Open Banking, Open Data and Financial-Grade APIs

This whitepaper has been written for Open Banking and Open Data ecosystem participants globally, including government officials and those tasked with designing such ecosystems.

March 3, 2022

Version: **Draft 1.0**

Lead Editor: Dave Tonge, FAPI WG Co-Chair

Why Open Banking?

Data is often referred to as the "new oil" of the digital economy. It is a powerful asset used by companies to improve their services and to build artificial intelligence (AI) models. However data can often be used to "lock" consumers into a service. A move to consent-driven access to all user data can break that lock, make it easier for consumers to move between different service providers and unleash a wave of innovation.

APIs are the best way to open up consent-driven access to user data and are ubiquitous in the digital world. Much of the software that we use in our daily lives is powered by services delivered via APIs[1]. The ability to get navigation directions, order delivery online, and communicate with email are use cases where data is provided via APIs. However many of these APIs are proprietary, although they may follow certain international standards, they are built to allow one company to use the services of another company. Such APIs are typically market driven and have a clear commercial rationale to be built and consumed by all parties.

There are several categories of APIs however where the commercial rationale is not as straight-forward, for example:

- Accessing bank account information (or any financial account information including checking, savings, stocks, bonds, mutual funds, and insurance)
- Initiating a payment directly from a bank account
- Accessing health information
- Accessing usage and tariff data from utility companies and telcos

Ecosystem collaboration is required to deliver these use cases, because bilateral implementations amongst all market participants is not viable at scale. Ecosystem-wide

[1] Throughout this paper, API refers to HTTP APIs made available to third parties

collaboration has emerged from industry-led efforts (with financial incentives) or reciprocity between participants, but widespread global adoption of open data APIs is hindered by several factors: :

1. Competition: By restricting access to data, company's make it harder for consumers to directly compare services, thus making it less likely for customers to move.
2. Control: Private companies prefer that any interaction with their services or data take place through an interface the company controls.
3. Security: opening up APIs is seen as opening up additional attack vectors.
4. Strategic: Many finance companies are scared of becoming high-cost "dumb pipes", i.e. providing the expensive and risky plumbing but having no interaction with the end user, (and therefore no opportunity to sell more services).

These barriers and lack of APIs in the finance sector has led to reduced innovation and increased costs in many markets. One example is accounting and tax software. Such software needs to be able to receive banking information from any bank that its customer uses. Without Open Data API access, such software either has to reach a proprietary agreement with every bank or data holder, or use expensive aggregation services that build data APIs but which are based on screen-scraping. This friction introduces security risks, reduces innovation, and makes it harder for new entrants to join the market. This fractured approach ultimately hinders consumers because they aren't able to benefit from the efficiencies that would arise from consolidating their own data.

A second example is users that hold multiple checking accounts and credit card accounts. The average American has 4 credit cards, according to the 2019 Experian Consumer Credit Review[2] and the average Brazilian has 3.6 credit cards.[3] Both fintechs and financial institutions can benefit from providing their customers a full view of their transactions and facilitate timely bill payment across their debit and credit accounts, savings, and investments.

Merchant payments is a third example. There is a clear need for merchants to be able to accept payments from consumers no matter which bank they use. The market has solved this problem through Card networks such as Visa and Mastercard. Although they provide additional services on top, part of the value proposition of such companies is simply their provision of connectivity between merchants, consumers and banks. From a technical perspective a consumer can authorize a payment from their account to a merchant using interoperable APIs instead, and merchants are interested in avenues that might yield lower costs to accept payments.

---

[2] https://www.cnbc.com/select/how-many-credit-cards-does-the-average-american-have/

[3] https://www.veriskfinancialresearch.com/reports/country-reports/latin-america/brazil.html

The last example is open health. Users often struggle to authorize the sharing of medical records between medical providers. Open Health initiatives offer a path to empower people to authorize the movement of sensitive data in a timely and secure manner.

Over the last 5 years there has been a movement to change the status quo. Starting with Open Banking, and more recently moving to Open Finance and Open Data. Much of this movement has been driven by regulators who seek to increase competition, empower their citizens and enable greater innovation.

This paper will describe this movement and provide an introduction to how the OpenID Foundation standards play a central role in many market-wide implementations.

A Global Movement

There have been services built around access to banking data for decades. Before Open Banking APIs, these services were primarily based on screen-scraping or file exchange, and screen scraping in particular posed material concerns around security. The lack of secure interoperable APIs was a significant barrier to entry and restricted innovation.

One of the first movers was Singapore, with a market-driven approach that started in 2015 and has been live since 2018 based on the key principles of user consent and “reciprocity” between banks and fintechs. There are now 1000 open APIs, serving both financial services and government use cases, and P2P payments in partnership with Thailand.

In the EU the move to Open Banking codified in the 2nd Payment Services Directive (PSD2) that was adopted into law in January, 2018 (after years of drafting and consultation). This directive was one of the first regulatory initiatives that required companies to open up API access. While most of the directive is aimed at payments, it created a new type of regulated entity - an “Account Information Service Provider”. Companies granted this permission would be allowed to access bank APIs.

At the same time in the UK the competition regulator had been investigating a lack of competition among retail banks. Having found the banks guilty of uncompetitive behavior and charging customers too much, one of its main remedies was to require the 9 largest banks to meet their obligations to PSD2 through a common API, and the Open Banking Implementation Entity was formed by these 9 largest banks to deliver on their regulatory obligations.

