Pushing the frontiers of payments: towards a global payments area

Industry expert input to CPMI Conference March 18-19, 2021

February 8, 2021

Ahead of the Committee for Payments and Market Infrastructure (CPMI) conference to be held on March 18-19, 2021, the Institute of International Finance (IIF) and OpenID Foundation are pleased to provide this response to some of the questions posed for industry expert input.[1]

The IIF and its members maintain a keen interest across the full scope of the FSB-CPMI initiative on the G20 Roadmap for Enhancing Cross-border Payments, and the associated 19 building blocks. However, in this instance we have developed a targeted submission that focuses specifically on certain aspects of payments interoperability with digital identity and trust. This response will foreground in particular the IIF's work with the OpenID Foundation[2] in the Open Digital Trust Initiative.

Digital Identity is one of the foundational technologies of the digital economy. Where the COVID-19 pandemic has accelerated the adoption of digital channels and the trend towards eCommerce, this has emerged as a crucial enabler for all firms, including small businesses, seeking to participate in the increasingly digitalized economy. Not surprisingly, the focus of our Open Digital Trust Initiative has gravitated to the interoperability of digital identity with payments.

Accordingly, as well as providing an overview of our Initiative and the draft **Principles for Digital Trust Networks** that we have developed, our comments address questions 7 and 9 of the call for industry expert responses, as well as question 10 relating to anti-money laundering and countering the financing of terrorist (AML/CFT).[3]

---

[1] CPMI, Pushing the frontiers of payments: towards a global payments area: call for industry expert responses (bis.org), December 23, 2020

[2] The OpenID Foundation is a non-profit international standardization organization of individuals and companies committed to enabling, promoting and protecting Open identity technologies. A public trust organization representing the open community of developers, vendors, and users, it provides needed infrastructure, managing intellectual property and brand marks and fostering viral growth and global participation in the proliferation of Open identity.

[3] In respect of questions 7 and 9, the submission is made jointly by the IIF and the OpenID Foundation. In respect of question 10, the submission is on behalf of IIF.

About the Open Digital Trust Initiative

The Open Digital Trust Initiative is an interoperable and open standards development, aiming to create a vibrant marketplace for digital trust services which would help individuals and entities to confirm identity and other attributes and to understand and manage risk.[4]

Open standards have played a major role in financial services and identity technology, and are key to validating the commercial viability of new technologies, facilitating multi-vendor interoperability, securing data portability and privacy of customers. Developing these standards in concert with updating regulatory requirements expedites the legal compliance needed for the implementation of innovative technologies, in a market-based approach that averts the need to navigate between competing frameworks.

Within the Initiative, the IIF is leading on policy development and the OpenID Foundation is leading on technical standards (see **figure 1**), together advancing a diverse global community's understanding of both the governance 'rules' and technology 'tools'.

1. The policy development activity is developing policy recommendations, requirements, and guidance for both public and private stakeholders in support of the project's wider objectives, across four working groups:
    - **Liability and legal framework**, looking at what liability settings and rules would be optimal to incentivize a range of actors to provide digital trust services;
    - **Individual (or user) centricity**, looking at how to ensure that digital trust networks share data about individuals on the basis of informed consent, while also remaining compliant with regulations around money laundering and maintaining appropriate audit trails;
    - **Interoperability**, including how to ensure that digital trust networks are open and federated; and
    - **Role of government and academic sectors**, looking across at the whole ecosystem and taking account of a range of information providers and consumers including sovereigns and others.

    These four working groups have engaged with a large number of ecosystem participants from the private, academic and government sectors, and have conducted ecosystem and interoperability stock takes.

    Principally through the Liability and legal framework and Individual centricity working groups, we have also developed a set of draft **Principles for Digital Trust Networks**, on which public feedback is invited.[5]

2. The technical protocols workstream, led by the OpenID Foundation, is focusing on updating standards by 2021. The specific standards under development, which are further described in the response to question 7 below, are:
    - Financial-grade APIs (FAPI) Standard;
    - e-KYC and Identity Assurance Standard.

