the given value.
- lte: The value is equal or lower than the given value.
- in: The value is equal to one of the elements in the given list.
- or: The value pass any of the given expressions.

The OP is entitled to change the specification to match any individual requirements.

See https://bitbucket.org/openid/ekyc-ida/issues/1186/expression-language for more discussions around it.
eKYC/IDA Outlook

- Expression Language
- New Claims
  - e.g., age verifications
- Support for Legal Entities
- Conformance Tests
- Work with potential adopters
  - TISA
  - European Commission
  - ETSi
There are 10 active working groups (WGs) tackling on the topics that are defined in their charters. (As of 2020-04-27)

WGs meet mostly online to share information and develop documents using issue tracking systems and git repositories and mailing lists.
Standards Creation

Standardization of the technologies in cooperative area

- Working Groups creates standards and other technical documentations.
- Anybody who signs the IPR Contribution Agreement can join WGs as a contributor. There is no fee associated with it.
- By agreeing to the IPR Contribution Agreement, individuals and corporations agrees to provide their IPR free of charge for the implementations of the Standards and Implementer’s Drafts.
- The standardization process follows “OpenID Process” that adheres to WTO TBT Treaty Annex 3.
We can not work alone
Working Together

IETF
OAuth WG
JOSE WG*1

*I1 Now closed

IIF
Open Digital
Trust Initiative

Internet Technical
Advisory Committee
(ITAC)

Global Open Finance Technical Standards WG
(GOFTS WG)

DID-SIOP Profile

JTC 1/SC 27/WG5 IdM+Privacy
TC 68 Financial Services

ISO
Open Digital Trust Initiative

Open and collaborative project, aiming to establish industry technical standards and a facilitative policy framework to support uptake.
Working Together

IETF

OAuth WG
JOSE WG

"1 Now closed

IIF

Open Digital Trust Initiative

Internet Technical Advisory Committee (ITAC)

OECD

JTC 1/SC 27/WG5 IdM+Privacy
TC 68 Financial Services

Global Open Finance Technical Standards WG (GOFTS WG)

DID-SIOP Profile
FAPI 2.0 & eKYC/IDA
Do not wait
Join FAPI and eKYC WGs.

- **FAPI 1.0**
  - 2016-06: RO ID 1
  - 2017-07: RW ID 2
  - 2018-10: MTLS
  - 2019-08: JARM ID 1
  - 2020-02: FAPI-CIBA ID 1
  - 2020-09: RFC8705
  - **2020-12** Final

- **FAPI 2.0**
  - 2019-08: FAPI-CIBA ID 1
  - 2020-02: PAR&RAR
  - 2020-09: Baseline=JAR+PAR+RAR+JARM
  - Advanced
  - Grant Management

* Projection Only
Create the future together.