In Australia, the Consumer Data Right went live in July 2020 granting consumers access to their data, not just at banks, but at any financial institution, for example insurance and

investment providers. New Zealand at the moment has a market-driven approach, but is considering similar regulation to Australia.

In the US and Canada there is a market-driven approach, spearheaded by the Financial Data Exchange. This non-profit entity is *"dedicated to unifying the financial services ecosystem around a common, interoperable and royalty-free technical standard for user-permissioned financial data sharing."* [4] There are currently over 200 participants, both data providers and data consumers. The market-driven approach may be supplemented by some level of regulation, both in the US and Canada.

Brazil has taken the regulatory approach and went live in 2021, with a mandate for all data holders to comply with standards, and mandates for relying parties to comply with standards as well. Brazil is moving to Open Insurance in 2022, and Open Health in consultation now. Elsewhere in Latin America, Mexico published its Open Banking legislation and other countries are on a course to introduce similar legislation over the next few years.

India has a number of different initiatives as part of its "India Stack" that can be classed as Open Banking . The regulatory-driven Unified Payments Interface (UPI) provides the standards and connectivity for bank-to-bank payments. On the data side, the DigiSahamati Foundation (Sahamati) is a *"self-organized Industry Alliance for the Account Aggregator ecosystem."* [5]

Elsewhere in Europe, Norway, although not in the EU, falls under PSD2 regulations. Switzerland however does not. There is still a move towards Open Banking in Switzerland that is primarily market driven and started with use cases aimed at SMEs. Ukraine and Georgia adopted Open Banking legislation in 2021 with a roll out planned for this year. Germany is also very active in Open Data initiatives through the efforts of the Berlin Group and their standards work.

In Africa, a regulatory approach[6] led by the Central Bank is due to go live in Nigeria in 2022, and there are Open Banking initiatives in early stages in Kenya, Rwanda, and South Africa as well. Markets like these are likely to address important new requirements like how to enable open data on "feature phone" devices, and thereby ensure more residents have access to the services.

---

[4] https://financialdataexchange.org/FDX/About/FDX/About/About-FDX.aspx

[5] https://sahamati.org.in/about/

[6] https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf

In Japan there have been regulatory initiatives to promote Open Banking from as early as 2015, however the roll out of APIs have largely been market driven and slower than other jurisdictions applying a purely regulatory approach.

We have also seen traction in Russia, Israel, Saudi Arabia, Bahrain, and the UAE. In total there are over 20 countries actively engaged in or exploring Open Data initiatives, a movement that is cascading around the world.

Why Stop at Banking?

The same reasons that regulators are in favor of Open Banking apply to other financial products and user data more generally. There is a clear trend from Open Banking to Open Finance and to Open Data[7].

The "Consumer Data Right" in Australia is a clear example of this as is GDPR in the EU and the Brazilian Central Banks Open Banking and Open Insurance initiatives. There is a move to give users, or "data subjects" the right to access and share their data. This is a fundamental shift. Historically companies have viewed the user data they hold as their property. This new legislation changes that calculus and establishes clear rights for users.

Open Finance is a simple expansion of Open Banking. Many banks provide investment, insurance and credit products as well as bank accounts. From the user's perspective it is strange that, under Open Banking legislation, they can share their bank account data, but not their investment account data. Open Insurance and Open Finance therefore builds on Open Banking and incorporates all types of financial data.

There are a few differences though when it comes to products aimed at retirement, e.g. pensions. In many jurisdictions a user may have multiple "pensions" without online access to those pensions. This is the case in the UK where access to pension data is managed by the Pensions Dashboard Project. This project has similar data APIs to Open Banking but with a clear difference. Instead of a user verifying their digital identity directly with the data provider, the verification happens centrally through a central "consent and authorisation" [8] service. Currently this is being implemented in the UK in a siloed manner - separate from existing Open Data ecosystems. This brings significant risk of fragmentation and lack of interoperability. A better model is Australia where the CDR anticipated user requirements, and their approach is deliberately designed to encompass all financial accounts.

Open Data embraces other categories of data across the ecosystem like telecommunications, utilities, government, and health. Singapore has already started to

[7] Open Data has historically meant non-user data, e.g. exchange rates, but recently it has been used to encompass all user data, e.g. health data as well as finance data.

[8] https://www.pensionsdashboardsprogramme.org.uk/2021/05/27/architecture-brief/

enable government use cases using the same open data platform. Australia is likely to be the first market to move into utilities. Open Health Data is moving forward in the US health care ecosystem (using OpenID Connect), and a new consultation by the Brazilian government announced this year to enable Open Health as well. It is worth noting that both health and government sectors have been slower to adopt API-based technology stacks, but the pressures of Covid (testing and vaccination) and the acute challenges of government benefit fraud are forcing the health and government sectors to reassess the technology infrastructure needed to meet this moment.

Market-driven or Regulation-Driven

Globally there have been two approaches to Open Banking: market-driven or regulation-driven.