    Both technical tracks are responsive to the COVID-19 pandemic, as many regions have seen a steep rise in the use of digital finance applications and services. In that context, the

[4] This Initiative was described in Episode 73 of the IIF's Finance, Regulation and Technology (FRT) podcast, and discussed in the wider context of digital identity interoperability and inclusion in Episode 78.
[5] https://www.iif.com/Publications/ID/4276/Draft-Principles-for-Digital-Trust-Networks

new eKYC and Identity Assurance Standard responds to the need for trusted online identity verification alternatives to in-person proofing requirements which have been problematic. The Financial-Grade APIs Standard helps secure the portability and privacy of personal data held by financial institutions and accessed in new online applications.

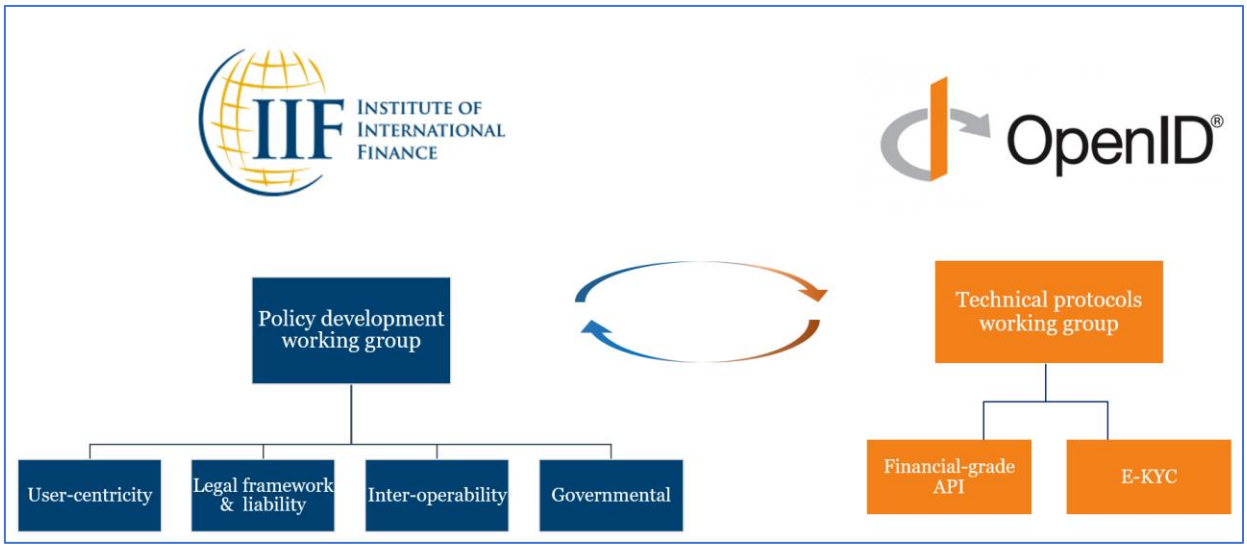
The open standards developed by the OpenID Foundation's technical protocols workstream are made freely available.[6] They are the product of a diverse team of experts seeking to ensure compatibility with technical and legal requirements internationally. Support in different regions for the FAPI standard helps align with emerging data portability requirements of major jurisdictions including the US, UK, EU and Australia.

The Foundation plans to continue an ongoing series of technical workshops with the Open Banking Implementation Entity in the UK as well as increasing the cadence and depth of similar technical workshops with the Financial Data Exchange (FDX) in North America and partners in Australia, South America and the Middle East.

The OpenID Foundation has recently signed an agreement with the IT Project Office of the Japanese Ministry of Economy, Trade and Industry (METI) to adopt the standard, its certification and conduct a pilot on legal entity identity, and it is coordinating this work with the Global Legal Entity Identifier (LEI) Foundation.

