**Full Assurance Profile Interface (FAPI) WG**

**What is the Full Assurance Profile Interface (FAPI) WG?**

**Overview**

Most high value web interfaces, such as banking, have traditionally been private connections to browsers or native applications unique to each institution. This has resulted in the formation of third party providers that were trusted by the user to scrape financial information from the financial institution (FI). There was no trust between the FI and the third party even though the users were willing to give their personal credentials to the third part to access the data at the FI. This is not good for any of the three parties involved. The FAPI is designed to provide assurance for all parties as to the identity of each entity and the security of the links between them.

In many cases, Fintech services such as aggregation services uses screen scraping and stores user passwords. This model is both brittle and insecure. To cope with the brittleness, it should utilize an API model with structured data and to cope with insecurity, it should utilize a token model such as OAuth [RFC6749, RFC6750].

This working group aims to provide a solution by developing a REST/JSON model protected by OAuth and other OpenID protocols. Specifically, the FAPI WG aims to provide JSON data schemas, security and privacy recommendations and protocols to:

* enable applications to utilize the data stored in the financial account,
* enable applications to interact with the financial account, and
* enable users to control the security and privacy settings.

The various profiles will address authorization flows in all cases and authentication were value transfers are permitted. All profiles will improve the security of the data and most will address the authentication process and assurance that the user is fully informed of the identity of all parties as well as the assurance that data is protected at the user’s device.

**Working Group Chairs**

* Nat Sakimura (Nomura Research Institute), Anoop Saxena (Intuit), Anthony Nadalin (Microsoft)

The chairs can be reached at <[openid-specs-fapi-owner@lists.openid.net](mailto:openid-specs-fapi-owner@lists.openid.net)>.

**List of Specifications**

* [Full Assurance Profile for authorization (Implementer’s Draft).](http://openid.net/specs/openid-financial-api-part-1.html)
* [Full Assurance Profile for authentication and authorization (Implementer’s Draft)](http://openid.net/specs/openid-financial-api-part-2.html).
* [Full Assurance Profile for User Agent Call backs (Working Draft)](https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_003.md?at=master&fileviewer=file-view-default).

Current thought around it can be found in this [presentation](http://www.slideshare.net/nat_sakimura/openid-foundation-foundation-financial-api-fapi-wg).

[**OpenID Foundation FAPI WG: June 2017 Update**](http://www.slideshare.net/nat_sakimura/openid-foundation-fapi-wg-june-2017-update)from [**Nat Sakimura**](https://www.slideshare.net/nat_sakimura)

[**OpenID Foundation Foundation Financial API (FAPI) WG**](http://www.slideshare.net/nat_sakimura/openid-foundation-foundation-financial-api-fapi-wg)from [**Nat Sakimura**](http://www.slideshare.net/nat_sakimura)

## OpenID Foundation Full Assurance Profile Interface Working Group Charter

### 1) Working Group name:

Full Assurance Profile Interface Working Group (FAPI)

### 2) Purpose

The goal of FAPI is to provide JSON data schemas, security and privacy recommendations and protocols to:

* enable applications to utilize the data stored in any high value account,
* enable applications to interact with any high value account and
* enable users to control the security and privacy settings.

Any high value accounts, such as financial, may be considered.

### 3) Scope

The group will define

* JSON format to represent account related data, e.g., Account Representation, Transactions, Current Status,
* REST API for the accounts,
* security profiles for OpenID Connect and OAuth,
* Assurance of the security of data at rest and in-transit.
* Assurance of the identity of each of the three parties to the others.
* Purchase history of commerce site, and
* Receipt Data

Out of scope:

Any specific industry API.

### 4) Proposed Deliverables

The group proposes the following Specification deliverables:

Read only APIs for

* OAuth and Open ID connect authorizations

Write Access API including account creation and web payment for

* Fully authenticated sites.

Device security assurance for

* User portable phones and other devices

### 5) Anticipated audience or users

Financial institutions, service Providers and any others who interact with high value accounts to provide the service to users.

### 6) Language

English

### 7) Method of work:

E-mail discussions on the working group mailing list, working group conference calls, and face-to-face meetings from time to time.

### 8) Basis for determining when the work is completed:

Rough consensus and running code. The work will be completed once it is apparent that maximal consensus on the draft has been achieved, consistent with the purpose and scope.

# Background information

In many cases, Fintech services such as aggregation services uses screen scraping and stores user passwords. This model is both brittle and insecure. To cope with the brittleness, it should utilize an API model with structured data and to cope with insecurity, it should utilize a token model such as OAuth [RFC6749, RFC6750].

There are some examples of API models such as OFX, but it uses SOAP/XML model. However, SOAP/XML model has grown unpopular among the developers. Also, the OFX does not deploy the token model but uses user password, causing insecurity.

This working group aims to rectify the situation by developing a REST/JSON model protected by OAuth.

### Related work:

* RFC 6749 OAuth Frameworks
* RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage
* RFC 7636 Proof Key for Code Exchange by OAuth Public Clients
* OAuth 2.0 Proof-of-Possession (PoP) Security Architecture
* OpenID Connect
* Open Financial Exchange
* ISO 20022 Payment Messages
* OpenBank API
* W3C Web Payments API
* IFX
* FIX
* SWIFT
* FS-ISAC Durable Data API

WG considers establishing liaison agreement with the following organizations:

* ISO/TC68 Financial Services
* W3C Web Payments WG
* Open Financial Exchange
* IFX Forum
* FS-ISAC

### Proposers

* Nat Sakimura, Nomura Research Institute
* John Bradley, Ping Identity
* Henrik Biering, Peercraft
* Junichi Tabuchi, KDDI
* Nov Matake, Yauth.jp
* Anthony Nadalin, Microsoft
* Anoop Saxena, Intuit
* Toshio Taki, Money Forward

### Anticipated contributions:

Financial APIs in development at Open Banking

International Financial consortia

Government agencies

Bottom of Form