Market Driven

Some jurisdictions, notably the USA and Singapore have let the market take the lead when it comes to Open Banking. Market driven approaches may be better at aligning incentives, and avoiding the pitfalls of a regulatory approach. For example, sometimes regulation is too prescriptive, such as the Payment Services Directive (PSD2) mandate that users must re-authorize data access every 90 days. While this requirement was designed to protect consumers, it had unintended consequences. Many users were forced to re-authorize their use of a service, disrupting their user experience. Furthermore, this PSD2 requirement disproportionately affected some consumers and business models over others[9]. Potential downsides of market-driven approaches is that they may take more time to implement, and the incentives may not be sufficient to ensure the ecosystem wide-adoption. Open data initiatives are exposed to the risks of network effects. If there are not a critical mass of users or data holders the ecosystem itself cannot achieve the flywheel effect needed to ensure users see their data across their accounts. Furthermore, the incentive models may not be sufficient to motivate service providers to serve all users, leaving segments of the population behind.

Regulatory Driven

In many jurisdictions like the UK, Australia, and Brazil, regulators have taken the lead in crafting legislation that requires banks to open up API access, with clear mandates and timelines for key market participants.

---

[9] PFM software was less affected by the rule than synthetic overdrafts. In addition consumers with multiple bank accounts were effectively penalized as they had to go through far more regular re-authorisation flows.

There are four clear public benefits to Open Banking which policy and regulation tends to address:

1. Competition
2. Innovation
3. Data Transparency
4. Regulation and Registers

1. Competition

Enabling competition was the driving force in the UK. In fact, Open Banking was launched in the UK by its competition regulator, the CMA (Competition and Markets Authority). The CMA's investigation into retail banking identified a lack of competition among the main UK banks and found that end-users were suffering from a lack of transparency about fees and charges. The CMA decided that requiring banks to provide API access to user data would make it possible for new services to aid consumers in finding the best bank for their circumstances.

Comparing banking products, switching bank accounts and operating multiple bank accounts are all things that Open Banking aims to make easier. These services are made possible by allowing access to transactional data via APIs such as:

- Account aggregation services - by making it easier for consumers to see all their accounts in one place, consumers can make use of multiple products from different banks at the same time,rather than being locked in to use a single provider.
- Accurate account comparison - consumers can be shown exactly how much they would have paid in bank fees had they been using a different bank account product
- Synthetic overdrafts - companies can provide automatic short term credit products to consumers that function in a similar way to overdrafts

If the UK driver for regulation was "user access to data", the EU's primary driver for Open Banking was payments. By forcing banks to allow API-driven payments, EU policymakers hoped to break the monopolies of the card networks, and introduce more competition. An important condition of the EU's 2nd Payment Services Directive was the requirement that banks couldn't charge any fees or require any contract for "Payment Initiation Service Providers" to initiate payments. The aim was to allow European-based payment institutions an ability to offer continent-wide payment services that avoided the "payment rails" of the US-based card networks.

In Australia, competition was also a primary driver of the "Consumer Data Right" legislation. The project overview states:

> *"CDR will give consumers greater access to and control over their data and will improve consumers' ability to compare and switch between products and services. It will encourage competition between service providers, leading not only to better prices for customers but also more innovative products and services."* [10]

Other regulators internationally have used a similar rationale.

One meaningful exception is Singapore, where the concept of reciprocity of information between banks and fintechs helped facilitate the development of 1,000 APIs without regulation or transaction based compensation; a different way to address competition between financial institutions and fintechs.

2.Innovation

As noted by the Australian introduction to the CDR, innovation is another key driver in the move to Open Banking. Australian regulators recognised the innovation that API's enabled in the wider economy and were keen to boost innovation in financial services.

The UK was the same. The 2016 report that led to the UK's Open Banking regulation introduced the innovation benefits of APIs as follows:

> *"API technology is the accepted norm for data-sharing and embedding functionality in an online environment. The use of APIs is widespread and today there are more than 14,000 public APIs available. The most popular APIs include familiar names such as Facebook and Google Maps, which are widely used across the Web to embed "like" buttons and maps. Many websites make extensive use of other companies' APIs, which has resulted in a significant amount of innovation and consumer convenience. APIs are a fundamental component of enabling an Open Banking Standard."* [11]

At a stroke of a pen, regulators have been able to give a springboard for innovation in financial services. In the year following the regulations going live in he UK, over 100[12] companies (many of them newly established) gained regulatory permissions to access the Open Banking ecosystem in the UK. Many innovative products have been launched and as of January 2022, there were 5 million[13] active users of Open Banking based services in the UK.

---

[10] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

[11] http://theodi.org/wp-content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf

[12] https://content.11fs.com/reports/open-banking-in-the-uk-whats-happened-so-far

[13] https://www.openbanking.org.uk/news/open-banking-passes-the-5-million-users-milestone/

3. Data Transparency

The EU's GDPR has had a significant impact on the approach companies take to data, even beyond the EU. It codified numerous rights of "data subjects". One of these rights is the "right to data portability", that requires the data subject to be given access to their data in a "structured, commonly used and machine-readable format" and "have the right to transmit those data to another controller". [14] In the GDPR this is a general right, and data controllers have many ways of complying with it. The data access side of Open Banking is essentially a more prescriptive implementation of this right. By ensuring that banks have to provide the same API access and provide this access without hindrance to registered third party providers, regulators have been able to increase data transparency for data subjects.