The Initiative welcomes inquiries from and engagement with all parties committed to an open, interoperable digital trust ecosystem.

Figure 1 – Open Digital Trust Initiative organization chart



Why Digital Trust matters

Particularly during the COVID-19 pandemic, the importance of Digital Trust has become apparent in enabling both individuals and enterprises to securely and easily prove an individual's or enterprise's identity or credentials to those with a need to know, while not over-sharing data.

[6] See https://openid.net/wg/ekyc-ida/ and https://openid.net/wg/fapi/.

Digital Trust has proven key to allowing for digital-only onboarding by financial institutions (including payment service providers) of new clients without face-to-face interactions. Another use case for Digital Trust has been in establishing secure payment pathways to facilitate the distribution of government subsidies to individuals and businesses.

Economies such as India and Singapore are starting to reap the rewards of the significant investments made in secure digital ID. Both the "India stack" (made up of the Unified Payment Interface (UPI) and the Aadhar biometric ID system) and the Singaporean MyInfo and SingPass systems are increasingly supporting their own ecosystems of third-party value-added service providers.

Going forward, those economies without a secure digital identity system (including many advanced economies) risk falling behind on measures such as the competitiveness of their economies, ease of doing business, and financial inclusion.

Digital Trust goes further than solely Digital ID and includes the ability for an individual or business to reliably, securely and quickly prove attributes such as age, residence, educational qualifications, entitlements to government programs or health status. In the corporate space, it also includes the ability for a legal entity to prove not just its own unique identity, but who its duly authorized representatives are at any given time.

While sovereign digital ID is a key enabler, the private sector also has an important role to play. For example, the BankID federated system in the Nordic countries provides a system whereby financial institutions can provide trust services by attesting to the identity and attributes of their own clients. In countries like the UK and Australia, the sovereign does not provide a secure digital ID system, but Open Banking or the Consumer Data Right allows individual clients to direct their financial institution to share data with selected third parties on the basis of informed consent.

In 2019, McKinsey Global Institute estimated that Digital ID could unlock economic value equivalent of 3–13% of GDP in 2030 across selected focus countries.[7] Digital Identity is also a key component of many aspects of digital transformation, enabling sophisticated analytics and partnerships across the ecosystem.

Question 7

Promoting the adoption of common standards and message formats, such as a harmonized version of ISO 20022, can play an important role in payment system interlinking and, more generally, addressing data quality and quantity restrictions in cross-border payments. Harmonized application programming interfaces (APIs) can enhance data exchange throughout the cross-border payment process. **What are the main challenges in agreeing on and implementing common message formats and API protocols for cross-border payments and how can we overcome them?**

IIF – OpenID Foundation comments:

The OpenID Foundation's **eKYC and Identity Assurance (eKYC & IDA) Working Group** is developing extensions to OpenID Connect that will standardize the communication of assured identity information, i.e. verified claims and information about how the verification was done and how the respective claims are maintained.

[7] McKinsey Global Institute (2019), Digital identification: A key to inclusive growth (mckinsey.com).

Legacy systems and established practices present challenges, but the Open ID Foundation is working to overcome them with open standards. This work seeks to overcome challenges that include:

- ambiguity and implicit assumptions regarding claims assurance;
- complex and costly custom solutions for communicating assured identity;
- inconsistent implementations;
- proprietary interfaces;
- in-person proofing, which is now a challenge due to COVID-19;
- emerging regulations such as GDPR, CCPA, and AMLD V;[8] and
- high costs of implementing and operating these services.

The vision is that eKYC & IDA will simplify and reduce costs of identity verification by:

- creating a standardized interface for communicating how verification of a user has been performed;
- clearly differentiating verified and unverified claims, thus removing ambiguity and allowing to represent both types of claims in the same assertion;
- simplifying integration of remote high assurance identification processes; and
- allowing purchase of vendor solutions that will interoperate with other standardized identity verification components.

The OpenID Foundation will provide a self-certification suite and testing framework for standardized eKYC software and implementation.

