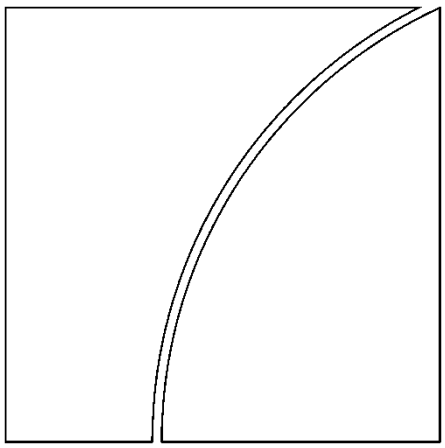
# Consultative Group on Innovation and the Digital Economy



# Enabling open finance through APIs

December 2020

## BIS Representative Office for the Americas

Comments are welcome and should be addressed to: CGIDEreport@bis.org, preferably by 31 January 2021

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).



ISBN 978-92-9259-445-9 (online)

# Table of contents

# Foreword

This report, "Enabling open finance through APIs", is the outcome of work conducted by BIS member central banks in the Americas within the newly established Consultative Group for Innovation and the Digital Economy (CGIDE).

The CGIDE was launched in February 2020 to meet the demand by BIS member central banks in the Americas for greater cooperation in the area of technological innovation and the digital economy. The BIS is well placed to support this objective, as technological innovation is a key area of focus in its medium-term strategy, Innovation BIS 2025. Technological changes are disrupting payment systems, financial intermediation and financial markets, all core areas of focus for the central bank community. This initiative is timely as several countries in the region are in the process of revamping their retail payment systems and regulating their fintech sectors, with a view to enhancing competition and financial inclusion.

The CGIDE provides a forum where senior officials of BIS-shareholder central banks in the Americas can cooperate to work towards the following general objectives:

1. Analysing and developing public technological infrastructures geared towards tackling common shortcomings in all participating jurisdictions.
2. Promoting an environment suitable to open banking, potentially through the development of key application program interfaces (APIs).
3. Analysing the implications of these public technological infrastructures in terms of market structure and regulatory implications.

The first project that the CGIDE decided to pursue, in February 2020, was that of exploring the technical issues surrounding the development of an identification and authentication API that could be used to implement privately and publicly administered open finance solutions with seamless scalability. The report marks the successful completion of this task. In particular, it analyses an API architecture based on an authentication app for mobile phones developed and maintained by a central validator. The scheme allows users to securely input their financial credentials into the transaction flow, creating secure relationships between financial institutions and third parties. While no central bank is endorsing the adoption of open banking or the analysed identification and authentication API scheme, the document can nevertheless serve as a useful general reference for central banks that want to develop their own payment initiatives.

The report is now published to inform the public of the cooperative efforts by the largest central banks in the Americas and to give industry experts the chance to provide their feedback. Comments are welcome and should be addressed to CGIDEreport@bis.org, preferably by 31 January 2021.

Miguel Díaz

Chair of the CGIDE, Bank of Mexico

Alexandre Tombini

BIS Chief Representative for the Americas

# Executive summary

In response to the need to facilitate payment services and expand the public's access to them, this report explores the development of an identification and authentication application program interface (API) that could be used to implement privately and publicly administered open finance solutions with seamless scalability. An open finance ecosystem can benefit financial system participants and society in general by creating an environment in which the competitive advantage of different players can be used to provide people with better financial services.

The Technical Task Force of the Consultative Group on Innovation and the Digital Economy (CGIDE TTF) analysed the relevance of an efficient and reliable identification and authentication method, and delved into a centralised API implementation for this objective. The report highlights the importance of open finance for the development of the financial system, lists the trade-offs regarding implementation schemes for open finance and serves as background for the other, more technical, documents: (i) a technical flow diagram of identity validation based on a centralised API architecture ("Centralised validator API proposal") (unpublished); (ii) general hardware requirements to implement the centralised solution ("Minimal technological requirements for central validator") (Annex A); and (iii) technical requirements for third parties on the central validator API architecture ("Technical requirements for third parties") (Annex B).

Remote and secure identification and authentication of users is the main requirement for parties in an open finance ecosystem to interact, since this ensures different entities that a given request has indeed made by their users. Moreover, an open and standardised API scheme can provide the interoperability needed for all interested parties to participate in the open finance ecosystem. In particular, the CGIDE TTF has been analysing an API scheme based on mobile devices to support the remote, secure and efficient identification and authentication of users of financial institutions. The analysed scheme is based on the establishment of a central validator (CV) that allows secure relationships to be created between financial institutions and third parties, without the need for them to come into direct contact with each other. This is accomplished by establishing secure connections between the CV and third parties on the one hand, and between the financial institutions and the CV on the other. The security schemes used by the CV would ensure that all connections in the scheme are established between previously certified entities for the orderly provision of financial services through third parties. Furthermore, the CV provides the necessary elements to guarantee that each party involved in the provision of services through this scheme accesses only the user information strictly necessary to allow the provision of a specified financial service.