4. Regulation and Registers

A defining aspect of most Open Banking regulation is that a register of entrants is created and rules are drafted governing which companies can be on the register. This is an important distinction to most other API ecosystems which are usually controlled by private companies. In contrast, existing financial regulators are often tasked with the job of determining which companies can and can't be on the open data registers, and they then implement those rules through policy and operational controls. By default, the technical interaction with a central register gives the private entity or the local government a control point over the ecosystem. Some governments conclude that the private sector will do the best job of performing this governance function, some conclude the government is best served to perform this function, and others have a hybrid model with government oversight of an open banking management entity.

Implementation Considerations

There are a number of important decisions to be made by ecosystems rolling out Open Banking or Open Data APIs. Here are some of the most important ones based on the OpenID Foundation's observations.

Functional Specifications

The actual functional APIs that are used to exchange data or initiate payments are likely to be ecosystem specific. These are the APIs that are used for example to:

- Fetch 3 months of checking account data

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2753-1-1

- Make a utility payment
- Get the latest account valuation

Functional specifications usually depend on the use cases that a market is aiming to achieve, the data they want to open up to users, and operational requirements. These functional specifications are also easier to extend and adapt over time. In contrast, making changes to a security profile is high-cost and high-risk.

This is a central reason why it's important that ecosystems separate out security profiles from functional APIs. This is a key design consideration that OAuth 2.0 recommends, and that the OpenID Foundation recommends, and it enables a healthy separation of concerns. The security profile should cover participant authentication, consent, authorization, and secure access. A domestic market can enjoy all the benefits of control over the functional specifications, while benefiting from a global standard for the security profile.

Early on the FAPI WG did consider standardizing functional APIs but concluded it wasn't practical, nor was there market demand, at that time. This may change as interest in supporting cross-border use cases matures.

Choosing the security profile

Some ecosystems develop their own security profiles, for example India and Singapore. To date, most markets have selected FAPI as a global standard, including FDX (for US and Canada) UK, Australia, Brazil, Nigeria, New Zealand, and Russia. Of the markets that selected FAPI, some markets such as the UK and Brazil wanted to add additional security requirements beyond the FAPI standard. They developed "domestic" FAPI profiles in partnership with the OpenID Foundation to ensure they would stay as close to the "main" FAPI profile as possible. There is also an example of a market that selected the FAPI standard, but developed a domestic FAPI profile locality, Russia. If there are additional security requirements meriting a domestic profile, the OpenID Foundation recommends doing this work in partnership with the OpenID Foundation to increase the number of "eyes" on it during the development, and help reduce the local market costs of maintaining it over time.

One of the key benefits of choosing FAPI and partnering with the OpenID Foundation, is access to the conformance test suites. These tests allow local markets to reduce test development costs, time to market, and reduce security and operational risks to benefit all market participants. To the degree a market wants a domestic profile, the OpenID Foundation can also partner with local markets on domestic profile test development, certification, and maintenance.

Certification Mandates versus No Mandates

The OIDF has observed that mandates do help overcome reticence to implement (UK, Brazil). If there are not adequate incentives to motivate participants to implement, and to do so in a timely manner, it is challenging to achieve scale that motivates users to transact and participants to implement the APIs. Brazilian central bank mandates have proven to be a useful tool to secure marketwide certification of data holders (e.g. banks), and relying parties are likely to have a mandate as well. It is worth noting that certification on production systems is required to ensure the full benefit of interoperability that "just works."

Oversight

It is important that an OpenData ecosystem has the right oversight and governance. In market-driven jurisdictions this is usually handled by the collective that defines the API standards. However in regulatory systems there are a number of approaches. Occasionally a regulator does the job (Brazil), at other times specific entities are created with independent trustees (UK). It is important that the organization which has the oversight role in an ecosystem has sufficient resources to ensure that all participants are operating in line with the rules and guidelines of the ecosystem.

Customer Experience Guidelines

As well as technical rules around APIs and policy rules around requirements for access, it is important that there are guidelines around user experience. This can ensure a consistent approach across participants and prevent data providers putting up unnecessary friction for end-users.[15]

Mobile Apps

A naive implementation of an Open Banking API may be purely web-based and not consider mobile apps. This would be a mistake as in some jurisdictions most banking interactions take place via mobile apps. The FAPI specs support two different ways of support mobile apps:

1. App to App Redirection

This is where a user is redirected seamlessly between apps as part of an authorisation flow. The main FAPI specs support this flow, however it is important that regulation-driven open

[15] An example of this can be found in the UK: https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/section-a/latest/

data rolls outs mandate that this approach is supported. It provides an excellent user experience coupled with strong security guarantees [16].

2. Decoupled Authentication

This flow involves a user authenticating on a different device from the one where they are receiving a service. It can be used to enable a user to authenticate on their smartphone while at a point of sale terminal. FAPI supports this flow via its Client Initiated Backchannel Authentication (CIBA) profile.

Some markets like Nigeria are keen to support users with feature phones, which rely upon USSD standards for text based mobile use cases. The OpenID Foundation is working with Nigeria, and the FAPI and MODRNA WGs to actively explore how to support feature phone users in Nigeria and beyond, while maintaining a high level of security.

Choosing Open Data Standards

Regulators and market initiatives have a clear rationale for Open Banking and Open Data APIs. But what standards should those APIs follow?