OpenID Connect for Identity Assurance 1.0 (2nd Implementer's Draft) was published in May 2020. This specification defines an extension of OpenID Connect for providing Relying Parties with verified Claims about End-Users. This extension is intended to be used to verify the identity of a natural person.

The **Financial-grade API (FAPI) Working Group** aims to develop technical protocols for the secure handling of financial-grade data used in use cases such as Open Banking.

Some Fintech services such as aggregation services use screen scraping and store user passwords. This model is both brittle and insecure. To cope with the brittleness, it should utilize an API model with structured data and to cope with insecurity, it should utilize a token model such as OAuth.

The FAPI Working Group is developing a REST/JSON model protected by OAuth. Specifically, the FAPI WG aims to provide JSON data schemas, security and privacy recommendations and protocols to:

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

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

So far, draft standards have been published as follows:

- FAPI 1.0 — Part 1: Baseline API Security Profile (Draft towards the final specification).
- FAPI 1.0 — Part 2: Advanced Security Profile (Draft towards the final specification).

[8] EU General Data Protection Regulation; California Consumer Privacy Act; 5th Anti-Money Laundering Directive.

- FAPI 1.0 — JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) (Implementer's Draft).
- FAPI 1.0 — CIBA Profile (Implementer's Draft).

Work is on track for finalization of these standards in 2021.

Question 9

Cross-border service levels on aspects such as data standards, message formats, fee arrangements, processing timelines, error and exception handling, and dispute resolution are often inferior to domestic ones. Often agreed service levels establishing a commonly binding framework for all participants are missing entirely in cross-border payments. **How can the use of agreed frameworks with a built-in enforcement mechanism based on both automated rules and institutional and contractual arrangements be agreed upon? What lessons can be learned from international card schemes and initiatives such as SWIFT gpi?**

IIF – OpenID Foundation comments:

The Open Digital Trust Initiative's draft **Principles for Digital Trust Networks** seek to provide one response to the challenge presented by this question. The draft Principles identify the high level 'rules of the road' that Digital Trust Networks should adopt in order to incentivize a high level of digital trust, user centricity and low cost, while ensuring that these networks are economically viable and the role of assurance provider is adequately rewarded and realistically protected from a liability perspective.

The broad vision is for Digital Trust Networks to comprise a set of participants, including both Users (who are also individual Data Subjects for individual data protection purposes in many cases, but also legal entities), Assurance Providers and Relying Parties. There is also scope for other types of intermediaries to be defined by a Network's rules.

Digital Trust Networks are anticipated to have associated Governance Arrangements, which should adhere to certain minimum principles, and may be separate legal entities. The Governance Arrangements will have responsibility for setting out Liability Rules, and other rules and requirements, to be complied with by Network Participants.

While the IIF and OpenID Foundation do not themselves propose to "police" the Principles, or award or allocate trust marks to particular Digital Trust Networks, they will encourage third-party verifiers, auditors and others to consider offering these services.

The Open Digital Trust Initiative may also road-test the draft Principles in the first half of 2021, through one or more Proof of Concept projects.

The draft Principles, submitted together with this input, are available here. Written feedback has been invited and can be provided by email to: mloldj@iif.com. Feedback should be submitted **by end-April 2021**. The aim is to release a version 1.0 of the Principles later in 2021. Submissions may be published, unless confidentiality is expressly requested.