The work of the CGIDE TTF did not include a review of all possible alternatives to achieve secure and remote identification and authentication through APIs. From that perspective, this document should only serve as a general reference for individual countries that want to develop their own payments initiatives, and consequently no member is endorsing the adoption of open banking or the analysed identification and authentication API and CV scheme.

## Background

An open finance ecosystem can benefit financial system participants and society in general, by creating an environment in which the competitive advantage of different players can be used to provide people with better financial services. The Technical Task Force of the Consultative Group on Innovation and the Digital Economy (CGIDE TTF)[1] was entrusted with exploring the development of an identification and authentication application programming interface (API) that could be used to implement privately and publicly administered open finance solutions with seamless scalability. The CGIDE TTF will report to the CGIDE on: (i) a technical proposal for a centralised API model for identity validation; and (ii) the cyber security issues involved in designing and operating such infrastructure.

To fulfil its objective, the CGIDE TTF has produced four documents: (i) this high-level note, which serves as background for the other more technical deliverables; (ii) a technical flow diagram of identity validation based on a centralised API architecture ("Centralised validator API proposal"); (iii) general hardware requirements to implement the centralised solution ("Minimal technological requirements for central validator"); and (iv) technical requirements for third parties on the central validator API architecture ("Technical requirements for third parties").

These documents present one option for the architecture that has many benefits, and are meant to provide readers with basic information to simplify their journey. This note explores the relevance of an efficient and reliable identification and authentication method, and delves into a centralised API implementation for this objective.

The work of the CGIDE TTF did not include a review of all possible alternatives to achieve secure and remote identification and authentication through APIs, but mostly focused on the analysis and design of a viable API architecture for those purposes. From that perspective, this document should only serve as a general reference for individual countries that want to develop their own payments initiatives, and consequently no member is endorsing the adoption of open banking or the analysed identification and authentication API scheme. In this regard, institutions across different jurisdictions are working on the design and implementation of various identification and authentication API schemes to support open finance ecosystems. Examples include the European Central Bank, the European Banking Authority and the National Payments Corporation of India.

## Importance of open finance for the development of the financial system

Open finance allows financial services to be provided through third parties with potential competitive advantages regarding: (i) the reach of their current network of users;[2] (ii) the trust that the public already places on them for the management of their information; and (iii) the convenience and familiarity of their user base, thanks to a simplified and intuitive user experience.

Open finance services can be classified into two main categories, based on their requirements for strong authentication procedures:

[1] The CGIDE comprises senior officials from the BIS shareholder central banks in the Americas, namely the central banks of Argentina, Brazil, Canada, Chile, Colombia, Mexico, Peru and the United States.

[2] According to the Basel Committee on Banking Supervision's *Report on open banking and application programming interfaces*, a third party is "any external legal entity that is not a part of the supervised banking organisation [providing the financial service]. Third parties can be supervised entities (eg banks, other regulated financial firms) or non-supervised entities (eg financial technology firms, data aggregators, commercial partners, vendors, other non-financial payment firms)". The report is available at www.bis.org/bcbs/publ/d486.htm.

- *Those that do not necessarily require strong authentication*. This category comprises services such as providing easy access to publicly available data (eg financial institutions' list of products or available infrastructure) through the interface of a third party.
- *Those that require remote and secure strong authentication*. This category, which is arguably the most relevant, includes services that require the use of third-party infrastructure to access or retrieve personal and transactional information, and the remote initiation of transactions (eg the triggering of a payment instruction or the contracting of financial services such as insurance or investments). Providing services in this category necessitates a remote and secure alternative to identify and authenticate users, since it requires access to, and potential exchange of, private data.

An open finance ecosystem could benefit all financial system participants in several ways. Incumbent financial institutions could reach a new sector of users by indirectly using data sources that were not traditionally available to assess the feasibility of providing services to clients (eg through their interaction with third parties' data on users' activity on e-commerce or other platforms to assess the possibility of granting them credit). Similarly, financial institutions could design and offer tailored services to their users through third parties and make better use of currently available technology to offer them an improved customer experience.

Similarly, by working in partnership with financial institutions, non-financial third parties could expand their range of services and serve a larger number of users. Moreover, by providing financial services, these firms could attract more users to their core business platforms, making them even more beneficial to new users.

Most importantly, users could benefit from tailored financial services and a better customer experience (which could let them access various services through the same channel). Furthermore, the inclusion of financial services on the platforms of recurrent service providers would allow more users to enjoy their benefits and expand financial inclusion.

## Open finance implementation schemes

The design of an open finance ecosystem is heavily influenced by the architecture of the identification and authentication APIs that underlie it. One of the defining characteristics of this architecture is how it handles connections between participants of the open finance ecosystem. The main alternatives are: (i) centralised connections; and (ii) multilateral (bilateral or independent networks) connections.[3] These alternatives have pros and cons that mirror each other to some extent.

