Open Banking and Open Data go Global

DRAFT

22 June 2022

Working Draft v.03

Lead Editor: Dima Postnikov

Table of Contents

DRAFT

DRAFT

Introduction

There is a global movement towards open banking and open data, but each market is implementing their own version.

The next big challenge is how to enable global interoperability and unlock cross-border use cases, and this paper explores global relying party demand and outlines what “good might look like” and how to get there.

This paper is written for the following audience: government and private sector thought leaders working on open banking, open data, cross-border payments, cross border identity, and international trade.

This whitepaper is a part of series of whitepapers by various OpenID Foundation groups:

- Open Banking, Open Data, and the Financial Grade API.
- The Global “Open Health” Movement: Empowering people and saving lives by unlocking data.
- OpenID for Verifiable Credentials.

DRAFT

Open Data ecosystem evolution

The need to expose customer data to external parties is not new. It has existed for a long time with legacy solutions using files, batch processing and message queuing to get data from the source to its destination.

Customers often were unaware that their data had been shared between different parties. Sometimes this has been covered by T&Cs and other legal disclaimers, sometimes it was just implied.

Changes to privacy expectations and regulations have introduced a requirement of customer's control of their data. It's become a norm that an end-user needs to provide an 'informed consent' for their data to be shared with external parties.

With the development of secure API frameworks, it is now possible to share customer data securely with explicit consent enforcement.

Open data ecosystems are API based access frameworks that expose user's data to trusted parties with the user's consent.

These Open Data ecosystems did not start with open banking. They typically go through 3 phases of evolution:

Phase 1: Private ecosystems exposing public APIs.
Phase 2: Open banking ecosystems.
Phase 3. Cross industry ecosystems

Note: apart from the API initiatives described, other types of integrations are still used in the wild like screen scraping, batch extracts or "customer download and share". This paper only focuses on API based integrations.

Phase 1: Private API ecosystems

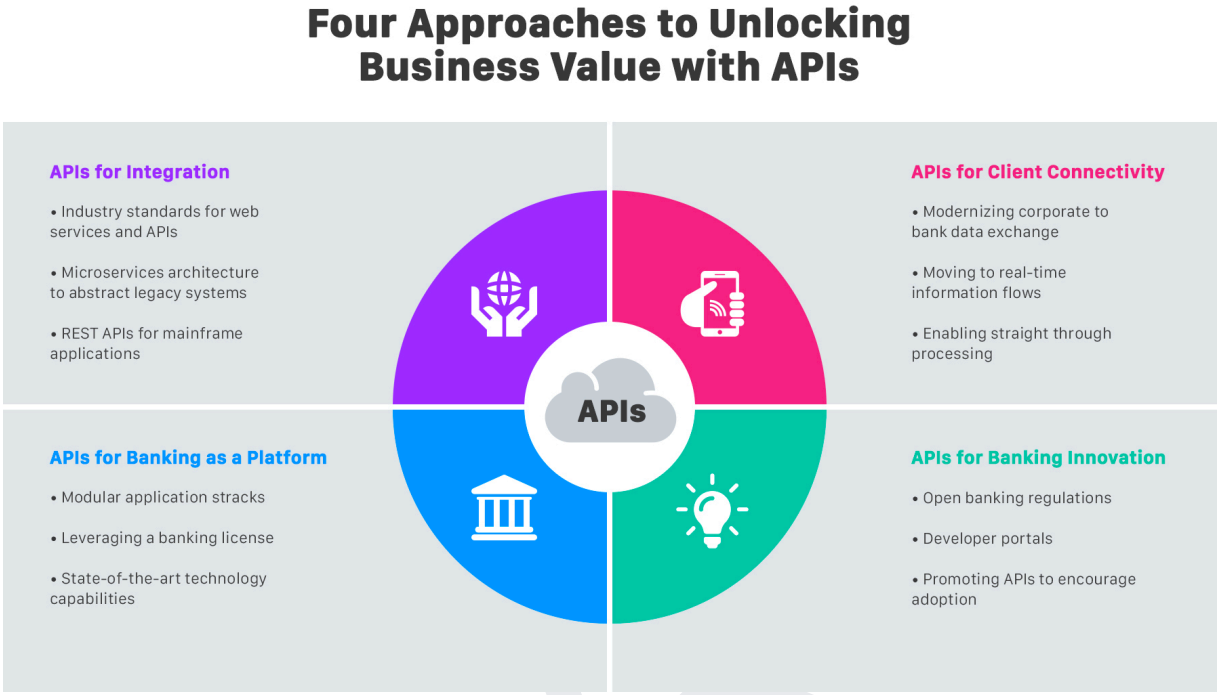
Many digitally savvy industry leaders have been exploring external API integrations well ahead of the regulation and their competitors (local or global), for a decade or so.

A number of leading banks and telcos attempted to set up their own API programs to provide access to customer data and banking functionality to external developers.

Banks recognised that external API ecosystems unlock partner integration, client connectivity, banking-as-a-service/-platform and ultimately increase innovation and established private API

DRAFT

programs, for example, Barclays API exchange, Deutsche Bank API program, BBVA API Market, Santander's Payments Hub[1].

