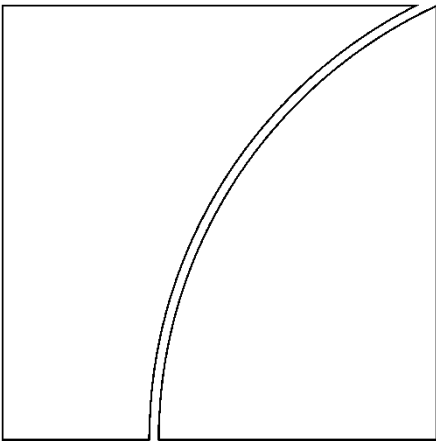


Consultative Group on Innovation and the Digital Economy



Enabling open finance through APIs Report on payment initiation

29 September 2021

BIS Representative Office for
the Americas

Comments are welcome and should be addressed to:
CGIDReport@bis.org



BANK FOR INTERNATIONAL SETTLEMENTS

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

© Bank for International Settlements 2021. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.

ISBN 978-92-9259-507-4 (online)

Table of contents

- Foreword..... 1
- Introduction..... 2
 - Background 3
- Payment initiation alternatives analysed by the CGIDE TTF..... 4
 - CV auth-app scheme 4
 - With an in-app scheme..... 7
 - Comparison of aspects 9
- Technical architecture..... 10
- Annex A: Members of the Consultative Group on Innovation and the Digital Economy..... 13
- Annex B: Members of the Technical Task Force of the Consultative Group on Innovation and the Digital Economy 14
- Annex C: Technological requirements identified for a Central Validator’s implementation..... 16
 - Attached “known technology” :..... 25
- Annex D: Cybersecurity in the API ecosystem 26
 - Cybersecurity governance 26
 - Cybersecurity guidelines 27
 - 1. Identifying assets and risks 27
 - 2. Protecting data and IT assets 30
 - 3. Detecting anomalies 35
 - 4. Incident response..... 36
 - 5. Recovering from incidents..... 37
- Annex E: Industry outreach learnings..... 39
 - General perspective..... 39
 - Adaptability 40
 - API as a publicly available club good..... 40
 - User experience 41
 - Risk management and liability 42
 - Stakeholder perspective 44

Developers	44
Financial institutions	45
Third parties for payment initiation	45
Annex: Definitions	46

Table of Figures

Figure 1: Payment initiation with CV auth-app	6
Figure 2: User Journey with AA scheme	7
Figure 3: Payment initiation with in-application	9
Figure 4: CV auth-app and in-app comparison	9
Figure 5: Technological requirements identified for a CV's implementation	11
Figure 6: Stakeholders analysed	39
Figure 7: Types of Goods	41
Figure 8: General outreach industry perspectives	43

Foreword

This “Report on payment initiation” is the second report published by the Consultative Group on Innovation and the Digital Economy (CGIDE) on “Enabling open finance through APIs”. The first report of the CGIDE, published in December 2020, explores 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. This second report analyses two alternative API architectures for payment initiation, both based on an authentication app for mobile phones developed and maintained by a central validator. The first involves the use of a stand-alone app managed by the central validator to authenticate customers for each transaction. The second involves an embedded functionality that allows customers to use their third-party app after an initial onboarding with the central validator’s authentication application.

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*. Thus, this group, as part of the implementations made in mentioned strategy, 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 report has been prepared by a technical task force of central banks experts under the guidance of the main central bank representatives in the CGIDE. It is now published to inform the public of the cooperative efforts by the largest central banks in the Americas. While no central bank is endorsing the adoption of open banking or the analysed API scheme, the document can nevertheless serve as a useful general reference for central banks that want to develop their own payment initiatives. Comments are welcome and should be addressed to CGIDEREport@bis.org.

Miguel Díaz
Chair of the CGIDE, Bank of Mexico

Alexandre Tombini
BIS Chief Representative for the Americas

Introduction

This report summarises the analysis conducted by the Technical Task Force (TTF) of the Consultative Group on Innovation and the Digital Economy (CGIDE) on the solutions available for payment initiation within a centralized application programming interface (API) architecture. Specifically, two solutions for payment initiation are explored: (i) the first makes use of a central validator (CV) auth-app such as the one described in the first report published by the CGIDE in December 2020,¹ provided by a CV for the authentication and validation; (ii) the second involves the use of a similar functionality natively integrated in a payment initiator's payment app. Both solutions build on the secure identification and authentication of users analysed in previous CGIDE work. In addition, the report summarises the main insights gained from meetings held with several industry participants.