- *Centralised connections*. In this type of architecture there is a central player with whom all the participants need to be connected. This implies that there is a unique network of connections within the open finance ecosystem, which is governed by the standards set by the central entity.
    - Pros:
        - Entry requirements for the network are the same for all parties interested in participating in the open finance ecosystem, making it easier for authorities to regulate and supervise the ecosystem.
        - The governance of a centralised solution makes it harder for entities with significant market power to impose conditions within the ecosystem (eg a third

[3] A third option is multiple networks, each with centralised connections, where there is interoperability between the central players of different networks. This option shares pros and cons with the two alternatives detailed in this note, but its analysis requires further work, which the CGIDE may decide to carry out in the future.

party with a large network has less bargaining power to impose conditions in this type of structure than in a bilateral relationship).
        - The network is less complex than with multilateral connections since fewer connections are needed to achieve full interconnection. This means that the model achieves full interoperability in the open finance ecosystem almost by default. Moreover, participants only need to generate secure connections with one entity to reach the whole network.
    - Cons:
        - From a business continuity perspective, centralised implementations might be prone to more suspensions in their service, since the failure of the central entity can affect the whole ecosystem.
        - Since all connections are standardised to the requirements set by the central entity, innovation might be hindered to some extent.
        - Similarly, some business models might find it harder to flourish in a standardised network, where no special conditions are given to specific sectors.
        - Reaching an industry-wide agreement on who the central entity should be might be a complex process if consensus is required.

- *Multilateral (bilateral or closed networks) connections*. In this type of architecture, there are different networks of connections between open finance ecosystem participants, which can have different entry requirements. This means that network participants can decide who enters their network, as well as whether the network will target a specific sector. Interoperability between different networks might be possible, but is not guaranteed and depends on the agreement and incentive alignment of the owners of the different independent networks.
    - Pros:
        - Open finance ecosystems relying on this kind of architecture might be more resilient to service suspensions since there is no unique point of failure. If interoperability is reached, users could, in principle, switch between networks if a particular network is not available at a certain time.
        - Since networks might focus their services on different sectors, potential ecosystem participants might find it more appealing to connect to just one subset of networks.
        - Networks having different entry and operation requirements might foster innovation in the provision of financial services through third parties.
    - Cons:
        - Since the governance of each network might be different, market power might play a role. Specifically, some interested parties might be denied access to a particular network, potentially being left out of a market sector.
        - The existence of multiple networks might diminish regulators' ability to:
            - properly align the incentives within every network
            - regulate and supervise every network
        - An open finance ecosystem relying on this type of API implementation might be fragmented, since interoperability is not guaranteed by design.
        - Overall, the complexity of the network within the open finance ecosystem might be higher, since more connections would be needed to achieve full interconnection. In turn, this could mean that a participant interested in various market sectors could have higher connection costs than with a centralised API architecture.

Other intermediate architectures, such as several central validating entities that are interconnected, are also viable, and have a mix of the pros and cons of the solutions described above.

The decision on which type of API architecture should be implemented depends on the characteristics of each jurisdiction. Moreover, the sector leading this implementation might be either an authority or the industry. In this regard, some examples of open finance models supported by different API architectures include:

- *Europe's revised Payment Services Directive (PSD2)*. This regulation was introduced by the European Union to acknowledge new players remotely accessing customers' payment accounts to make payments on their behalf and to give them an overview of their various payment accounts. Institutions holding the payment accounts of customers can provide access to these new players via APIs.[4]
- *The United Kingdom's open banking*. In 2016, The UK Competitions and Market Authority (CMA) set up the Open Banking Implementation Entity (OBIE) to introduce its own open banking initiative, which builds on its PSD2 obligations. This initiative mandates that the nine leading banks in the UK implement a predefined and standard API to securely provide open banking. In contrast with PSD2, UK's OBIE has released a set of API technical specifications for its initiative and does not leave the details up to the market. [5]
- India:
    - Unified Payments Interface (UPI): This initiative allows account holders in India to send and receive money instantly through third parties using mobile devices, without giving their bank account details or the user login and password they have registered with their financial institution.[6]
    - Account aggregators (AAs) framework: An AA is a non-bank financial institution regulated by the Reserve Bank of India (RBI) that manages consent for financial data-sharing. An AA provides interfaces to its users so that they can consent to the sharing of private financial data. The data travel from the financial institution hosting the data (eg a bank where the AA user has an account) to the institution requesting them (eg a lender from which the user wishes to obtain credit) via open and standardised API endpoints prescribed by the RBI. Since different institutions can become AAs, competition in the sector of financial data-sharing in India can be expected to develop under the AA framework.[7]
- *Singapore's Financial Planning Digital Services (FPDS)*. This initiative aims at facilitating data portability with a secure API framework underneath giving consumers greater access to, and control over, their financial data. The proposed consent mechanism for the sharing of data will be facilitated using SingPass, the single sign-on service already used by all residents to access government e-services. Consumers could then grant access to financial institutions of their

[4] A summary of the key points of the PSD2 is at eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366.

[5] More information on the UK's open banking initiative can be found on the OBIE website: www.openbanking.org.uk/.

[6] Further details on the UPI can be found on the NPCI website: www.npci.org.in/product-overview/upi-product-overview.