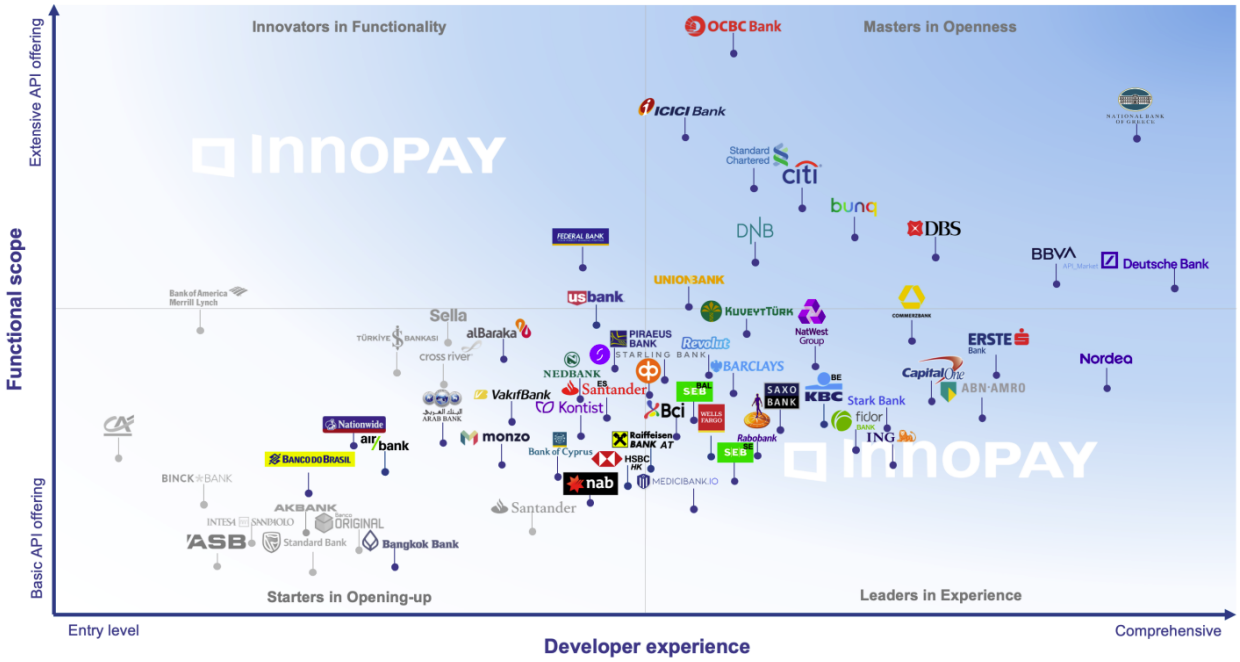


These programs are unregulated and typically centered around one company, controlled by one entity.

Going forward, these ecosystems and the size of them will continue to grow with API adoption rising. According to a 2020 McKinsey global survey on APIs in banking, nearly 20 percent of banking APIs are used externally to support integration with business partners, including suppliers. Banks also have plans to double the number of these APIs by 2025[2].

The number of banks offering APIs to their partners outside of regulated Open Banking ecosystems and the number of APIs is growing. Innopay notes in its yearly report a 17% increase of APIs in 2022 per bank in year since 2021[3]. The banks' API platforms are measured on their functional scope (basic to extensive) and developer experience (entry level to comprehensive).

1 https://dzone.com/articles/top-10-banking-apis-how-to-make-your-app-and-trans
2 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/whats-new-in-banking-api-programs
3 https://www.innopay.com/sites/default/files/media-files/Open%20Banking%20Monitor%202022.pdf



* Grey logo indicates limited portal accessibility, thereby complicating full assessment

Phase 2: Open Banking ecosystems

Private ecosystems, described above, started delivering significant benefits for the bank's customers and partners.

What if a fintech needs access to more than one bank? What if a customer has accounts in more than one bank?

Regulators and industry bodies in different countries across the world understood the value of using a common API access framework for an entire ecosystem. Open Banking brought the following benefits to consumers and fintechs:

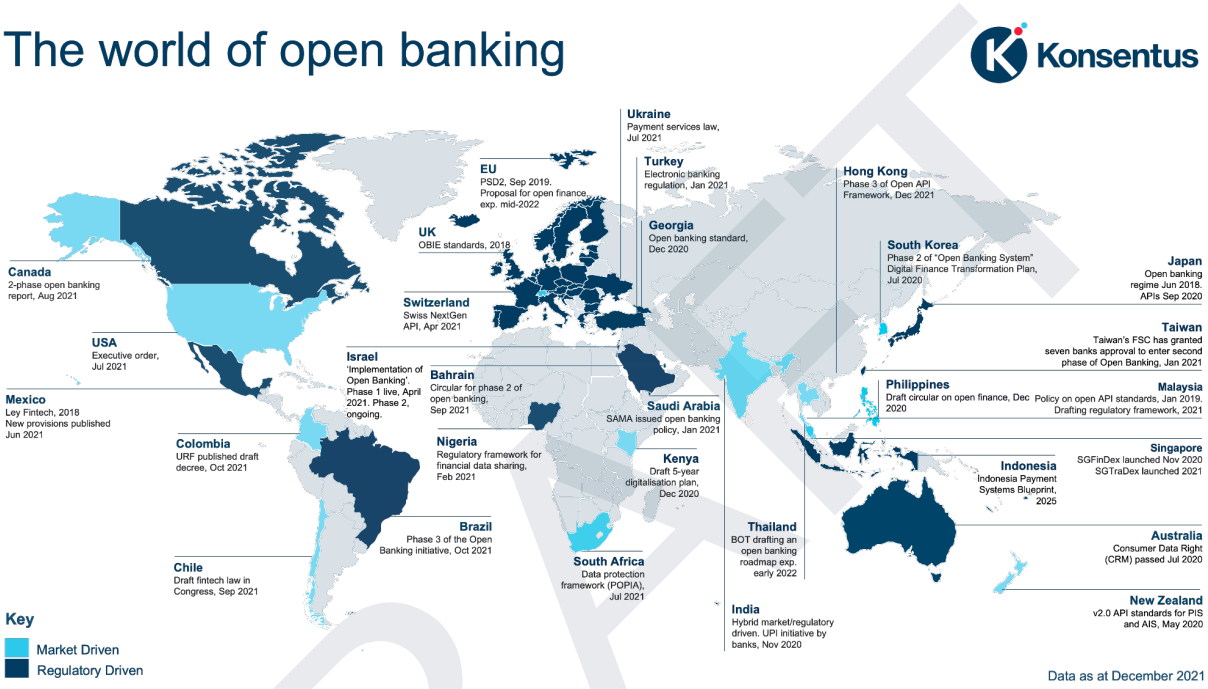
- Consistent way of accessing data across the whole industry.
- Secure data transfer.
- Mandated user control (explicit consent)
- New features previously not possible.
- More competitive market.

The elegance of a common framework, together with the user-consent based control it enabled, has led to rapid market adoption. Starting with the UK and PSD2 countries, followed by Australia and Brasil, there are active initiatives in the US, Canada, Saudi Arabia, UAE, Israel and more than 12 other jurisdictions. These open banking ecosystems can be market driven (US or NZ), partially regulated (UK for CMA9 banks only) and fully regulated (Australia and Brasil).

DRAFT

There are also hybrid scenarios, where the regulators, like in Japan or in Europe (raw PSD2 regulation), mandated APIs to be provided without a standardized API contract. While this model provides full coverage of the Data Providers, it still carries significant complexity for Data Consumers.