Question 10

Data frameworks, ranging from data protection to data privacy and data localization requirements, interact and sometimes conflict with information needs in the cross-border payment context. In some cases, there is real or perceived tension between regulatory requirements, including banking regulation and AML/CFT rules, on the one hand, and restrictions on cross-border data flows and data storage, on the other. Sharing of information across borders is required for cross-border supervision and oversight as well as more effective risk management within those cross-border PSPs that are incorporated in multiple jurisdictions. **Where do conflicts between data frameworks and cross-border payments emerge and how can they be addressed?**

IIF comments:

Data frameworks, ranging from data protection to data privacy and data localization requirements, can indeed interact and sometimes conflict with information needs in the cross-border payment context. This is particularly acute with the flow of information concerning financial crime matters, where cross-border friction can negatively impact the inherently multi-jurisdictional nature of the international payments market. As the CPMI has reported to the G20, difficulties in this area can arise from underlying legal frameworks and there are challenges coordinating and securing support for alignment with international rules and standards and cooperative supervision and oversight arrangements.[9]

Addressing these issues through a coordinated international effort would benefit the global payments ecosystem and also improve the wider approach to tackling illicit financial flows. Put simply, limitations to information sharing hamper increased effectiveness. These constraints are at odds with the realities of criminal operations, which are not bound by international borders, and indeed actively exploit them to evade civil and criminal penalties. This undermines law enforcement's ability to build a network view of criminal activity and it weakens financial institutions' ability to fully review their exposure to financial crime risk at an international level.

This global problem is not only encountered where financial institutions seek to share intelligence with foreign law enforcement or other institutions, but can manifest itself within a banking group, where some jurisdictions impose limitations sharing data on a group-wide basis.[10] New technology for risk management and compliance in this area will also struggle to reach its full potential if the correct, good quality data is unavailable to facilitate machine learning and other activities which can help to achieve better outcomes.

When considering domestic and cross-border data exchange, it is also important to emphasize that data protection and data privacy remain critical. Such protections are not mutually exclusive to sharing information on illicit financial activity, a topic recognized by the FATF in changes to FATF Recommendation 2 (noted below), and this should be addressed more widely at the national and regional levels.

In tackling these issues, the IIF supports the G20 Enhancing Cross-border Payments Roadmap's efforts to deal with constraints on cross-border data-sharing. Critically, the adaptation of data-

[9] CPMI, Enhancing cross-border payments: building blocks of a global roadmap, July 2020

[10] For further analysis, the IIF previously published a survey of its members on the legal and regulatory barriers that exist to effective information sharing on financial crime related matters. The survey contained information concerning 92 countries across Europe, North America, Asia, Africa, Latin America and the Middle East. The report can be found here: https://www.iif.com/publication/regulatory-report/iif-financial-crime-information-sharing-report

sharing rules and supervisory and oversight standards to facilitate cross-border exchange of data should be addressed holistically on an international basis.

Consideration of the following issues would assist with the goals of the public sector on improving confidence between financial institutions and between jurisdictions, thus facilitating cross-border data flows and fostering improved digital identity frameworks and shared customer due diligence infrastructures – all of which would benefit an enhanced cross-border payments architecture:

1. Harmonized Implementation of International Standards Concerning AML/CFT Information Sharing:

   Effective implementation of the current FATF Recommendations and guidance which facilitate information sharing should be prioritized. Specifically, changes which were adopted in recent years to FATF Recommendation 2 (cooperation between data protection authorities and AML/CFT authorities and the compatibility of AML/CFT and data protection rules) and the interpretative note to FATF Recommendation 18 (financial institution group-wide information sharing) should be implemented consistently and swiftly across FATF countries with an eye toward ensuring practical and tangible outcomes which improve the environment for exchanging intelligence.[11]

   We encourage member jurisdictions of the Basel Committee on Banking Supervision (BCBS) and beyond to consistently implement guidance on sound management of risks related to money laundering and financing of terrorism which enables greater interaction, cooperation, and information exchange between AML/CFT and prudential supervisory authorities.[12] This globally consistent guidance will assist in filling gaps in this area, including in relation to mechanisms which facilitate such cooperation in the jurisdictional and international context.