[7] Further information on the AA framework can be found on Sahamati's (a self-organised collective of the AA ecosystem) webpage: sahamati.org.in/about/. Regulatory details on the AA licensing framework can be consulted at www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142.

choosing to share information about their bank accounts, credit cards, pension contributions, social security savings and government housing scheme payments.[8]

- *Brazil's open banking initiative*. The Brazilian central bank is working on the development of an open banking ecosystem, for which regulation has been issued to allow the provision of financial services through third parties by the end of 2021. The specific identification and authentication API architecture is yet to be established, as decided by the industry with the authorisation of the central bank. The main goals of this API scheme are to foster competition, efficiency and data security, and to strike the right balance between incumbents and new players.[9]

## The role of identification and authentication

In a traditional relationship between two entities to jointly provide a service, the two interacting parties typically know each other beforehand. This means that they have already agreed to specific terms of service as well as security and communication standards, which allow them to establish connections to exchange information in order to provide a given service. However, if the parties do not have a relationship with each other, different challenges need to be tackled in order for them to be able to interact securely and remotely.

In particular, a lack of trust between parties, potential incompatible technological infrastructures and misaligned incentives for the relationship to develop should be addressed. In this regard, remote and secure identification and authentication of users is the main requirement for this interaction, since this ensures different entities that a given request was indeed made by their users. Moreover, an open and standardised API scheme can provide the interoperability needed for all interested parties to participate in the open finance ecosystem.

In this context, an open and standardised scheme of APIs, together with a clear set of rules, can align the incentives of the interacting parties so that each entity benefits from their remote relationship, as the second section of this note details. Furthermore, these rules, potentially in conjunction with appropriate regulation, can ensure the security and integrity of the connections between the participants of the open finance ecosystem. In this regard, for the proper functioning of the ecosystem, an institution or group of institutions should be designated as administrator(s) with responsibility for validating that all participants properly fulfil all of the ecosystem's connection requirements and operation rules. The entity that plays this role will depend on the ecosystem's design and the characteristics of the jurisdiction where it is deployed. Nevertheless, there are certain minimum requirements that third parties must have in order to allow for this trust network to sustain itself (see "Technical requirements for third parties").

## Proposal analysed by the CGIDE TTF

A framework to facilitate the secure and interoperable provision of financial services through third parties should:

i) Ensure interoperability, so that it is possible to enjoy economies of scale and exploit network externalities.

ii) Promote the necessary conditions for fair competition between financial service providers in cooperation with third parties, ensuring a level playing field for all market entrants.

iii) Ensure that user information is transmitted, processed and managed securely.

[8] Further information on the FDPS initiative and a comparison with PSD2 available at www.moneythor.com/2020/04/29/open-banking-in-singapore-comparing-psd2-fpds/.

[9] For a summary of the open banking regulation issued by the Central Bank of Brazil, see www.bcb.gov.br/en/pressdetail/2330/nota.

iv) Be as scalable and general as possible, so that it caters for both currently foreseeable services as well as future innovation.

v) Foster the integration of third parties into the open finance ecosystem (subject to the required level of security). This might imply setting a standard API, rather than an approach that allows the market to develop multiple different API standards (requiring multiple integrations by each third party).[10]

Considering these features, the CGIDE TTF has been analysing an API scheme based on mobile devices to support the remote, secure and efficient identification and authentication of users of financial institutions. While the CGIDE TTF considers that the analysed implementation is viable, this is not the only possible scheme, as mentioned above, and the ideal solution for each jurisdiction will depend on several factors, such as the level of involvement of the industry in the design of the API architecture, the powers given by law to the authority leading its implementation, the target use cases that the open finance ecosystem expects to cover, or the desired user experience. From that perspective, this document should only serve as a general reference for individual countries that want to develop their own payments initiatives, and consequently no member is endorsing the adoption of open banking or the analysed identification and authentication API and central validator (CV) scheme.

The analysed scheme is based on the establishment of a CV that allows the creation of secure relationships between financial institutions and third parties, without the need for them to come into direct contact with each other. This is accomplished by establishing secure connections between the CV and third parties on the one hand, and between the financial institutions and the CV on the other. The security schemes used by the CV would ensure that all connections in the scheme are established between previously certified entities for the orderly provision of financial services through third parties. Furthermore, the CV provides the necessary elements to guarantee that each party involved in the provision of services through this scheme accesses only the user information strictly necessary to allow the provision of a specified financial service.