This chart from Konsentus shows that Open Baking is a global movement. In a few years time there won't be any gray areas left on this chart[4].



For more context on how Open Banking evolved globally, country status, and the key implementation considerations (like the FAPI security profile), refer to the OpenID Foundation's March 2022 Whitepaper on "Open Banking, Open Data, and the Financial-Grade API"[5].

4 https://www.konsentus.com/resources/the-world-of-open-banking/

5 https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

DRAFT

Phase 3: Cross-industry open data ecosystems

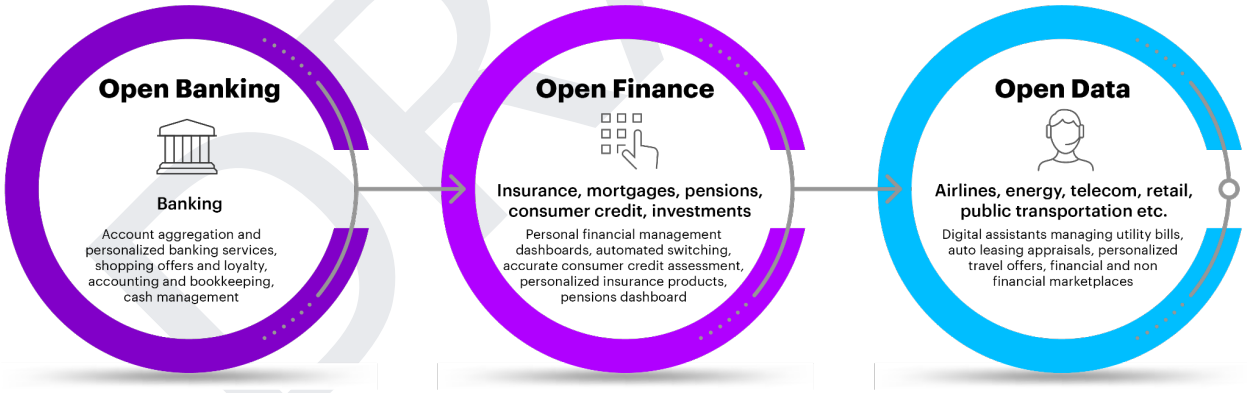
When Open Banking is implemented in a region, it's only natural for a consumer or a fintech developer to ask a question: why can't we use the same access mechanism to get my data / customer data from insurance companies, pension funds, telecommunication and energy providers?

This simple question is driving the move from Open banking to Open Finance and Open Data across many industries. While Open Finance has the ability to interlink multiple use cases in the finance industry, open data links it further with other industries serving customers.

The momentum towards Open Finance and Open Data is currently driven by domestic markets, and usually those that are government controlled:

- Brasil also has aggressive plans to scale its Open Banking (live from 2021) to Open Insurance in 2022, and they are exploring a move to Open Health as well.
- In 2022, Australia is going live with the Open Energy sector to complement its Open Banking ecosystem (Consumer Data right) live from 2021. Open Telecommunications is the next sector to go live in 2023.
- The UK is considering expanding Open Banking (live from 2018) to Open Finance to take care of a wider range of use cases.

According to Forester, Open Finance will be a continuous process, "marking a fundamental shift in how customers access financial services and how firms deliver them"[6].



[6] https://www.forrester.com/blogs/open-finance-will-reshape-the-relationship-between-banks-and-their-customers /

DRAFT

What have we learned?

Use cases

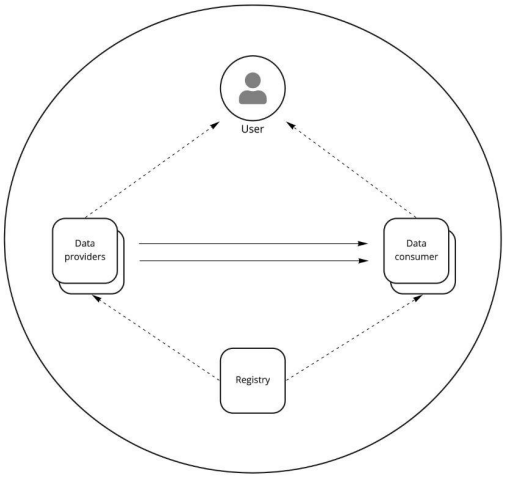
There are three top set of use cases that a typical open banking or open finance ecosystem delivers:

- Consumer identity data
- Consumer Account information data
- Payment initiation

These are quite common across the globe.

Open Data / API ecosystem building blocks

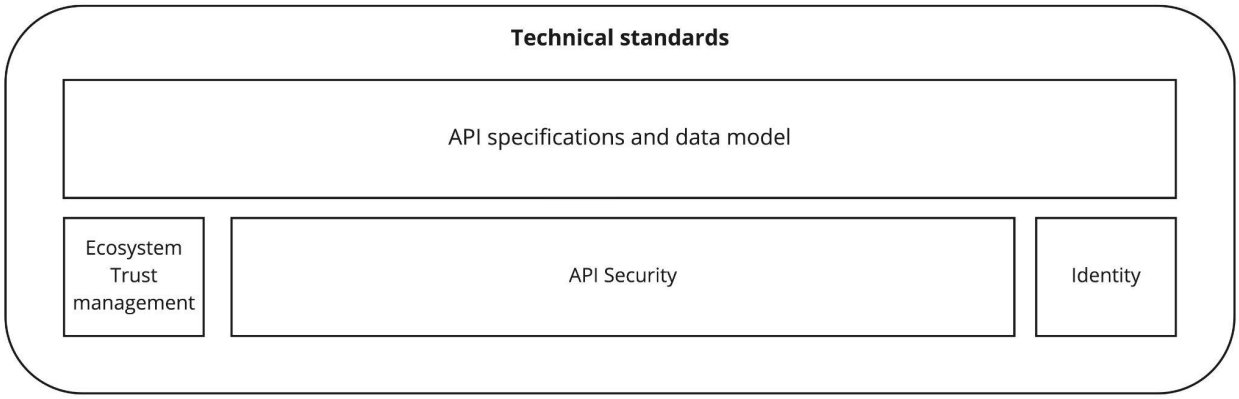
In order to set up any API ecosystem, you need to define business / legal rules and technical standards.



