#OpenID Foundation Workshop

# OpenID® Foundation Financial API WG

http://openid.net/wg/fapi/

October 2016


Sascha Preibisch

CA Technologies, Principal Software Architect

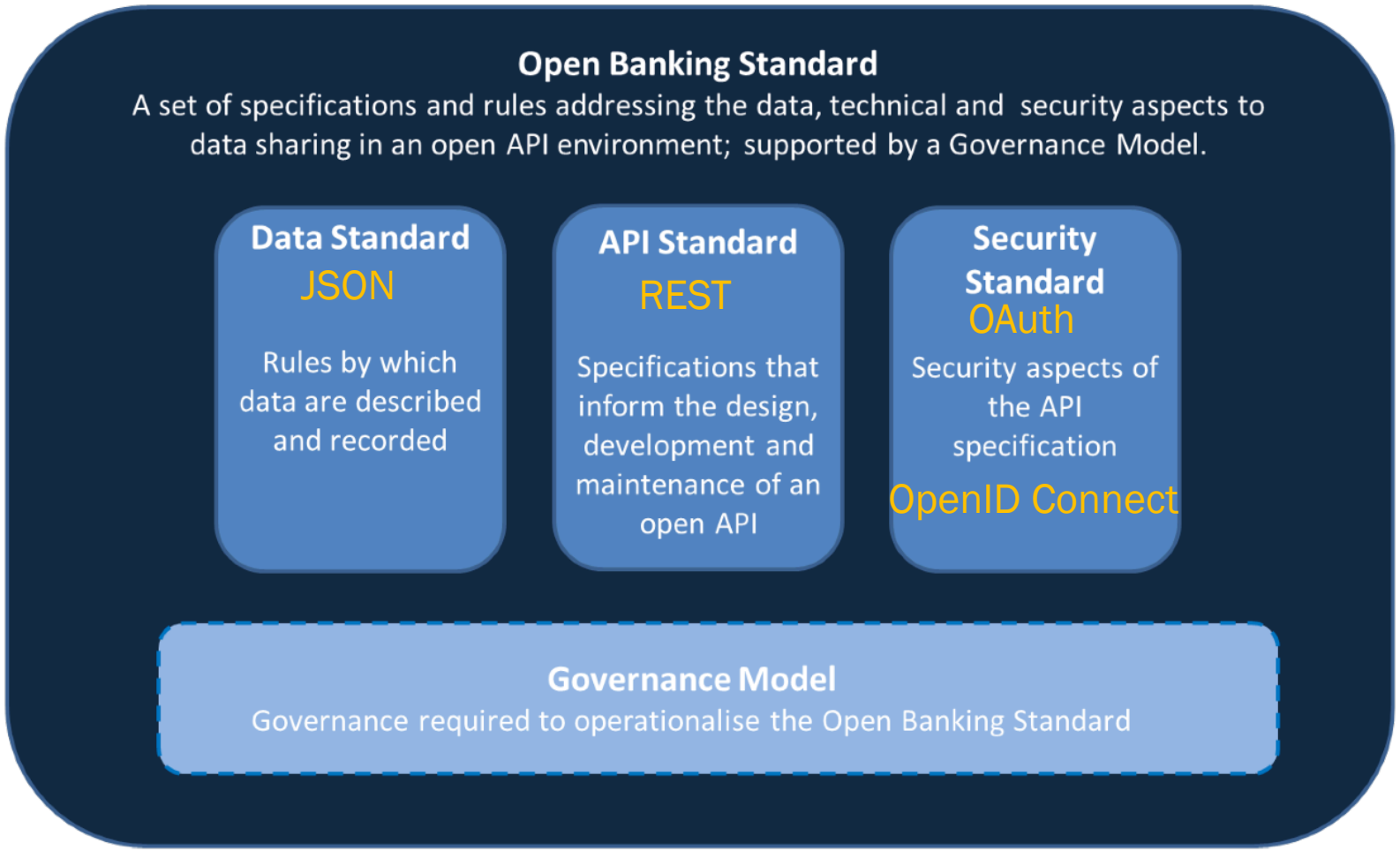
FAPI WG contributor

# OpenID Foundation
# Financial API WG (FAPI WG)

Since: June 2016

# Purpose

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




(SOURCE) ODI OBWG: The Open Banking Standard (2016)