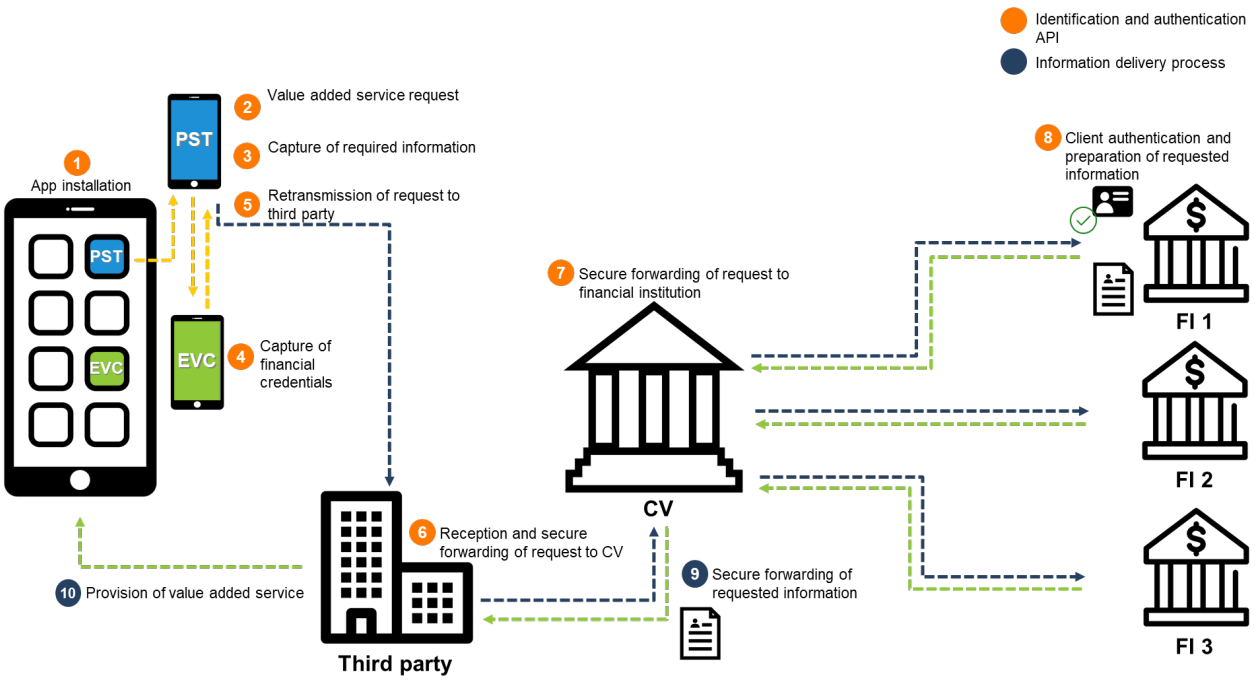
The technical requirements for the key elements of the analysed API scheme (ie the CV, third-party apps and servers, authentication app and servers) are described in detail in "Centralised validator API proposal" and "Minimal technological requirements for central validator". Furthermore, the technical requirements for the third parties interested in participating in an API scheme like the one analysed in this note are detailed in "Technical requirements for third parties".

Below we outline the general process for identifying and authenticating users with their financial institutions through a third party by using an API scheme with a CV handling the secure connections in the API architecture:

1. The user installs on their device the third-party application of their choice, as well as the CV authentication application.
2. The user logs in with their third party to request the desired financial service.
3. The third party requests that the user enter the information needed to identify their financial institution and the financial product or service related to their request.
4. The CV application asks the user to enter the authentication that they use with their financial institution. The application then encrypts the authentication data so that only the financial institution can view them, and removes them from the device so that no other party can access them. Additionally, the CV application performs tests to verify the overall integrity of the user's device.

[10] One approach might be to start by specifying APIs for the minimum range of functionality (payment initiation and account information) but allow private sector participants to propose extensions of the functionality, in the way that firms or industry groups can propose new ISO 20022 message standards for new use cases.

5. The third-party application aggregates and encrypts the information collected, and then sends it to the third party's servers.
6. The third party receives and validates the request, and retransmits it to the CV through a secure channel. The third party has access to only the data required to process the request. In particular, the third party does not have access to the credentials with which users authenticate themselves with their financial institution. The third party can check the breach status of the user's device, ie check its overall integrity and whether it is rooted.
7. The CV reviews the information received to ensure that it comes from a certified third party and verifies that it is a legitimate request. The CV can also check the breach status of the user's device.
8. Where appropriate, the CV retransmits the request to the corresponding certified financial institution through the secure channels it maintains with all of them. The CV does not have access to the authentication credentials with which the user authenticates with their financial institution.
9. The financial institution authenticates its client with the information provided by the CV application and, where appropriate, prepares to deliver the information related to the user's request.
10. The user is notified of the result of the request.




After completing the previous steps, a financial institution can verify that a request received through the CV did indeed come from its client, and is assured that the request was made through a certified third party. This allows it to safely proceed to provide the service or data that fulfil its client's

request.[11] Moreover, an identification and authentication scheme of this kind would ensure interoperability within the financial system since any certified third party could provide financial services to the users of any of the financial institutions within the scheme.

The centralised API scheme described above currently relies on the existence of an authentication app developed and maintained by the CV. This app is a fundamental piece of the scheme since it allows the users to securely input their financial credentials into the transaction flow. Moreover, the app ensures that only the user's financial institution can read these financial credentials and validates the status of the user's smartphone. However, a separate secure authentication app is not the only means to carry out these activities.

Indeed, the solution used in the scheme could be either in-app (natively integrated as a library inside the project) or an external authentication app (which necessarily implies inter-app communication). The decision on which alternative is better depends on elements such as the desired user experience, the reach of the solution (in terms of the number of people being able to use the API scheme) and the practicality of the solution for all the envisioned use cases for the API scheme.