There are three primary questions to answer:

1. What data model to use
2. What data format and transport to use
3. How will the APIs be protected and access authorized

Data Model

The data model question, while important, is not too difficult to solve. Many ecosystems have opted for data models based on ISO20022. This substantive work by the ISO standards community helps define what a “balance” is and defines different account types. Whether jurisdictions adopt ISO20022 or not, the clear requirement is that data models and schemas are clearly defined and documented. Markets that are interested in international interoperability of data and payments as some part of their roadmap, may want to choose ISO20022 to reduce the risk of a future development burden.

[16] https://openid.net/2019/10/21/guest-blog-implementing-app-to-app-authorisation-in-oauth2-openid-connect/

Data Format & Transport

This question is again relatively easy. Most ecosystems have adopted RESTful JSON APIs, as this is currently the most ubiquitous approach in the wider market. Some ecosystems also support XML, especially if there are legacy APIs that have existing defined XML messages.

API Security

All of these initiatives have the following technical requirement:

- To allow a user to securely grant access to their data or services at one company to another company

There are usually some additional requirements:

- To only allow eligible and conformant companies to request access
- To allow customers to grant fine-grained access
- To allow customers the ability to revoke access they have granted

The above problems can't simply be solved by generic http APIs used between two bi-lateral parties, or amongst entities in a private ecosystem. There needs to be a secure interaction between three or more parties that will work on a federated basis, with all participants implementing the same standard under the same governance model.

The Inception of FAPI

The most widely used standard used to meet the requirements of a federated ecosystem is OAuth 2.0

OAuth 2.0 was published by the Internet Engineering Task Force (IETF) in 2012. It is an Authorization Framework that is widely used to enable third party access to data and services. It is a framework and can be implemented with varying degrees of security depending on the services it is being used to protect. Most tech companies who allow third party access to their data or services use OAuth 2.0 already.

OAuth 2.0 alone is not a solution to the above requirements of an open banking ecosystem. This is where the OpenID Foundation's specifications come in.

OpenID Connect Core was published by the OpenID Foundation in 2014 as an "identity layer on top of the OAuth 2.0 protocol". It made it possible for users to perform "social logins" by "signing in" and verify their identity to third party services. It has been implemented by Google, Microsoft, Apple and others and is used by billions worldwide for B2C, B2B and B2B2C use cases across verticals. As part of the design of OpenID Connect additional security mechanisms were specified that increased the security of OAuth 2.0.

In 2016 the OIDF Financial API Working Group was formed with the specific goal of providing security recommendations and specifications to enable secure APIs in financial services. The working group soon focussed on 2 security profiles, now referred to as FAPI 1.0 Baseline and FAPI 1.0 Advanced. These 2 profiles built on the work of OAuth 2.0 and OpenID Connect to provide an opinionated secure profile of OAuth 2.0 suitable for use in financial services.

The profiles developed in the FAPI WG are written in a "checklist" style and have a set of automated conformance tests that developers can use to verify that their software is implementing the profile correctly. These standards were not developed in isolation, rather early on the working group sought out collaboration with the Open Banking Implementation Entity (OBIE) in the UK, ISO TC68, the Brazilian Central Bank, the Australian Consumer Data Standards body, Financial Data Exchange (FDX), FDATA and many others.The FAPI 1.0 standard has also been subject to comprehensive security analysis by the University of Stuttgart using their WIM method[17].

This work then led to the OBIE, the first regulatory driven Open Banking initiative, to require the use of the FAPI standards for banks and third parties in its ecosystem. As well as the UK, the FAPI standards were subsequently adopted by:

- USA & Canada (through the Financial Data Exchange)
- Australia
- Brazil
- Nigeria
- New Zealand
- Russia[18]
- ISO TC68 SC9 WG2 - WAPI[19]

In fact, the majority of markets that have moved into Open Banking / Open Data have selected the FAPI standards (although the largest single implementation is in India). The FAPI standards provide the building blocks to solve the hardest problems of a consent-driven Open Data roll out, and the rest of this paper will describe how.

[17] Daniel Fett, Pedram Hosseyni, and Ralf Küsters, An Extensive Formal Security Analysis of the OpenID Financial-grade API. 2019 IEEE Symposium on Security and Privacy (S&P 2019). (Technical report.)

[18] https://www.cbr.ru/StaticHtml/File/59420/Standart_08072021.pdf

[19] https://www.iso.org/standard/74353.html

Why Choose the FAPI Security Profile

While some ecosystems develop or "roll" their own security profiles, there are significant advantages to choosing the FAPI standards and services provided by the OpenID Foundation.

Proven Technology

FAPI is proven. It has been implemented at scale in multiple jurisdictions. Choosing FAPI reduces operational risks of failure.

Secure

The FAPI standards are secure. As well as surviving large numbers of penetration tests, they have also had formal security analysis[20] from leading academic security researchers. The FAPI working group contains security experts who found and pushed for a fix to a "Cross Browser Payment Initiation Attack" [21] that was present in several PSD2 APIs. Unlike proprietary or market specific implementations that are limited in the number of "eyes" looking at the code, the FAPI standards (and OAuth and OIDC) benefit from hundreds if not thousands of "expert eyes" on the open standards, globally.