# Enable

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

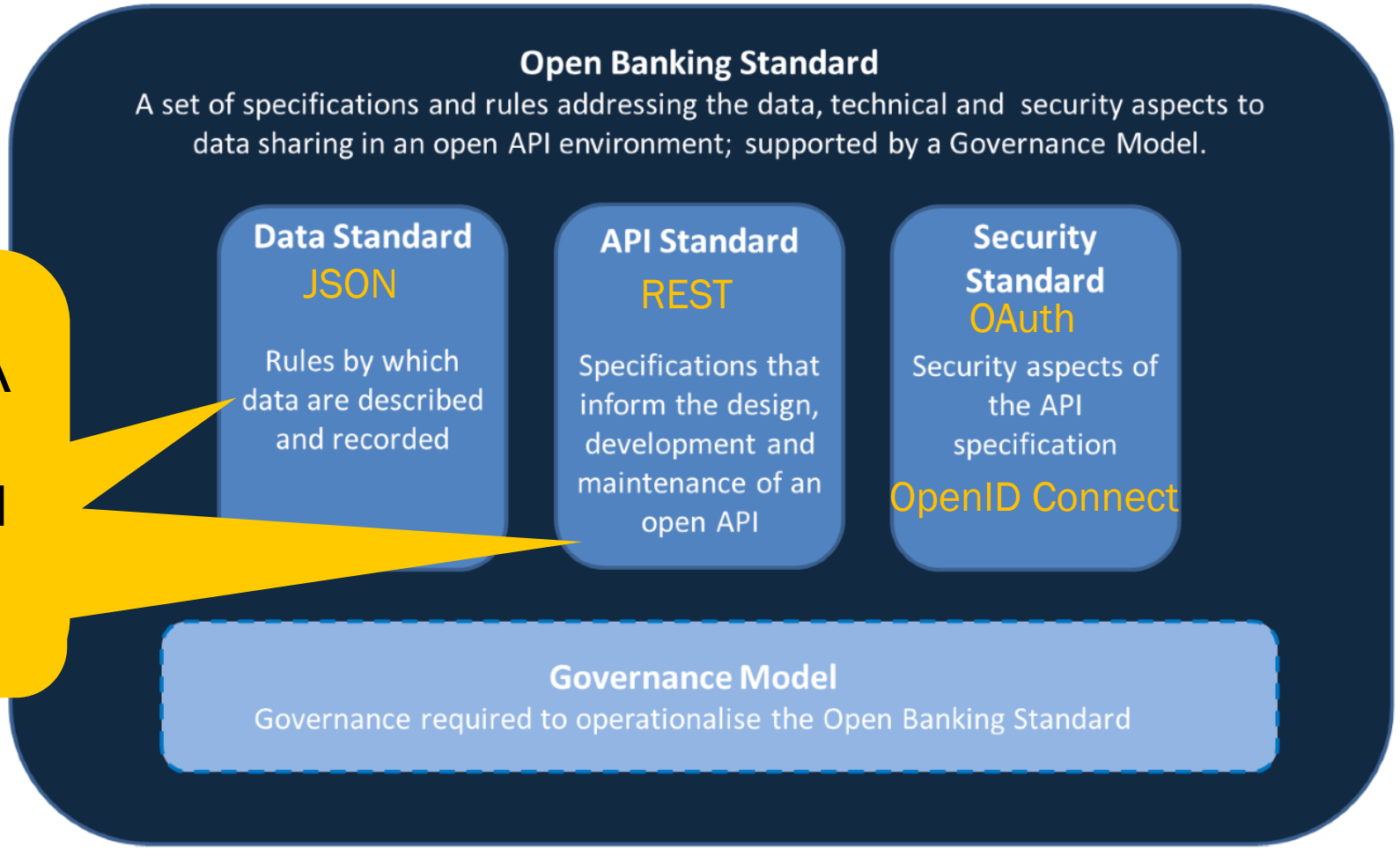
Both commercial and investment banking account as well as insurance, and credit card accounts are to be considered.