In this regard, an authentication app solution (as described above) has the advantage of being highly efficient, since a single app can serve any number of third-party apps. Additionally, a single entity (the CV) handles the different versions and updates of the app, which facilitates orderly management of the authentication app's features. However, an authentication app solution also requires users to install an app on their smartphones whose purpose they might find obscure, thus reducing the likelihood that they will be willing to enrol in the open finance ecosystem. Additionally, switching between the CV app and the third-party apps might not be practical in use cases where the user's smartphone or internet connection do not allow this interchange to be smooth.

On the other hand, an in-app solution does not require users to install an app on their smartphones different to those that they wish to use. Similarly, since there is no need to switch between apps, the user experience might be simpler and more intuitive on a broader spectrum of smartphones. However, every third-party app to be used in the scheme would need to include the features of the secure app, which would make all these apps heavier (in terms of the memory they take up in a smartphone) and could generate different user experiences within the API scheme to some extent. In this regard, while security for credential exchange is critical, the user experience for the authentication flow (whether carried out by a CV or a private entity) is of equal importance for the implementation of any successful open finance ecosystem. On top of this, there is a certain risk when several third-party apps have to be verified by a trusted entity to avoid unsecure features that could expose user credentials.

Since both the in-app and authentication app options have pros and cons, the right choice for the API scheme of each jurisdiction should adequately balance the elements discussed above, considering the envisioned open finance ecosystem for each territory.

[11] Whether the communications needed to fulfil this request should also be exchanged through the CV is a point that requires a deep analysis. On the one hand, the participation of the CV would make these communications secure and reduce the overall complexity of the open finance ecosystem. On the other hand, however, if usage of the open finance ecosystem grows significantly, the CV must consider scalable infrastructure to avoid a bottleneck for the provision of financial services through third parties.

# Annex A: Minimal technological requirements for Central Validator

- Internet-based layer
  - Internet service
    - 150 Gbps Symmetric capacity
    - 2 different providers
  - Load balancing system (Traffic management)
    - 2 rack modules (High availability)
    - Mirror scheme with failover
    - Support capacity of at least 10 times more than expected in the following year
    - ECC or RSA encryption algorithms for TLS use
    - Using TLS v1.2 or higher for HTTPS
    - Hardware DDoS Protection
    - 64-bit architecture
    - Network interfaces at least 1Gbps, preferably 10Gbps in multimode optical fibre
  - Firewall
    - 2 rack modules (High availability)
    - Support capacity of at least 10 times more than expected in the following year
    - HTTP and HTTPS support
    - ISO/IEC 27001 Certification
    - SOC2 Certification
    - FIPS 140-2 Certification
    - Block known exploits, malware and spyware (constantly updateable) through all ports, regardless of common threat evasion tactics employed.
  - Switch
    - 2 rack modules (High availability)
    - Support capacity of at least 10 times more than expected in the following year
    - Support for 10Gbps connections
  - Router
    - 2 rack modules (High availability)
    - Support capacity of at least 10 times more than expected in the following year
    - Support for 10Gbps connections
  - DDoS attack preventing system
    - 2 rack modules (High availability)
    - Support capacity of at least 10 times more than expected in the following year
    - DDoS protection from active botnets
    - DDoS protection from active DDoS campaigns based on IP reputation
    - Advanced web crawler service
    - GeoIP tracking
    - Domain and IP reputation to block threats
    - Detect and stop both IPv4 and IPv6 attacks
    - Support for HTTPS connections

- Protection on TCP/UDP/HTTP(S) flood attacks, botnet protection, hacktivist protection, host behavioural protection, anti-spoofing, configurable flow expression filtering, payload expression-based filtering, permanent and dynamic blacklists/whitelists, traffic shaping, multiple protections for HTTP, DNS and SIP, TCP connection limiting, fragmentation attacks, connection attacks

- HSM system
  - 2 rack modules (High availability)
  - FIPS 140-2 Level 3 certification
  - Symmetric cryptography:
    - Algorithms: AES, ARIA, SEED
    - Encryption modes: CBC (Cipher Block Chaining), GCM (Galois/Counter Mode), CCM (Counter with Cipher Block Chaining-Message Authentication Code)
  - Asymmetric cryptography:
    - RSA or DH keys whose modulus has a bit length of up to 4096 bits, as well as keys whose sizes are not necessarily powers of two, such as 3072 bits. ECC keys with bit lengths of at least 224 bits
    - At least the following algorithms: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES)
  - At least the following digestion functions: SHA-2 and SHA-3 family
  - Minimum performance for signing operations:
    - 8000 operations per second using the RSA algorithm, keys whose corresponding module length is 2048 bits and exponent 65537, as well as a SHA-512 function for signature and 2KB Payload
    - 6000 operations per second using the RSA algorithm, keys whose corresponding module length is 3072 bits and exponent 65537, as well as a SHA-512 function for signature and 2KB Payload
  - High availability mechanisms
  - Network interfaces at least 1Gbps, preferably 10Gbps in multimode optical fibre
  - Use of roles and users for a correct segregation of operational and administrative functions
  - Multi-factor authentication

- Servers (High availability scheme) - Active-Passive / Cluster
  - 4 rack servers:
    - 128 GB RAM
    - 3 Tb hard disk drive (solid state/SAN)
    - 2x Processor 2.30 GHz
    - 2 Gigabit network cards (10 Gbps)
    - Replication tool for active-passive schema
    - Fail over recovering system
    - Backup system
    - 64 bit operating system
    - Hardening based on standards such as NIST or CIS
    - Third-party software downloaded only from official repositories, from where its authenticity can be verified