Technical standards

Rules and regulations
(**business** and **legal**)

Typical API ecosystem setup requires the same technical building blocks:



1. **Identity protocol** defines how you transfer identity information from a Data Provider to a Data Consumer with End-User consent..
2. **API security profile** defines how parties are authenticated, authorisation / data request and response are secured, message integrity is preserved.
3. **Trust management framework** is required to establish a minimum trust level between different participants. How do I know who to trust and who is allowed to do what?
4. **Functional API specifications** and API data model provide common understanding of data between Data Providers and Data Consumers.

DRAFT

Based on a survey of multiple ecosystems, we have learnt the following:

	Private API ecosystems	Open Banking ecosystems	Cross industry open data ecosystems
Identity	OpenID Connect	OpenID Connect	OpenID Connect
Security profile	Custom, usually OAuth based, can be FAPI	Dominated by FAPI	Dominated by FAPI
API specifications and data model	Custom with minimal ISO2022 usage	Regional with some ISO2022 usage	Regional
Trust management	Custom	Regional Central register	Regional Central register

Identity protocol

Most ecosystems across the globe have adopted OpenID Connect 1.0**.** This end-user authentication OAuth 2 extension has been a de facto industry standard with broad vendor support.

API security profile

One key decision the governing entity must determine is the standard for the API security profile.

While each ecosystem is still local/regional and specific to its jurisdiction, the majority of Open Banking / Open Finance / Open Data ecosystems have chosen OAuth-based FAPI as their API security profile. In addition, in some countries, FAPI CIBA is used for decoupled authentication, available and used. This global adoption allowed multiple vendors to provide support for FAPI and reduce the costs of adoption.

While most live ecosystems (e.g.: Brazil, UK) are running on FAPI 1.0, some others (e.g.: Norway, Australia) started considering FAPI 2 framework adoption. FAPI 2 simplifies security profile, especially for Data Consumers (clients), adds additional common building blocks (Grant Management, Pushed Authorisation Request and Rich Authorisation Request) to improve functionality and increase interoperability in the area of fine grained consent capture and management.

For more context on FAPI, refer to the Foundation's "Open Banking, Open Data and the Financial-Grade API" whitepaper[7].

[7] https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

DRAFT

Trust management framework

There is practically no standardization in this area. Every jurisdiction had to solve it on their own.

In private ecosystems, trust establishment between the participants is simple, custom and controlled by one entity.

In Open Banking and Open Finance, trust management is usually done through the central registry typically managed by the regulator.

Given that setting up an Open Banking framework across the globe is a repetitive task, a new breed of vendors has appeared on the market - ecosystem providers. For example, a company like Raidiam industrialized Open Banking ecosystem setup based on their previous experience in the UK, Brazil and Australia.

API specifications and API data model

In regards to API data models, there is also some standardization as some ecosystems like OBIE and the Berlin Group have opted for data models based on ISO 20022 (where available), although some implementations deployed custom data models.

The area of the greatest ecosystem divergence is functional API specifications that are typically custom, and controlled by the governing body of each ecosystem.

There is no standardization effort to date trying to develop a set of API specifications and data models common across multiple ecosystems with the exception of the Berlin Group (10 European countries) and FDX (US and Canada).

Every jurisdiction had to produce their own blueprints.

Standardization blockers

The OpenID Foundation paper mentioned above covers the reasons why standardization is important:

- Proven technology
- Secure
- Cost savings and vendor support
- Conformance testing and certifications[8].

While the use cases are common across all open banking ecosystems and jurisdictions, Berlin group is the only initiative working on standardization across multiple jurisdictions in Europe (Germany, France, Italy, Macedonia, Netherlands, Portugal, Austria, Slovakia, Serbia and etc).

Possible reasons lack of global standardization are:

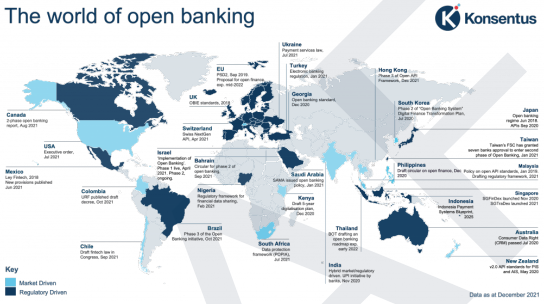
[8] https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf

DRAFT

- No governance authority has a say on what API specifications are used in a different jurisdiction.
- It is hard to standardize API specifications and data models because of local differences.
- Additional effort is required to coordinate with other authorities.
- Every authority prefers ‘made here’ design.
- The need to do so hasn’t been articulated.
- There are a number of global open banking middleware providers that simplify API specifications for relying parties that need it (e.g. True Layer or Tink).

What is next for Open Banking, Open Finance and Open Data?

The development of open data ecosystems to date has been advancing but has been limited to its local jurisdictions.



Could it be that the next stage of Open Banking, Open Finance and Open Data is global interoperability between different local ecosystems?

Imagine, if a UK-based fintech could connect to multiple banks across the globe to deliver a global version of Personalized Financial Management? Just because their customer has bank accounts in different jurisdictions.

Or a car rental company in Norway can verify customer identity in Australia and accept a payment directly from an Australian bank?

DRAFT

Global Use Cases

The rise of global relying parties

Tech platforms and fintechs

Apple

In March 2022, Apple acquired UK Open Banking startup Credit Kudos[9]. This open banking startup is focusing on a specific use case: credit decisioning.

In June 2022, Apple announced a new service to make Apple Pay payments in 4 installments over a few months for no interest (WWDC keynote), without the Apple Pay merchant making any changes. While the economics of this model is not clear yet, it is clear that Apple continues beyond Payments, Apple Card, ID in Wallet, the Kudos acquisition and installments to offer their customers a wide range of financial services.

While Apple has been rolling out their financial products slowly across the world, ultimately its ambitions are global.

Google

In 2021, Google acquired Japanese payment service startup Pring[10].This fintech company focuses on P2P payment in Japan and is licensed.

Paypal

Paypal is a fintech operating global payment that can be used in 200+ countries.

As a fintech player, Paypal currently has 200+ ways to access payment rails in each country apart from instances where existing credit card schemes could be used.

As a regulated payment services provider in some jurisdictions, Paypal is obliged to enable Open Banking to conform to regulation. To achieve this, Paypal's team has to support a variety of API and security standards in each country.