Documents produced by the CGIDE TTF are: (i) this high-level note, which serves as background for the technical deliverables; (ii) technical flow diagrams of payment initiation processes based on a centralised API architecture (available upon request); (iii) an update on the general hardware requirements to implement the payment initiation solution described in this report (Annex C: Technological requirements identified for a Central Validator's implementation); (iv) cyber security elements relevant for designing and operating such infrastructure for the respective payment initiation scheme (Annex D: Cybersecurity in the API ecosystem); and (v) a report on work with the industry to deepen analysis of stakeholders in the open banking ecosystem (Annex E: Industry outreach learnings).

As in the previous report, the work of the CGIDE TTF did not include a review of all possible alternatives for payment initiation to achieve secure and remote identification and authentication through APIs. From that perspective, this document should only serve as a general reference for stakeholders that want to develop their own payment initiation initiatives, and consequently, no CGIDE TTF member is endorsing the adoption of open finance for the analysed identification and authentication API and CV scheme.

The first section of this report presents a brief background on CGIDE work on enabling open finance through APIs. The second part presents the payment initiation alternatives for authentication and validation along with technical details. The third section examines the technological requirements identified for the implementation of a CV. The concepts used frequently in the document are defined in Annex: Definitions .

¹ Consultative Group on Innovation and the Digital Economy (CGIDE), *Enabling open finance through APIs*, December 2020.

Background

The main objective of the CGIDE TTF is to explore the development of an API solution for identification and authentication that can be used to implement privately and publicly managed open financial solutions with seamless scalability. Therefore, one of the questions the CGIDE TTF is currently asking is how to develop a way in which basic financial services provided by financial institutions can be made available to customers through third parties in an efficient and secure manner. To address this question, the CGIDE TTF has worked on two reports. The first report was published in December 2020 with the technical elements needed to authenticate and validate the identity of a customer interacting with third parties, based on a CV.²

As part of the mentioned first report, the CGIDE TTF highlighted the importance for the participants in an open financial ecosystem of remote and secure identification and authentication of users. It focused on the analysis and design of a viable architecture for those purposes in which implementation in the context of a payment initiation assures different entities that the request has indeed been made by their users. Identification and authentication processes stems from the fact that, in the context of traditional relationships among entities for the provision of payment initiation services, the participants usually know each other in advance and have agreed specific terms of service in order to establish connections to exchange information for the purpose of providing a payment service. However, if the parties have no prior relationship with each other, different challenges must be addressed to enable them to interact securely and remotely. In particular, the lack of trust between the parties, possibly incompatible technological infrastructures and misaligned incentives for the relationship to develop need to be addressed.

The objective of this architecture is to find a scheme in which customers are allowed to reach their financial institutions through additional interfaces in a secure and efficient way. This scheme is in addition to building trust among the financial institution and the third-party in the customer authentication process. This makes the proposed scheme a mechanism for establishing secure connections and core authentication. The design of an open financial ecosystem is heavily influenced by the architecture of the identification and authentication APIs that support it. One of the defining characteristics of this architecture is how connections between participants in the open financial ecosystem are managed. The main alternatives are: (i) centralised connections; and (ii) bilateral or multilateral connections (including independent networks). These alternatives have pros and cons that mirror each other in a certain degree. Both options were explored in the first CGIDE report, this report focuses only on centralised connections. With centralised connections there is a central actor to which all participants must be connected. This implies that, unlike a decentralised scheme, there is a single network of connections within the ecosystem, which is governed by the rules set by the central entity. Besides that, the scheme proposed by the CGIDE TTF for payment initiation 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.