- Update scheme to mitigate operating system vulnerabilities, at least 3 times a year
- Upgrade scheme to mitigate third-party software vulnerabilities, at least once a year

- Private network-based layer
  - Private network provider
    - VPN capability
    - LAN2LAN capability and scalable up to 10Gbps by link

  - Load balancing system (Traffic management)
    - 2 rack modules (High availability)
    - Mirror scheme with failover
    - Support capacity of at least 10 times more than expected in the following year
    - ECC or RSA encryption algorithms for TLS use
    - Using TLS v1.2 or higher for HTTPS
    - Hardware DDoS Protection
    - 64-bit architecture
    - Network interfaces at least 1Gbps, preferably 10Gbps in multimode optical fibre

  - Firewall
    - 2 rack modules (High availability)
    - Support capacity of at least 10 times more than expected in the following year
    - HTTP and HTTPS support
    - ISO/IEC 27001 Certification
    - SOC2 Certification
    - FIPS 140-2 Certification
    - Block known exploits, malware and spyware (constantly updateable) through all ports, regardless of common threat evasion tactics employed

  - Switch
    - 2 rack modules (High availability)
    - Support capacity of at least 10 times more than expected in the following year
    - Support for 10Gbps connections

  - Router
    - 2 rack modules (High availability)
    - Support capacity of at least 10 times more than expected in the following year
    - Support for 10Gbps connections

  - HSM system
    - 2 rack modules (High availability)
    - FIPS 140-2 Level 3 certification
    - Symmetric cryptography:
      - Algorithms: AES, ARIA, SEED
      - Encryption modes: CBC (Cipher Block Chaining), GCM (Galois/Counter Mode), CCM (Counter with Cipher Block Chaining-Message Authentication Code)

        - Asymmetric cryptography:
            - RSA or DH keys whose modulus has a bit length of up to 4096 bits, as well as keys whose sizes are not necessarily powers of two, such as 3072 bits. ECC keys with bit lengths of at least 224 bits
            - At least the following algorithms: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES)
        - At least the following digestion functions: SHA-2 and SHA-3 family
        - Minimum performance for signing operations:
            - 8000 operations per second using the RSA algorithm, keys whose corresponding module length is 2048 bits and exponent 65537, as well as a SHA-512 function for signature and 2KB Payload
            - 6000 operations per second using the RSA algorithm, keys whose corresponding module length is 3072 bits and exponent 65537, as well as a SHA-512 function for signature and 2KB Payload
        - High availability mechanisms
        - Network interfaces at least 1Gbps, preferably 10Gbps in multimode optical fibre.
        - Use of roles and users for a correct segregation of operational and administrative functions
        - Multi-factor authentication

    - Servers (High availability scheme) - Active-Passive / Cluster
        - 4 rack servers:
            - 128 GB RAM
            - 3 Tb hard disk drive (solid state/SAN)
            - 2x Processor 2.30 GHz
            - 2 Gigabit network cards (10 Gbps)
            - Replication tool for active-passive schema
            - Fail over recovering system
            - Backup system
            - 64 bit operating system
            - Hardening based on standards such as NIST or CIS
            - Third-party software downloaded only from official repositories, from where its authenticity can be verified
            - Update scheme to mitigate operating system vulnerabilities, at least 3 times a year
            - Upgrade scheme to mitigate third-party software vulnerabilities, at least once a year

- Database layer
    - Servers (High availability scheme) - Active-Passive / Cluster
        - 2 rack servers:
            - 128Gb RAM
            - 3 Tb hard disk drive (solid state/SAN)
            - 2x Processor 2.30 GHz
            - 2 Gigabit network cards (10 Gbps)
            - Replication tool for active-passive schema
            - Fail over recovering system
            - Backup system

- Storage layer
    - SAN
        - Storage capacity: at least 10 times estimated data for the following next year
        - Backup system (fibre optic based)
        - Storage cluster
            - 5 Tb storage capacity
            - RAID Array 1+0, preferably RAID 6
            - 2 Gigabit network cards (10 Gbps)
            - 2 x Intel 6-core, 1.7GHz

## Annex B: Technical requirements for third parties

1. **Application to participate in the platform.** Required to get access to technical specifications document (API). The application must include:
    a. Detailed business case
    b. Confidentiality clauses for developers (Terms and conditions)
    c. Project plan to implement solution