Global companies like Paypal, could benefit from having a consistent, global approach to Open Banking standards and market requirements.

[9] https://www.theblockcrypto.com/post/138898/apple-acquires-uk-open-banking-startup-credit-kudos
[10] https://www.pring.jp/news_info/227

DRAFT

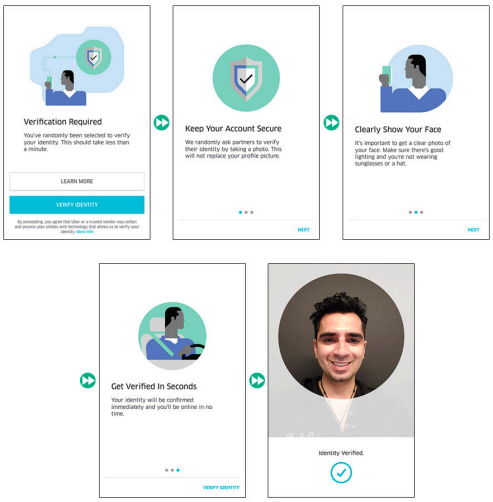
Block

Afterpay is a global fintech company operating “buy now, pay later (BNPL)” service in Australia, the United Kingdom, Canada, the United States, and New Zealand with 16m+ users[11].

Cash App is a highly successful service developed by Block that allows it to make peer-to-peer money transfers in multiple jurisdictions. Currently, this service is available in the United States and United Kingdom and it has grown from 3m to 44m+ plus users in ~5 years[12].

Sharing economy

PWC has predicted in 2015 that sharing economy revenue will grow from $15 to $335 billion dollars[13]. Sharing economy sector is dominated by global companies operating in different countries across the world: AirBNB, Uber, Taskrabbit and similar companies. For example, Uber is operating in 72 countries.
To improve ride safety, drivers need to perform identity verification. To improve payment experience, Uber needs to connect to different payment schemes available in the supported areas.



Currently, these companies have to access identity and financial services differently in each country (if such services are available at all) and they will significantly benefit if this access could be standardized.

Social networks

Global social media networks, like Facebook (~3b users) or Twitter (200m+ users), have been under pressure to verify their users identity to prevent anonymised harmful activity, providing

11 https://en.wikipedia.org/wiki/Afterpay
12 https://www.businessofapps.com/data/cash-app-statistics/
13 https://www.pwc.com/hu/en/kiadvanyok/assets/pdf/sharing-economy-en.pdf

traceability if an offense occurs, for example, scams and cyberbullying[14]. Proper identity verification could reduce occurrences of fake users, fake news and false influencers. Twitter, optionally, provides an ability for users to get their identity verified to let the audience know that their account is authentic.

Twitter reports that fewer than 5% of accounts are fakes or scammers, commonly referred to as "bots"[15]. Facebook has also launched a 'Page Publishing Authorization' for some Facebook pages, with Instagram (1b+ users) implementing a system to verify some suspicious pages. Some networks, like Tiktok (~700m+ users) and Facebook, perform some form of age verification to prevent users under the age of 13 from accessing their app. While initially they relied on users' self attestation, now they are increasingly employing AI algorithms to determine the age of its users.

Tiktok is also planning to test ways to age-restrict some types of content in its app[16]. This is not possible without identifying the users and/or their guardians.

Other types of global services, like dating and gaming are either regulated to choose to perform age verification. For example, in Japan dating services have to rely on mobile network operators' (MNO) verification services in the absence of other widely accepted options. MNOs themselves are required to perform KYC checks for all subscriptions.

Given the global nature of these networks, should they choose to use identity verification for some of the use cases above, this would require a fragmented country-by-country approach. Unless there was a global, consistent and interoperable approach.

DRAFT

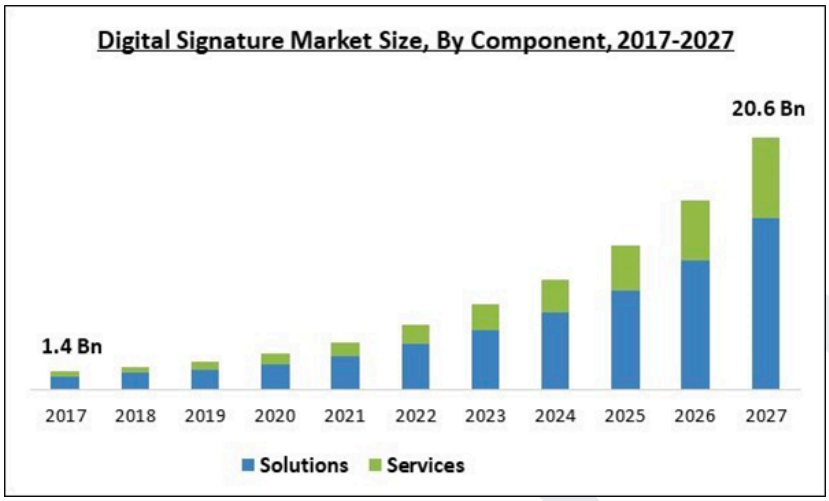
14 https://petition.parliament.uk/petitions/575833

15 https://theconversation.com/how-many-bots-are-on-twitter-the-question-is-difficult-to-answer-and-misses-the-point-183425

16 https://www.engadget.com/tik-tok-is-testing-ways-to-age-restrict-content-for-teens-100010082.html?src=rss

Global Digital Signing providers

COVID-19 pandemic drove the adoption of digital signing across the globe. According to Research and Markets, digital signing market is expected to continue to grow to US$ 20+ billion by 2027:



Global providers like Adobe and Docusign specialize in providing core document signing capabilities. In order for a user to sign a document, then need to be authenticated. This means that document signing solutions need to integrate with authentication providers.

eIDAS regulation standardized the process of electronic singing and its authentication requirements in Europe, but, unfortunately, it only works in Europe[17].

Global Assured Identity Network (GAIN) initiative is working on defining a consistent approach for Relying Parties to integrate with different Identity Information providers across the globe. Digital signing is one of the key use cases pursued by the GAIN community[18].