Security of the relationship is accomplished by establishing secure connections between the CV and third parties for payment initiation on the one hand, and between any interested account holding institution and the CV on the other. Security protocols are used by the CV which ensure that all connections in the scheme are established between entities – amended on the basis that it is the entities which had previously been certified – for the orderly third-party provision of financial services. In the context of payment initiation, this framework facilitates the secure and interoperable provision of services through third parties. It encourages the integration of parties into the open finance ecosystem and ensures that user information for the payment is securely transmitted, processed and managed. This framework allows

² CGIDE, op cit.

for the promotion of necessary conditions for fair competition, ensuring a level playing field for all market participants, scalability, and the space for future innovation.

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 specific financial service. This scheme could be implemented through two alternatives:

- i. An independent CV auth-app, which suggests that the authentication is managed by this app which was developed and provided by the CV; or,
- ii. An embedded authentication process in a third-party app. The third-party app is the one is the application that the third-party payment initiation service provider makes available to the user to initiate payments. In this case, the authentication is managed by the third-party within its application.

CV scheme is at the core of the authentication process, and the app solution is crucial to this. It allows a user to securely input their financial credentials into the transaction flow and ensures that only the user's financial institution can read these financial credentials. The CV scheme also validates the integrity status of the user's device. In this context, an open and standardised API scheme payment initiation, along with a clear set of rules, can align the incentives of the interacting parties so that each entity benefits from its remote relationship. However, there are certain minimum requirements that third parties must have in order for this trusted network to be sustained. Those requirements are identified in the previous report by CGIDE TTF in the section titled, *Technical requirements for third parties*.³

Payment initiation alternatives analysed by the CGIDE TTF

In this second report of CGIDE, the objective is to define the elements necessary to operate a payment initiation process based on the architecture of a CV described above. This document presents the payment initiation alternatives based on the authentication and identity validation process described in the first report. Thus, recapping, it is possible to identify two ways of implementing a functional architecture using: (i) a stand-alone app managed by the CV to authenticate customers for each transaction; and (ii) an embedded functionality that allows customers to use their third-party app after an initial onboarding with the CV's authentication application.

CV auth-app scheme

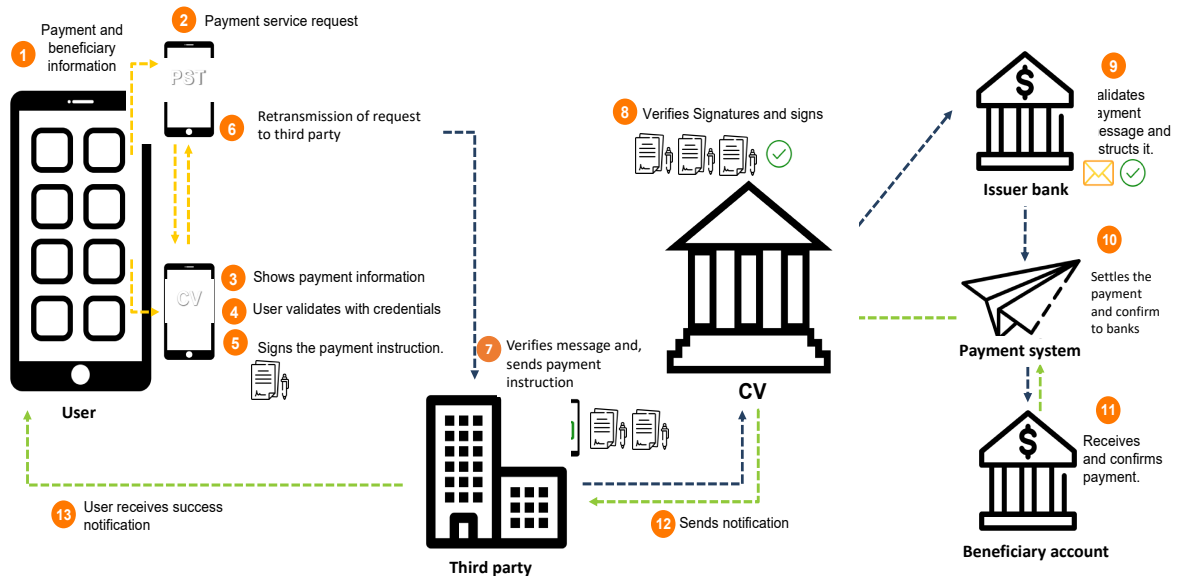
We outline below the general process for payment initiation through an auth-app solution in which a CV handles secure connections within the API architecture. The process is:

1. The user installs the third-party application of their choice on their device, as well as the CV auth-app, and provides payment and beneficiary information as part of the payment application. Payment information required beneficiary's name, beneficiary account identifier, beneficiary's bank, beneficiary's account type, amount and payment description.
2. The third-party requests the signing of the payment instruction via the CV auth-app.
3. CV auth-app shows payment information to the user transaction ID, account identifier, issuer bank and beneficiary's information.