2. **Implementation.** Development of necessary changes to implement services and processes dictated by technical specifications document applicable to existing and new Front and Back components.
    a. For backing services (validated by an external consultant):
        i. Use of digital signatures to guarantee non-repudiation and integrity of data. The third party must validate all digital signatures provided by services
        ii. Use of encryption to guarantee confidentiality of data
        iii. Pentest analysis, every year, with a plan to attend detected vulnerabilities
        iv. Complete logging for all transactions for a stablished period of time: Minimum based on FI's regulation (for transactions disputes) / Maximum based on wanted functionality for users
        v. Health check operations for web services monitoring on CV side
    b. For mobile solutions apps (validated by an external consultant):
        i. Validate that devices support secure element hardware to manage credentials and only such storage facilities must be used to store sensitive data, user credentials and cryptographic keys
        ii. Avoid devices with unsecure operative system (ie rooted, jailbroken, etc)
        iii. Implementing secure pinning for certificate management (certificate-pinning)
        iv. Secure (encrypted) storage of data (user information and transactions), for that to be possible all data considered sensitive in the context of the mobile app needs to be clearly identified
        v. Source code analysis, every year, using a specialized tool and human inspection with a complete resolution of detected vulnerabilities
        vi. Dynamic runtime analysis, every year, with a complete resolution of detected vulnerabilities
        vii. A mechanism for enforcing updates of the mobile app should exists
        viii. A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures
    c. For both sides of their solution (validated by an external consultant):
        i. An explicit policy stating how cryptographic keys are managed, and the lifecycle of cryptographic keys is enforced
        ii. Security controls enforced on the client side are also checked on their respective remote endpoints
        iii. An explicit policy stating that no sensitive data should be included in OS backup or application logs, shared or kept in memory without business functionality that required

3. **Fulfilment of Infrastructure requirements.** Fully complying with minimal requirements for hardware and telecom.
    a. Mandatory use of secure protocols for internal and external communications including the use of HTTPS with TLS v1.2 for web services requests
    b. Include use of Public Key Infrastructure (PKI) to manage digital certificates
    c. Servers and telecom equipment up to date for firmware and patches to avoid security vulnerabilities
    d. Monitoring on whole infrastructure for:
        i. Processes up and running
        ii. Health (CPU, RAM, Storage, etc) or servers and telecom equipment
        iii. Network bandwidth usage and consumption
        iv. Baseline changes
        v. Admin access and privileges
    e. Secondary or backup site
    f. Backup management plan

4. **Environment's access for testing and deploy.** This must include full access to Beta environment. Central Validator will provide digital certificates and grant permissions to access the Beta environment.

5. **Pre-certification process.** Pre-check for correct operation of third party' solution considering low-charge transactionality scenarios. This process is mandatory when applications on third party side impact platform functionality.

6. **Certification process.** Fulfilment of operational script to validate third party solution considering complete processes and high-charge transactionality scenarios. Once the third party completes the certification process, Central Validator will provide the digital certificates and permissions to operate on Production environment. This process is mandatory when applications on third party side impact platform functionality. With every new certification for a third party, Central Validator is delivering a valid token to access platform.

7. **Production testing of solution in a limited user's universe.** Validate the correct operation of third party solution with real world users and transactions. All transactions on this operational mode will be conciliated between Central Validator, third party and Financial institutions.

8. **Monitoring during a limited period.** Reconciliation of every transaction to validate correct processing and time response. In case Central Validator detects non-compliant transactions on third party side, the first could instruct to the second to repeat certification process.

## Annex C: Members of the Consultative Group on Innovation and the Digital Economy

### Members

| | |
|---|---|
| Central Bank of Argentina | María Daniela Bossio |
| Central Bank of Brazil | Angelo Duarte |
| Bank of Canada | Eric Santor |
| Central Bank of Chile | Pablo Furche |
| Central Bank of Colombia | Andrés Mauricio Velasco |
| Bank of Mexico | Miguel Díaz (Chair) |
| Central Reserve Bank of Peru | Milton Vega |
| Board of Governors of the Federal Reserve System | Francesca Carapella |
| Bank for International Settlements | Alexandre Tombini |

### Observers

| | |
|---|---|
| Bank for International Settlements | Jaime Cortina |
| | Fabrizio Zampolli |
| | Viviana Alfonso |
| | Jesse Johal |

## Annex D: Members of the Technical Task Force of the Consultative Group on Innovation and the Digital Economy

**Members**

| | |
|---|---|
| Central Bank of Argentina | Mara Misto Macías |
| | Silvina Ojeda |
| | Fernando Romero |
| | Gustavo Pereyra |
| | Mariano Vazquez |
| Central Bank of Brazil | Daniel Gersten Reiss |
| | Saulo Medeiros de Araújo |
| Bank of Canada | Alin Dan |
| Central Bank of Chile | Miguel Musa |
| | Enrique Gonzalez |
| Central Bank of Colombia | Samuel Gutiérrez |
| Bank of Mexico | Miguel Díaz (Chair) |
| | Othón Moreno Gonzalez |
| | Angel Salazar Sotelo |
| | Daniel Garrido Delgadillo |
| | Rafael Villar |
| Central Reserve Bank of Peru | Milton Vega |
| | Marco Granadino |
| Board of Governors of the Federal Reserve System | Philip Ridgway |
| | Franklin Ervin |
| | Alex Lee |
| | Peter Lone |
| BIS Innovation Hub Singapore | Andrew McCormack |

| | |
|---|---|
| Bank for International Settlements | Fabrizio Zampolli |

**Observers**

| | |
|---|---|
| Bank for International Settlements | Alexandre Tombini |
| | Jaime Cortina |
| | Viviana Alfonso |
| | Jesse Johal |