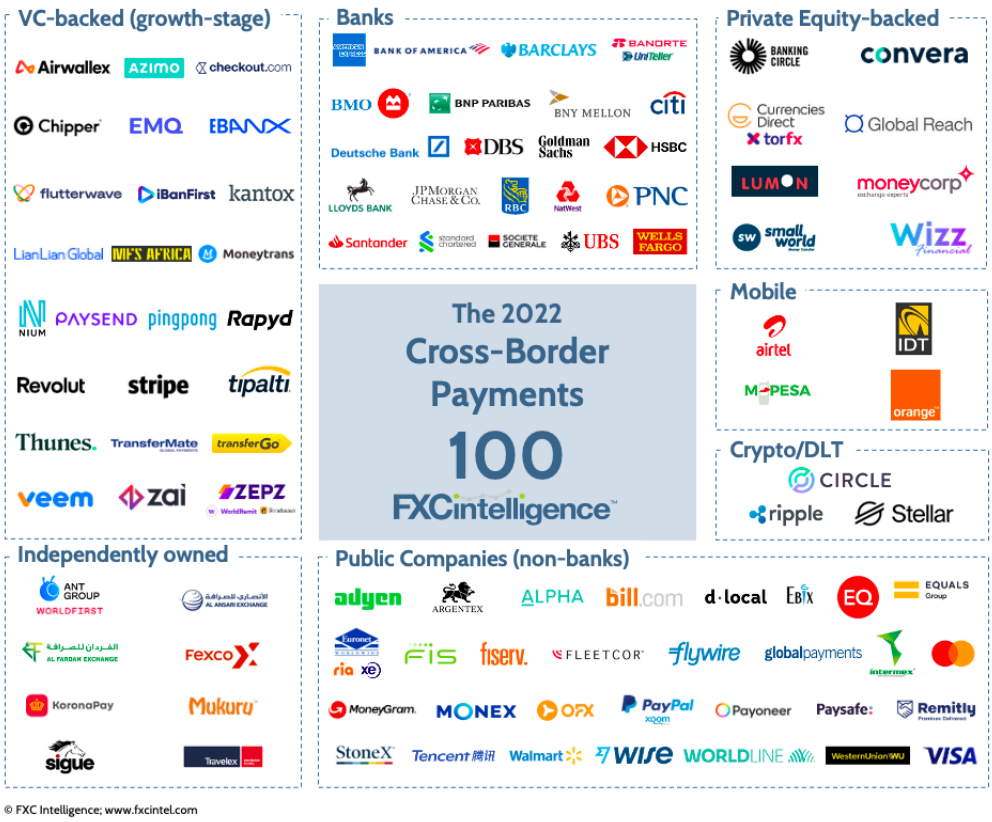
Cross border payments sector

FXC Intelligence has published The Top 100 Cross-Border Payment Companies report in 2020, 2021 and in 2022[19]. According to his report, the cross-border payments sector continues to grow, and investors continue to back it. This demonstrates the unfulfilled need in the market, especially in fragmented b2b payments space.

[17] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+-+Get+started

[18] https://gainforum.org/GAINWhitePaper.pdf

[19] https://www.fxcintel.com/research/reports/the-top-100-cross-border-payment-companies



© FXC Intelligence; www.fxcintel.com

Separately from market developments, the G20 (an intergovernmental forum comprising 19 countries and the EU) has made cross-border payments one of its key priorities[20]. The Financial stability Board (FSB) together with the Committee on Payments and Market infrastructures developed a roadmap to address cost, speed, transparency and access of cross border payments.

The roadmap consists of 19 building blocks.

[20] https://www.fsb.org/2021/10/g20-roadmap-for-enhancing-cross-border-payments-first-consolidated-progress-report/

Source: CPMI: Enhancing cross-border payments: building blocks of a global roadmap - Stage 2 report to the G20 (July 2020)

The following building blocks could be potentially relevant for global interoperability discussed in this whitepaper:

- Building block 5: Applying AML/CFT rules consistently and comprehensively
- Building block 8: Fostering KYC and identity sharing

  Consistently identifying customer customers and beneficiaries is required to make cross border payments, identity and data sharing work.
- Building block 6: Reviewing the interaction between data frameworks and cross-border payments

  Cross border data sharing might be impacted by national privacy and data protection legislation.
- Building block 14 - Adopting a Harmonized ISO 20022 version for message formats (including rules for conversion/mapping)
- Building block 15 - Harmonizing API protocols for data exchange.

  Non-standardised data formats create additional complexity, unnecessary transformation, delays and potentially manual processing. This also adds risk of misinterpretation and data loss, lowers data quality. Adoption of common message formats and standardized APIs *"can lead to additional efficiency gains by avoiding workarounds and translation from one implementation to another*

during integration of systems, thus facilitating interoperability and reducing the implementation costs for new providers and enhancing the ability to achieve fully automated straight through processing functionalities"[21].

The BIS Innovation Hub, SWIFT ran ISO 20022 hackathon in March 2021 to highlight the potential of cross-border payments standardisation. 60 teams from payments and technology market participants demonstrated high interest and high potential of using common message standards and standardized API specifications[22].

- Building block 16: Establishing unique identifiers with proxy registries

  FSB is conducting analysis of developments in the use of Digital IDs in the financial sector to uniquely identify organizations and individuals participating in financial transactions.

Cross border payments problem is far from being solved but there is a lot of activity, both government and market-driven attempting to fulfill this need.

Credit card schemes

Mastercard

Mastercard has been strategically building its open banking platform over the last few years. In February 2019, Mastercard announced its partnership with Token, open banking platform provider operating in 13 countries in Europe[23].

In June 2020, Mastercard has made a significant investment by purchasing Finicity for US$825m[24]. Ability to have access to solutions operating across multiple markets is considered strategically important for Mastercard.

Fincity has been operating primarily in North America, so Mastercard has also acquired European open banking platform Aiia in September 2021. "Open banking is democratizing financial services by putting consumers at the center of where and how their data is used to provide the services they want and need."[25].

In parallel, Mastercard has been investing in its cross-border digital identity solution and has discussions in multiple markets like Egypt, Montenegro, Australia.

Visa

In June 2021, Visa acquired European open banking platform Tink for EUR1.8b after its abandoned Plaid acquisition. "Tink is integrated with more than 3,400 banks and financial institutions, reaching millions of bank customers across Europe"[26].

In November 2021, Visa invested in Australian open banking platform Basiq.[27].