³ CGIDE, op cit.

4. User validates the information and confirms transaction by inserting their authentication elements⁴ via the CV auth-app. The CV auth-app is based on the authentication method of the user's financial institution. The third-party application then encrypts the payment data (provided by the user in stage 1 above) so that only the financial institution can view them. It then removes them from the device so that no other party can access them. Additionally, the CV auth-app performs tests to verify the overall integrity of the user's device.
5. The CV auth-app signs the payment instruction CV auth-app's signature means that there are integrity and non-repudiation protocols. In other words, the auth-app is acting as a secure route for payment initiation.
6. The third-party application reviews CV auth-app credentials to ensure the source is a certified CV auth-app. The third-party application then aggregates and encrypts the information collected, and then sends it to the third-party application servers using a secure channel.
7. The third-party application server receives and validates the payment request and retransmits it to the CV through a secure channel. The validation guarantees payment application integrity. The third-party application server has access only to the data required to process the payment request. In particular, the third-party application does not have access to the credentials with which a user authenticates themselves to their financial institution. The third-party can check the breach status of a user's device, i.e. check its overall integrity.
8. The CV verifies both the payment application and CV auth-app signatures – it can also check the integrity status of the user's device – and includes its own signature to ensure that it comes from a certified third-party application and verifies that it is a legitimate request. Then the CV sends a payment request to the issuer bank. The CV does not have access to the authentication credentials with which the user authenticates with their financial institution.
9. Issuer bank validates the payment instruction message and sends the payment to the payment system.
10. The payment system settles the payment and the issuer bank and recipient bank receive payment confirmation.
11. Recipient bank notifies the payment system when beneficiary account was credited.
12. Payment system notifies the payment app.
13. The user receives notification of the payment final status through their payment app.

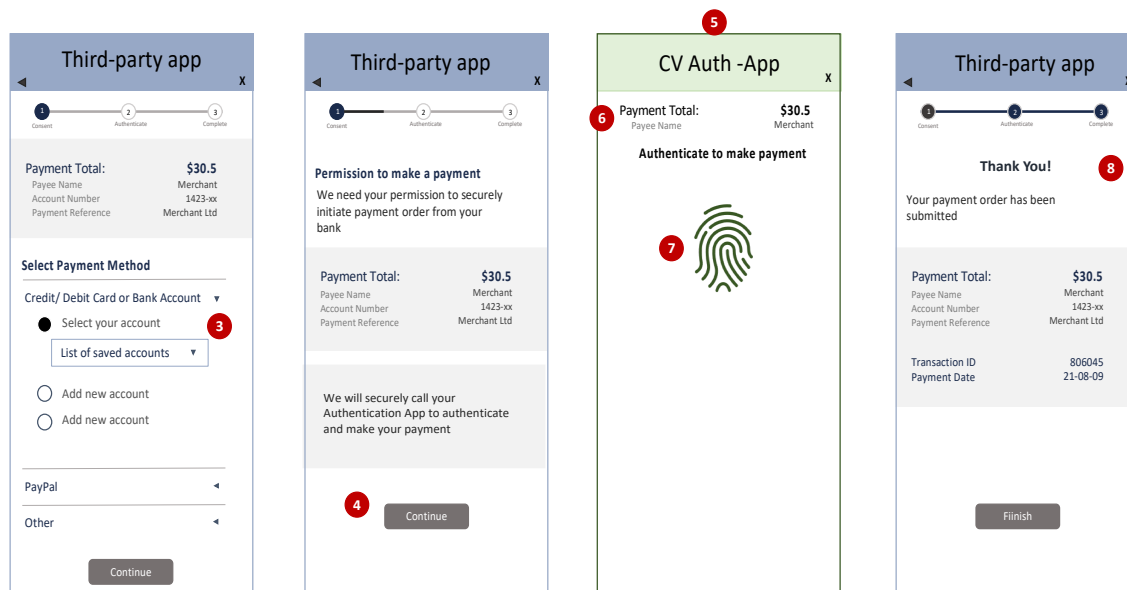
⁴ These authentication elements are those with which the user identified himself and generated with the aa in stages prior to payment initiation. The elements depend on the features that the CV implements in the auth-app. An example of these elements could be a previously established username and password, or facial identification, depending of the operative system of the user device. We avoid using the word credentials to avoid confusion with the user's payment credentials.