2. Further Updates to International Standards Concerning AML/CFT Information Sharing

   We have encouraged FATF to continue to work to improve the effectiveness of its member states' information sharing regimes. Specifically, as the FATF Recommendations offer a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, the IIF believes that the Recommendations would benefit from incorporation of the following amendments – where such detail is absent – in order to enable more effective information sharing. It is important this be done whilst also balancing that exchange with the highest standards for data protection, data security and customer privacy:

   - Countries should ensure that secrecy and privacy laws, and tipping-off or similar provisions, do not inhibit the exchange of relevant information, including Suspicious Activity Reports (SARs) and associated underlying information, across borders

[11] For further information on these issues, please see: IIF Staff Paper, Economic and Financial Crime Risk and the Sharing of Intelligence: Updating and Enabling International and Domestic Cooperation in Combatting Illicit Financial Flows, October 2020: https://www.iif.com/Publications/ID/4125/IIF-Staff-Paper-on-Financial-Crime-Intelligence-Sharing.

[12] BCBS, Sound management of risks related to money laundering and financing of terrorism: revisions to supervisory cooperation, July 2020 and IIF, Re: Introduction of guidelines on interaction and cooperation between prudential and AML/CFT supervision, February 2020: see https://www.iif.com/Publications/ID/3752/IIF-Letter-on-BCBS-AMLCFT-and-Prudential-Supervision-Consultation.

between entities in the same group enterprise; between entities in different group enterprises; and between enterprises and governments, in both directions, for the purpose of managing financial crime risk. Countries should ensure that adequate legal protections for banks sharing information in good faith are in place to facilitate the sharing of such information.

- Countries should ensure that, where an entity is required to report a suspicion which is based, in whole or part, upon information gathered from outside its own group enterprise or from other jurisdictions, that the applicable laws do not prevent the inclusion of that information in the report which is to be filed.
- Countries should ensure that, where an entity is required to report a suspicion which relates to activity across a number of group enterprises or jurisdictions, that the applicable laws facilitate the filing of identical reports in each relevant jurisdiction.

3. National and Multilateral Public/Private Sector Information Sharing Development

In addition to critical enhancements to – or implementation of – international standards in this area, it is also important to facilitate information sharing between the public and private sectors through country and regionally led initiatives. Countries and regional bodies should continue to actively support the creation of public/private partnerships (PPP) as a means to advance information sharing goals. At the center of an intelligence-led financial crime mitigation model is the PPP – a collaboration between financial institutions, law enforcement and the regulatory community. PPPs are an important first step in the ability to deliver operational benefits and efficiency gains, and they can provide a framework to build the relationships and dialogue between stakeholders to help coordinate and catalyze coherent reform of the wider financial crime risk management framework.

Many of the same challenges on information sharing gateways can exist for PPPs, however they are an effective tool for addressing risk in this area and should be considered as essential in the wider context of fulfilling domestic and international anti-financial crime objectives. Where there is statutory underpinning for PPP data sharing, this can also expedite overcoming some of the impediments outlined herein. [13]

[13] For further information on public-private partnerships, please see: IIF/Deloitte, The Global Framework for Fighting Financial Crime: Enhancing Effectiveness and Improving Outcomes, October 2019: https://www.iif.com/Publications/ID/3606/The-Global-Framework-for-Fighting-Financial-Crime-Enhancing-Effectiveness-Improving-Out-comes .

Conclusion

The IIF welcomes this opportunity to inform the CPMI and conference attendees of current developments which may be of direct interest to the implementation of the G20 Roadmap for Enhancing Cross-border Payments.

In that regard, the IIF and Emerging Payments Association have established a **Joint Consultative Forum on Enhancing Cross-Border Payments**, which is in the process of being stood up as we identify co-chairs and interested members.

We would expect that the Forum can over time come to play a valuable role as a trusted interlocutor for CPMI, the standard-setting bodies, international standardization organizations and national authorities with regard to the implementation and evolution of the Roadmap.

We will welcome opportunities to discuss these issues further. For any questions or clarifications on our comments, please contact Brad Carr (bcarr@iif.com) or Laurence White (lwhite@iif.com) at the IIF, or Don Thibeau (don@oidf.org) at the OpenID Foundation.