Cost Saving

Choosing FAPI significantly reduces costs for ecosystem participants. FAPI security profiles have already been implemented by most vendors in the IAM industry. This means less costly customisation or bespoke work is required if an ecosystem choses FAPI, and it also reduces the vendor lock-in and switching costs downstream. Furthermore there are multiple open source libraries that implement OpenID Connect and FAPI that can be used by data receivers in an ecosystem to accelerate implementation.

Furthermore, by choosing FAPI, ecosystems can take advantage of economies of scale. Multiple ecosystems, vendors and experts are working to ensure that the FAPI standards are secure and maintained. This saves costs vs maintaining bespoke standards.

Conformance Tests

Choosing a standard is not enough to ensure interoperability. The only way to ensure that different pieces of software have implemented a standard correctly is through comprehensive conformance tests, and to ensure all parties are tested before implementation and define a reasonable cadence of recertification over time. This

[20] https://arxiv.org/abs/1901.11520

[21] https://bitbucket.org/openid/fapi/src/master/TR-Cross_browser_payment_initiation_attack.md

conformance approach ensures consistent user experience, greatly reduces support costs, and enables data providers and data consumers to confirm that they comply with the standards and their obligations to the ecosystem. In ecosystems where there are no conformance tests, there is often a higher implementation and support cost for both data providers and consumers, often with extensive diligence to remediate issues that impede interoperability. This is because developers may either make mistakes, or interpret a clause in a standard differently. Conformance tests ensure that these issues are caught and fixed during development which is far and away the best time to make corrections.

The OpenID Foundation offers certification as an optional service to the global community. The OpenID Foundation uses a self-certification approach which ensures a low cost model for those that wish to or are required to certify (pricing is currently $1k/ certification for Members, and $5k for non-members). There is also a free test bed available to market participants, and all tests are open source and actively maintained to ensure alignment with the standards. As of February 2022, the Foundation has certified 244 FAPI deployments globally for a total of 739 certifications with the number of certifications consistently increasing. The UK and Brazil mandated OpenID Foundation certification as part of the due process to register participants, an approach recommended by the OpenID Foundation. The latest FAPI Certifications can be accessed here, as all certifications conducted by the OIDF are made public. https://openid.net/certification/#FAPI_OPs.

The OpenID Foundation maintains several suites of conformance tests, with some suites geared towards particular ecosystems. Some regulators, e.g. the Central Bank of Brazil, require Data Providers to prove conformance to a standard using the OpenID Foundation certification program. Some markets like US/Canada (FDX), Russia, and Australia have selected FAPI, but they have not chosen to use the OIDF certification program at this time.

Global Interoperability

By choosing FAPI, ecosystems retain a path to global interoperability and cross-border use-cases. For example transferring medical records, identity records or opening financial accounts across borders can all be made simpler if a common security profile is used. Market participants that want to support users and entities with cross-border requirements are already exploring how to converge open data standards to enable these use cases.

What if FAPI Is Not Selected

Open Banking is by nature a domestic-market led initiative, and it is likely to remain so for many years to come. A handful of markets will have the interest and capacity to develop bespoke open-banking standards.

Several leading markets like Germany, India, and Singapore all pursued domestic standards to support their local Open Data requirements. India can be applauded for being the largest scale Open Data implementation, and Singapore for their reciprocity approach. Germany is globally recognized as a thought leader in security standards work. The OpenID Foundation recognizes the expertise and strengths of these markets, and is engaged with all three to explore opportunities to converge efforts, and right now global interoperability is proving to be a fertile area of shared interest.

Most markets will probably not want to develop their own security profile, and instead will select FAPI to meet their security requirements. Markets can benefit from all the security advantages of a globally proven open standard, at no cost, while maintaining full domestic control of all aspects of the implementation.

OIDF seeks to engage bi-laterally with all markets to support their needs, both those that select FAPI and those that do not. In addition, OIDF is the "co-convenor" of the Smart Data Foundry Technical WG in which representatives from over 20 countries convene on Open Data, including government, private sector, and academia meet to discuss standards convergence, identify key academic topics of interest,and share best practices with a wider community.

The FAPI Specifications

The FAPI Working Group produces and maintains many different specifications and documents. These all have the aim of providing ecosystems with secure and interoperable specifications for financial-grade APIs.

While the main documents that are often referred to simply as FAPI, are the OAuth 2.0 security profiles, there are four different types of document within the working group:

- Security profiles of OAuth 2.0 and other specifications - that aim to provide specific implementation guidelines for security and interoperability (e.g. FAPI 1.0 and FAPI 2.0)
- Specifications that describe new endpoints or operations (e.g. Grant Management). Such documents are usually created out of specific requirements that FAPI WG members discover in ecosystems implementing FAPI security profiles.
- Implementation advice, guidance and security advisories (e.g. Cross-Browser Payment Initiation Attack)
- Specifications that FAPI WG members submit to the IETF OAuth Working Group and work with colleagues there to publish as RFCs (e.g. RFC9126 - OAuth PAR)

Documents are taken through a rigorous process before being published as final specifications. This includes public review periods, implementers drafts and often formal security analysis.