The independent CV auth-app solution brings some efficiencies such as the possibility of using it a wide array of third-party payment apps and the ability to handle the different versions and security updates facilitating the management of auth-app’s features in one app. However, it requires the installation of another app in addition to the third-party app. In the event that users are not appropriately informed about its functionality they may find it complex and this might reduce the likelihood of enrollment. Additionally, switching between the CV auth-app and the third-party apps might not be practical where the user’s smartphone or internet connection does not allow for a smooth interchange. This report does not consider flaws in the process or breakpoints, but only provides an overview.

From the user’s perspective, it is necessary to establish how initiating a payment would work to ensure a simplified experience. In addition, in this scheme there may be several third-party applications connected to the same auth-app CV. One use case is that users can initiate payments making a one-time payment for a specific amount to a specific payee. They can do this by giving their consent to third parties and sending an instruction to their authenticators.

When all the information for a complete payment order (including the users' account data) is transmitted from the third parties to the auth-app it can be directed back to the third parties' domain without any further steps in the authenticating application's domain once the user has been authenticated. The following describes the steps to initiate a payment from the third-party application with a simplified user perspective.



1. The user connects to the application arranged by the third-party of their choice. This scheme assumes that the user has authenticated and performed the registration processes determined by the third-party.
2. The user instructs the third-party's application to make a payment and then the third-party provides the beneficiary's data.
3. The user selects the option provided by the third-party to make the payment through the authentication application.
4. The user provides consent to initiate payment order and be redirected to the authentication application interface
5. The user is redirected to the authentication application interface. It can be displayed in the foreground; the objective is to make the user aware that the next step is with the CV auth-app and not with the third-party.
6. The CV auth-app displays the payment details including payee information, amount and account identifier to be debited. It prompts the user to authenticate it to confirm the completion of the transaction.
7. The user enters the information requested by the CV auth-app.
8. The user is redirected to third-party to receive confirmation of transaction

Third parties should follow-up with the CV auth-app to check and update users with the most current information they can receive regarding the execution of the payment.

With an in-app scheme

The solution may be also implemented through an in-app model, that is, through a natively integrated library inside the third-party app. An in-app solution does not require users to install another app on their smartphones in addition to the provided by the third-party. With an in-app solution, since there is no need to switch between apps, the user experience might be simpler and more intuitive on a broader spectrum

of smartphones. On the other hand, it might feel more comfortable to share credentials in a single trusted CV application rather than providing their payment information to each third-party application. Furthermore, every third-party app to be used in the scheme would need to include the features of the CV auth-app scheme, which would make all these apps larger – in terms of device storage space they take up in a smartphone – and could generate different user experiences within the API scheme to some extent. This is aside from the additional effort on the part of the third party to integrate authentication into their native application.