---

21 https://www.fsb.org/wp-content/uploads/P131021-1.pdf

22 https://www.bis.org/press/p210325.htm

23 https://token.io/press/mastercard-selects-token-io-as-a-partner-for-its-new-open-banking-hub-1

24 https://investor.mastercard.com/investor-news/investor-news-details/2020/Mastercard-to-Acquire-Finicity-to-Advance-Open-Banking-Strategy

25 https://investor.mastercard.com/investor-news/investor-news-details/2021/Mastercard-Expands-Open-Banking-Reach-with-Acquisition-of-Aiia/

26 https://www.businesswire.com/news/home/20210623006027/en/Visa-To-Acquire-European-Open-Banking-Platform-Tink

DRAFT

Summary

Both Visa and Mastercard have consistently demonstrated their keen interest in global open banking solutions by investing significant amounts of funds over the last few years.
With the lack of global interoperability standard that covers both technical, legal and regulatory aspects of integration, the only option these credit cards schemes had to date was to invest into intermediaries that simplify integrations per region. Most of the acquired solutions operate in one region where they originated (e.g.: EU and US / Canada). While credit card schemes themselves are not subject to Open Banking regulatory mandate, their ecosystem of merchants and fintechs could benefit from open banking data easily available in all jurisdictions.

Governments

In addition to G20 cross border payment activities mentioned above, the government recognised the need for global interoperability between digital identity schemes to facilitate economic recovery from COVID-19, for example to support the opening of domestic and international borders..

Financial crime, borne of illicit activities with unquantifiable human impact, costs the global economy up to 5% of GDP per year. A humongous amount is being spent on anti-money laundering and anti-terrorist financing but so far it has not been effective. For every $1,000 of 'illegal funds' in the financial system, $100 is spent on compliance, but only $1 is intercepted. That is only 0.1%. Global interoperability between digital identity schemes is deemed to be a solution towards rectifying the situation.

In 2021, the governments Australia, Canada, Finland, Israel, New Zealand, Singapore, the Netherlands, the United Kingdom, and the World Bank (as an observer) as a part of Digital Government Exchange established Digital Identity Working Group to develop pathways to mutual recognition and/or interoperability between existing digital identity schemes[28].

DRAFT

[27] https://www.pymnts.com/news/investment-tracker/2021/visa-invests-in-open-banking-platform-basiq/

[28] https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

Solution

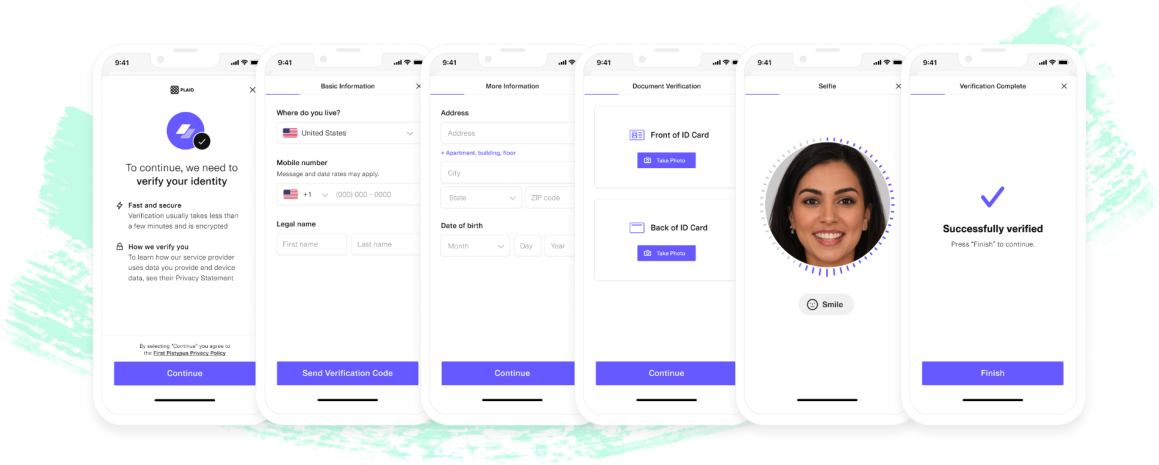
Option 1. Intermediary providers.

There are a number of technology providers in the market fulfilling the gaps described above.

Providers like TrueLayer and Moneyhub allow their global clients to abstract complexities of each individual jurisdiction with a simplified set of APIs for account information and payment initiation.

Plaid initially has been focusing on global account aggregation use cases, helping to connect apps with customer accounts in different financial institutions, which is a classic open banking use case.

Recently, with the purchase of Cognito, Plaid expanded their offering into identity and KYC space[29]. By doing identity verification in-house, adding income verification and payments, Plaid can now provide end-to-end flow for their customers.



Stripe, on the other hand, has started with payments. In 2021, it has expanded into identity with the product called Stripe Identity[30]. Recently, in May 2022, Stripe has announced further expansion into bank connectivity with Stripe Financial Connections[31]. Now their customers have fewer systems to connect to and manage, they can utilize the same platform for payments, subscriptions, payouts, ID and income verification.

These and other intermediary providers:

29 https://plaid.com/blog/introducing-identity-verification/

30 https://techcrunch.com/2021/06/14/stripe-goes-beyond-payments-with-stripe-identity-to-provide-ai-based-id-verification-for-transactions-and-more

31 https://stripe.com/newsroom/news/financial-connections

- Focus on providing consistent global API for:
    - identity verification
    - account information
    - and payments
- Use open banking APIs where available, with fallback to screen scraping and direct integrations.
- Provide simple and developer friendly APIs.