An overview of the key documents as of March 2022 can be found in Appendix 1

The Future of FAPI

Moving forward there are 3 key areas that the OIDF is exploring with relation to FAPI:

1. Market Lifecycle Support

With 20+ markets actively exploring or implementing Open Banking, the OpenID Foundations will be sharing our knowledge on Open Banking, FAPI, and (if they select FAPI) we will support their implementations.

2. FAPI 2.0 Framework

The FAPI Working Group is taking learnings from the implementation of FAPI 1.0 to create a framework for FAPI 2.0 that will provide all of the standards necessary to implement an Open Data ecosystem. This includes work on new specifications such as Grant Management and Dynamic Client Registration as well as deployment advice. Given some markets are adopting the FAPI 2.0 standards this year, and the OIDF is progressing Security Analysis on both the FAPI 2.0 baseline & advanced specifications starting March 2022.

3. Global Interoperability

In an increasingly interconnected world there is an appetite for global interoperability, whether that is for cross-border payments or the secure transfer of health data. The OIDF is collaborating with a number of organizations to explore this area, including those that have not selected FAPI. In addition, the Foundation is working on the Global Assured Identity Network (GAIN) which has similar aims to support global interoperability for assured identities.

4. Usage in other verticals

Originally the FAPI Working Group was focussed on APIs within financial services and it was called the Financial API Working Group. However the name was changed to “financial-grade” API to reflect the fact that its security profiles are suitable for APIs in other verticals beyond finance. The foundation is focussing on all aspects of Open Data including Finance, Insurance, Health, and government use cases. Some use cases like insurance may not require any changes to the FAPI standards (as per Australian Consumer Data Standards).

The Foundation is conducting a study of the Health sector to discuss the fit of FAPI to serve health initiatives in the US, Norway and UK, which will lead to a whitepaper and recommendations for the global health community.

Convergence of Open Data with other e-Government initiatives like eIDAS 2.0 (EU Digital Wallet) and the digital credential issuance under the ISO 18013-5 mobile driving license and W3C Verifiable Credential standards is more complex. The OpenID Foundation is working on a whitepaper for government officials to address the convergence of eGovernment, Health, and Open Data alongside their longstanding concerns about cybersecurity, identity and access management, and digital transformation..

The OpenID Foundation

The OpenID Foundation is a non-profit standards body whose vision is to help people assert their identity wherever they choose. It's mission is to lead the global community in creating identity standards that are secure, interoperable, and privacy preserving.

As the foundation has a wider remit than pure standards bodies such as the IETF it is able to help to markets implementing Open Data APIs to reach their goals. The Foundation does this in many ways such as:

- Sharing OIDF learnings from other markets
- Ensure market participants understand the FAPI standard and what it can offer
- Establish partnerships with local government and Open Banking management entities, and with global entities in the Open Banking domain
- If the FAPI standard is selected, provide market support:
    - Webinars to explain the standards to local implementors
    - Ensure any local requirements are met by the FAPI standard, such as local security profiles
    - Provide certification support that aligns to market processes and requirements
    - Help remediate issues
    - Discuss other standards that may fit their local roadmap in the future, e.g. OIDC for Identity Assurance, Shared Signals and Events
    - Help the global community explore how global interoperability o

This support is offered without cost or obligation, unless there is market specific development work or certifications required. The Foundation is primarily funded through membership. All market participants are warmly encouraged to join the Foundation (www.openid.net) to help deliver on the OpenID Foundation's vision and mission.

Conclusion

Open Banking, Open Finance and Open Data have arrived and are here to stay. The manner in which ecosystems implement them can have a profound effect on costs, innovation and security.

The OpenID Foundation is committed to providing open and interoperable security standards that can enable this movement. By using the FAPI specs, ecosystems can take advantage of security standards that are proven and rigorous, and leverage existing certification test suites to ensure FAPI compliance.

The OIDF warmly welcomes individuals, companies and organizations to join the OpenID Foundation to support the work on the all of our standards (www.openid.net), including the FAPI family of standards.

Like all OIDF working groups, the FAPI Working Group operates in a transparent manner, anyone can join and contribute simply by signing a contribution agreement.[22] There are regular weekly calls, a mailing list and an issue tracker to keep the global community connected[23]. More on the FAPI WG here: https://openid.net/wg/fapi/.

If you are working for an Open Finance or Open Data initiative and would like to learn more about the OpenID Foundation we can support your goals both domestically and internationally then please reach out to director@oidf.org, we look forward to working with you.

[22] There is no cost associated with this agreement, more information is available here https://openid.net/intellectual-property/

[23] https://openid.net/wg/fapi/ and https://bitbucket.org/openid/fapi/issues

Appendix 1 - FAPI Specifications

Financial-grade API Security Profile 1.0 - Part 1: Baseline

Status: Final
Location: https://openid.net/specs/openid-financial-api-part-1-1_0.html

This is a secure profile of OAuth 2.0 that is suitable for protecting APIs with a moderate inherent risk. It has been through a rigorous review process and is published as a final specification.

This specification was originally called the “Read-Only API Security Profile”, but its name was changed to reflect the fact that in many ecosystems “read” APIs are just as sensitive as “write” APIs.

Mode ecosystems, implementing FAPI 1.0, require the use of the advanced profile - however this profile is the only FAPI spec that supports public clients (i.e. software that runs in a browser or in a mobile app that communicates directly with an authorization server and which shares a single client identifier).