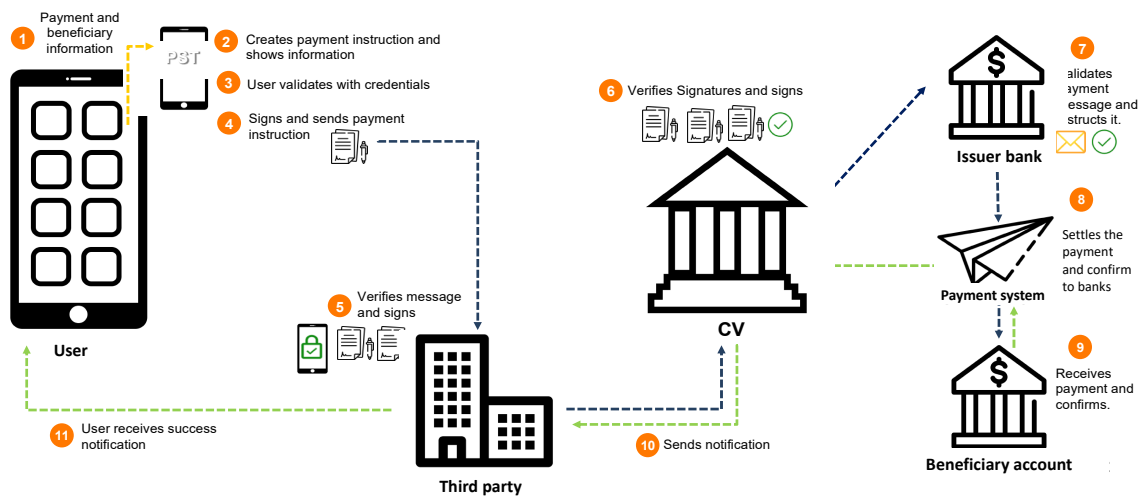
Although there is no separate application, the differences between the CV auth-app and the in-application schemes are found in steps 2 and 3 above. We will focus the analysis on the differences between schemes since everything else remains constant. Thus, we outline below the process for payment initiation through an in-app solution up to step 5, by using an API scheme with a CV handling the secure connections in the API architecture (in-application scheme):

1. The user installs the third-party application of their choice on their device and provides payment and beneficiary information. Payment information required: beneficiary's name, beneficiary account identifier, beneficiary's bank, beneficiary's account type, amount and payment description.
2. Third party app creates the payment instruction and shows the payment information to the user.
3. User validates the information and enters their authentication elements.⁵ The third-party application asks the user to enter the authentication elements that they use with their financial institution. The application then encrypts the payment 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 third-party app performs tests to verify the overall integrity of the user's device.
4. The third-party application aggregates and encrypts the information collected and then sends it to the third-party application servers using a secure channel
5. The third-party application server receives and validates the request and retransmits it to the CV through a secure channel. The third-party application server only has access to the data required to process the request. In particular, the third-party app server 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, i.e. check its overall integrity and whether it is rooted.

The subsequent steps (indicated in the diagram from 6 to 11) are equivalent to steps 7 to 13 of the scheme with a CV Auth-app outlined above in Figure 1.

However, it is relevant to mention that the key difference between the two payment initiation alternatives explored in this report is with respect to the financial liability implications that may result from management of certificates and information necessary to validate client's identity. On one hand, under the use of a CV auth-app scheme, the authentication process is managed by a secure central validating app which does not store information about authentication factors for payment initiation. Consequently, there is no shifting of responsibility through third parties. This is because every party in the system has jointly decided that the CV is a trusted central entity. On the other hand, with the in-app scheme the third-party manages and has access to user credentials within the same application. This implies that it has responsibility for key management and, consequently, for users' data in payment processing. It should be noted that this document does not consider flaws in the process or breakpoints, but only provides an overview.

⁵ These authentication elements are those with which the user identified himself and generated with the aa in stages prior to payment initiation. The elements depend on the features that the cv implements in the aa. An example of these elements could be a previously established username and password, or face Id, depending of the operative system of the user device. We avoid using the word credentials to keep from confusing them with the user's payment credentials.



Comparison of aspects

The decision about which alternative to establish depends on elements such as the desired user experience, reach of the solution (in terms of the number of people being able to use the API scheme) and the applicability of the solution for all the envisioned use cases for the API scheme. Since both the CV auth-app and the in-app options have pros and cons, the right choice for the API scheme for each jurisdiction should adequately balance the elements discussed above, considering the envisioned open finance ecosystem for each.

CV auth-app and in-app comparison

Figure 4

Aspects	CV auth-app scheme	In-application scheme
Authentication channel	The auth-app needs to be separately installed by the user on their device.	The auth-app is a natively integrated library inside the third-party app
Liability	There is no shift of liability through the third-party.	It implies responsibility for management of the keys, and consequently, the user must rely on the processing of payment data, made by each third-party.
User experience	Might be affected by a different app installation on user’s device.	Might be simpler and more intuitive.