The trade-offs for the benefits above are:

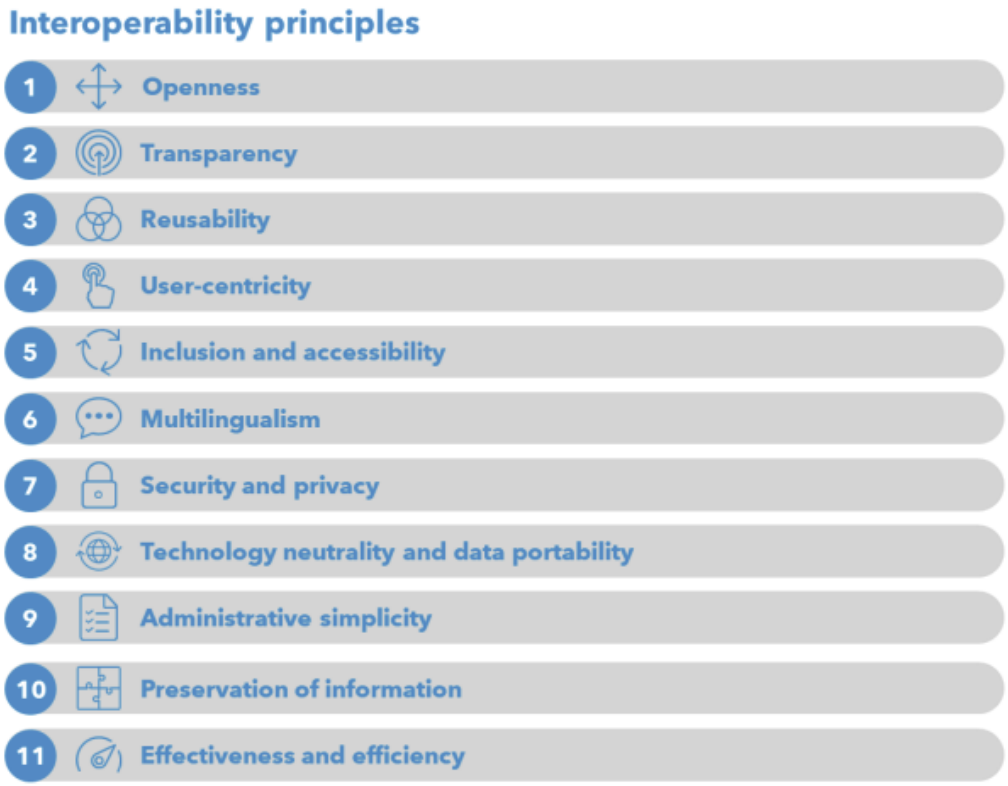
- Custom (non-standard) API and security profile specifications.
- Reliance on a vendor to support additional jurisdictions.
- Additional entity processing and storing end-user data.

DRAFT

Option 2. Direct integration between participants of different schemes.

General principles for interoperability

DGX working group has defined a generic set of principles that could be used as a starting point[32]:



Additional principles that could assist in the case of intra-scheme interoperability across a variety of use cases beyond identity:

1) Data transfer is peer to peer.
2) Not prescribing to participant schemes to change what standards they use internally. Define the standards used to interoperate between the schemes.
3) Minimize the effort for participants, minimally invasive structure
4) Encapsulate "local" in the local scheme (delegate translation to the schemes and not the RP). This could be a shared or entity service, an SDK or another solution.
5) Compliance with local regulation is the local's scheme responsibility.
6) Participant on-boarding, vetting and integration is to be done at a local scheme level (by scheme operator)
7) Autonomy of local networks is preserved.

[32] https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

Interoperability layers

Selection of the standards is the fundamental activity that will enable interoperability. It's best not to invent new standards where possible.

Identity

Use OpenID Connect to carry identity information between the participants. OpenID Connect is a common language already understood by many private and open API ecosystems[33].

API security profile

Use FAPI security profile to protect APIs. This OAuth 2 based profile is used by the growing majority of the schemes.

Use version 2 of FAPI framework (FAPI 2) because it delivers a simplified security profile and additional building blocks for interoperability.

Trust Management

In order to achieve global trust management, the following principles could be considered:

1) Trust establishment is done on a scheme to scheme level. Data transfer is peer to peer.
2) Not prescribing to participant schemes to change what standards they use internally. Define the standards used to interoperate between the schemes.
3) Minimize central infrastructure and governance, no central point of failure or control. No central decision making on what's allowed and what's not, no scheme can decide on behalf of the other scheme.
4) Participant on-boarding, vetting and integration is to be done at a local scheme level (by scheme operator). Ideal outcome for relying parties would be if they can "register once and use it everywhere".

Functional API specifications

A practical approach to achieve interoperability at the API level between different markets could include the following:

- Deliver simplified APIs using that can be used across the globe.
- Optimize APIs for global RP consumption

Delivery considerations

- Start simple, keep it simple, iterate on demand.
- Start with account information and progress to more complicated use cases, like payments later. For example, the MVP roadmap could consist of:
    - Account details
    - Transactions

[33] https://openid.net/specs/openid-connect-core-1_0.html

DRAFT

- Confirmation of Payee
- Payment initiation for simple immediate payments within the local ecosystem. Potentially could use v1 of OBIE Payment initiation API specification as a starting point. Payment initiation APIs should be payment scheme agnostic. Local schemes could decide what existing “payment rails” are used for payment execution..

Next Steps [In discussion]

Join existing working groups and communities:

- SWIFT, FDX, STET and the Berlin group established a working group on common API standards.
- OIX is working on scheme governance, business level interoperability and liability.
- OIDF GAIN is working on trust management and global identity scheme interoperability.
- FSB is working on common building blocks for cross-border payment initiation.
- DGX is working on digital identity scheme interoperability.

DRAFT

Annex A: Acknowledgement

Project Leader: Dima Postnikov

Contributors: Gail Hodges, Nat Sakimura, Daniel Goldscheider

Annex B: Bibliography

1. OpenID Foundation: Open Banking, Open Data, and the Financial Grade API (2022). <https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf>
2. OpenID Foundation: The Global “Open Health” Movement: Empowering people and saving lives by unlocking data (2022).
3. OpenID Foundation: OpenID for Verifiable Credentials (2022). <https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf>
4. GAIN: GAIN Digital Trust (2021) <https://gainforum.org/GAINWhitePaper.pdf>
5. Innopay: The current status of Open Banking and a glimpse into the future of Open Finance (2022), <https://www.innopay.com/sites/default/files/media-files/Open%20Banking%20Monitor%202022.pdf>
6. McKinsey Digital: What’s new in banking API programs (2022), <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/whats-new-in-banking-api-programs>
7. Australian Payment Network: TrustID Framework (2022), <https://www.auspaynet.com.au/insights/Trust-ID>
8. DGX Digital Identity Working Group: Digital Identity in response to COVID-19 ver.04 (2022), <https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf>
9. G20: G20 Roadmap for Enhancing Cross-border Payments (2021) <https://www.fsb.org/wp-content/uploads/P131021-1.pdf>
10. PWC: Sharing or paring? Growth of the sharing economy (2015) <https://www.pwc.com/hu/en/kiadvanyok/assets/pdf/sharing-economy-en.pdf>

DRAFT