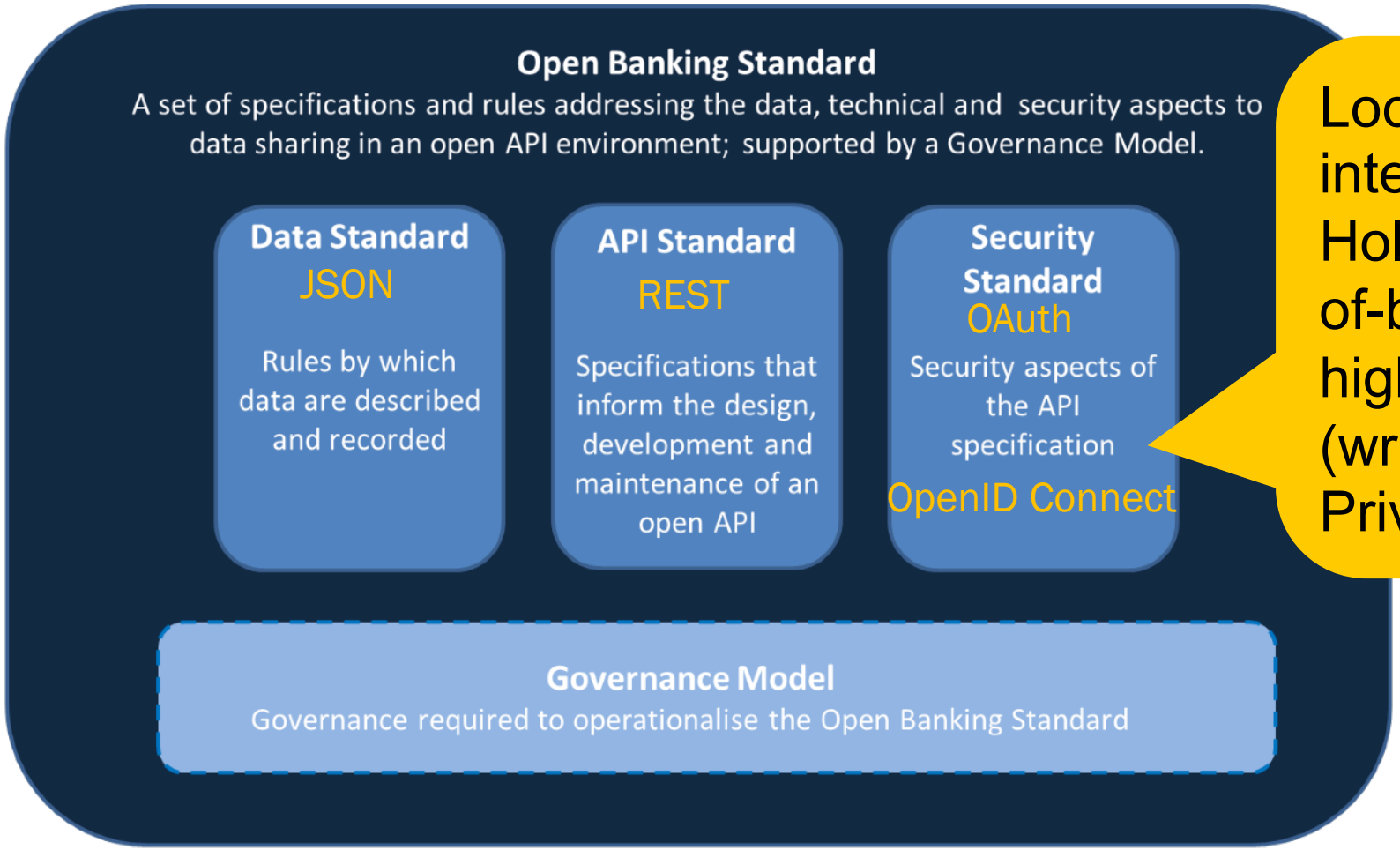
(Source) OpenID Foundation Financial API WG draft charter

It will also help foster
the FinTech companies.

# Possible Approaches

Based on FS-ISAC DDA
Internationalize
Convert to Swagger and HAL.






Locked down profile for interoperability.
Holder of Key and out-of-band authorization for higher risk scenario (write).
Privacy Considerations.

# What we have achieved so far

- Approaching the goal in two parts
  - Part I: READ access
  - Part II: READ and WRITE access
- Specified a list of API's
- Specified security requirements
- Specified error handling
- Contacted external organizations and the industry
  - EBA: European Banking Authority
  - Apigee
  - UK Implementation Entity

# Topics of FAPI working draft

- Scope and normative references
- Terms and definitions
- Symbols and Abbreviated terms
- *Getting Tokens*
- *Accessing Protected Resources (Using tokens)*
- *Resource APIs*
- *API-ID's and API Errors*
- Security and Privacy Considerations
- Acknowledgement and Bibliography

# Getting token

- SCOPE values for read operations
  - rAccount, rCustomer, rImage, rStatement, rTransaction
  - FinancialInformation equates to the ones listed above
- Redirection URI must be registered per authorization server
- User authentication with at least LoA2 as defined in X.1254
- One-Time use and short lived authorization_code
- Client Secret with an entropy of at least 128 bits

# Accessing Protected Resources

- TLS 1.2
- GET/ POST
- No support for access_token in URL
- Content-type: application/json; charset=UTF-8
- Support for CORS
- x-fapi-requestId
  - Client sends the header per request
  - Server includes in in its response
  - Especially important for server side logging

# Resource APIs

- /account*
- /availability
- /capability
- /customer
- /transfer*
- /atm*
- /products

# API-ID’s and error codes

- Each API has an assigned API-ID
- Each type of error has an assigned error-code
- Error responses include an HTTP error header
  - Header: x-fapi-err
  - Value: ‘API-ID’-’error-code’
- Errors can be handled without parsing the error message

# Once complete, consider submitting it to ISO/TC 68

- ISO 20022 Financial Services - universal financial industry message scheme.
  - Part 1: Overall Methodology and Format Specifications for Inputs and Outputs to/from the ISO 20022 Repository
  - Part 2: Roles and responsibilities of the registration bodies
  - Part 3: (TS) XML design rules
  - Part 5: (TS) Reverse engineering
  - Part 6: Message Transport Characteristics

# Join the group!

https://openid.net/wg/fapi/