Financial-grade API Security Profile 1.0 - Part 2: Advanced

Status: Final
Location: https://openid.net/specs/openid-financial-api-part-2-1_0.html

This specification builds on FAPI 1.0 - Part 1: Baseline and is suitable for protecting APIs with high inherent risk - it is also at the final specification stage.

This specification was originally called the “Read and Write API Security Profile”, but its name was changed to reflect the fact that in many ecosystems “read” APIs are just as sensitive as “write” APIs.

This is the most widely implemented FAPI spec. Most implementations use it as an extension of OpenID Connect, however it can be implemented on a “vanilla OAuth 2.0” server.

Financial-grade API: Client Initiated Backchannel Authentication Profile

Status: Implementers Draft
Location: https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_CIBA.md

As part of the ongoing liaison with PSD2 initiatives in Europe the following three types of interaction between the user and the financial institution were identified:

- Redirect - the user is redirected from the data consumer to the data provider for authentication on the same device (this is the standard OAuth 2.0 based method of interaction)
- Decoupled - the data provider initiates the authentication of the user on a different device
- Embedded - the data consumer collects the users credentials and passes them through to the data provider

FAPI CIBA is a profile of the OpenID Connect's CIBA specification that supports the decoupled flow. There are many use-cases that require a decoupled flow, for example using FAPI APIs to support a Point of Sale terminal.

Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

Status: Implementers Draft
Location:
https://bitbucket.org/openid/fapi/src/master/Financial_API_JWT_Secured_Authorization_Response_Mode.md

This specification was created by the working group to bring some of the security features defined as part of OpenID Connect to OAuth 2.0. Many implementations of FAPI 1.0 - Advanced, use the ID Token as a detached signature to protect the authentication response. JARM defines a way for servers to sign authentication responses without having to use an ID Token.

FAPI 2.0 Baseline and Attacker Model

Status: Implementers Draft
Location: https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Baseline_Profile.md & https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Attacker_Model.md

FAPI 2.0 has a broader scope than FAPI 1.0. It aims for complete interoperability at the interface between client and authorization server as well as interoperable security mechanisms at the interface between client and resource server.

As a consequence, FAPI 2.0 provides mechanisms for obtaining fine-grained and transactional authorization for API access and security mechanisms for replay detection in addition to the mechanisms already defined in FAPI 1.0 focusing on the security of the authorization flow.

The working group also evolved the profile to be easier to use for developers based on the results of an analysis of various open banking implementations, the recommendations of the latest OAuth Security BCP, and a comprehensive security threat model.

FAPI 2.0 Advanced

Status: Working Group Draft
Location: https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Advanced_Profile.md

The advanced profile is an extension of the baseline profile and provides non-repudiation for all exchanges including responses from resource servers.

Grant Management for OAuth 2.0

Status: Implementers Draft
Location: https://bitbucket.org/openid/fapi/src/master/fapi-grant-management.md

This profile specifies a standards based approach to managing “grants” that represent the consent a data subject has given. It was born out of experience with the roll out of PSD2 and requirements in Australia.

RFC8705 - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

Status: Final
Location: https://www.rfc-editor.org/rfc/rfc8705.html

The authors of this specification are FAPI WG members and it is a fundamental building block of many FAPI implementations. Many financial ecosystems were already using Mutual TLS - so it made sense to specify an interoperable way to use mutual TLS together with OAuth 2.0.

RFC9126 - OAuth 2.0 Pushed Authorization Requests (PAR)

Status: Final
Location: https://www.rfc-editor.org/rfc/rfc9126.html

An early version of this specification was defined in an implementers draft of FAPI 1.0. It provides a mechanism for the authorization request parameters to be “pushed” to the server rather than passing them through the front-channel. It brings security and simplicity at the cost of 1 additional API call.

OAuth 2.0 Rich Authorization Requests (RAR)

Status: Draft
Location: https://www.ietf.org/archive/id/draft-ietf-oauth-rar-10.html

This document is on a standards track in the IETF OAuth Working Group. It is an optional part of FAPI 2.0 and it provides an interoperable way to provide complex authorization data, for example the type of data needed to initiate a payment. Traditional OAuth 2.0 based deployments use coarse-grained scopes to signify the operation a user is granting access to (e.g. “read profile”, or “publish to timeline”). Our experience with FAPI has shown that such coarse-grained scopes are not enough for many use cases. Many ecosystems have implemented their own custom way of communicating rich authorization data - RAR defines a standard for this.

FAPI Developer site: https://fapi.openid.net/

Appendix 2 - Glossary

Term	Definition
OAuth 2.0	The OAuth 2.0 Authorization Framework (RFC6749)
OIDC	OpenID Connect Core - a simple identity layer on top of the OAuth 2.0 protocol
Authorization Server	The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization. In the context of Open Banking this is the Bank.
Client	An application making protected resource requests on behalf of the resource owner and with its authorization. In the context of Open Banking this is the Third Party.
Resource Owner	An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end-user.
Data Provider	A company that holds data on an end-user - in the context of OpenBanking this would be a bank
Data Consumer	A company that consumes data from a data provider for an end-user, in the context of OpenBanking this would be a third party provider
OIDF	The OpenID Foundation - a global standards body focussed on digital identity and security standards.
IETF	Internet Engineering Task Force - a global standards body that publishes RFCs