OpenID Foundation Financial API Working Group Charter (Draft)

## 1) Working Group name:

Financial API 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 the financial account,

enable applications to interact with the financial account, and

enable users to control the security and privacy settings.

Both commercial and investment banking account as well as insurance, and credit card accounts are to 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,

Purchase history of commerce site, and

Receipt Data

Out of scope:

Web Payment (will refer the W3C Web Payment WG product if needed.)

## 4) Proposed Deliverables

The group proposes the following Specification deliverables:

Read only APIs for

Commercial Bank Accounts,

Investment Bank (brokerage) Accounts,

Life Insurance Accounts,

Casualty Insurance Accounts,

Credit Card Accounts.

Write Access API including account creation but excluding web payment for

Commercial Bank Accounts,

Investment Bank (brokerage) Accounts,

Life Insurance Accounts,

Casualty Insurance Accounts,

Credit Card Accounts.

## 5) Anticipated audience or users

Financial institutions and service Providers who interacts with the financial 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 The OAuth 2.0 Authorization Framework: Bearer Token Usage

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

(Add Names)

## Anticipated contributions:

Financial API Pre-Working Draft