User trust	Might feel more comfortable since user only needs to trust a single application to handle their credentials	Might be adversely impacted since user needs to share payment information with every third-party they want to use.
Efficiency	Highly efficient since a single app can serve any number of third-party apps	The authentication channel can only serve one third-party app each.
Smartphone requirements	Switching between the CV auth-app and third-party apps might not be practical in cases where the user's smartphone or internet connection does not allow this interchange to be smooth. Device must have enough capacity to perform this change of apps.	Larger apps in terms of memory usage, since they need to include the features of the secure app.
Secure features	Just one CV auth-app must be verified by the CV.	Several third-party authentication channels must be verified by the CV
Management of updates (from CV perspective)	Single management of versions and updates of the authentication channel	Multiple versions and updates of the authentication channel since each third party manages its own updates.
Between app communication	Inter-app communication required.	Communication within the same app.

Technical architecture

A traditional relationship between entities implies that they know each other, have previously established terms of service, conditions for sharing information as well as the different elements in place which are needed for a secure connection. A challenge that institutions often face is technology and systems differences; an API framework can facilitate the necessary interoperability for all stakeholders in the open finance ecosystem.

Thus, a clear set of rules for using an API scheme, such as the one mentioned above, can align the incentives of the interacting parties so that each entity benefits from their relationship through the CV, as the second section of this report details. Furthermore, these rules, potentially in conjunction with appropriate regulation, can ensure the security and integrity of the open finance ecosystem. In this regard, for the proper functioning of the ecosystem, the CV must fulfil its fundamental role of establishing secure relationships among the participants.

The preceding report of the CGIDE TTF presented the *Minimal technology requirements for Central Validator* consistent with the key elements of the analysed API scheme. This involved third-party apps and servers, and authentication app and servers. This report updates those requirements to identify the applicable technology elements for the implementation of a CV in the context of payment initiation. Requirements are summarised in the following table, but the details are included as part of Annex C.

Summary of technological requirements for CV	
1. Internet -based layer. This layer is for allocating services offered by the CV and is mainly consumed by third parties.	
2. Private network-based layer. This layer offers connectivity services between financial institutions and the CV, with the vision of maintaining a scheme that has high availability, service stability and protection against cyberattacks.	
3. Database layer. This layer provides management capabilities for two types of CV's data: data that requires high processing speed and data that requires storage for persistence and availability.	
4. Storage layer. This layer provides scalability in storage space in a simple way in case the computer equipment does not support hard disk growth.	
5. Transaction manager layer. This layer provides simple integration of communication between applications, oriented to publish-subscribe schemes.	
Technological components tradeoffs resume	
Internet service	Despite the high cost associated with installing and maintaining a dedicated and private telecommunications infrastructure for the internet-based layer, availability requirements drive the decision over shared and public links. A load balancing function in this layer will make it resilient to high transaction scenarios.
Load balancing system	Despite the high cost of load balancers, they ensure reliability and availability by monitoring the health of the application and only sending requests to servers and applications that can respond privately.
Firewall	The use of a firewall reduces the risk of malicious traffic. Investing in a high-performance device, it will allow the maintenance of a good level of security of the internal network without affecting the performance of the system.
Switch & Router	Despite the cost of a 10 Gbps device relative to a 1 Gbps device, this will reduce latency problems.
Distributed denial of service (DDoS) attack preventing system	A mitigation system that designates security resources and protocols necessary to mitigate the effects of a DDoS attack.
Hardware security module (HSM)	Despite the cost and possible decrease in performance compared to not having it, this should guarantee proper storage and management of the cryptographic keys used by the CV.

Server pool	Despite the cost of having equipment with high processing or high storage capabilities and considering the complexity that the use of cluster schemes may imply, it must guarantee good performance and availability of the services provided by the CV to third party participants.
--------------------	--

The technical requirements for the third parties interested in participating in an API scheme like the one analysed for payment initiation are those outlined in the section titled *Technical requirements for third parties* in the previous report of the CGIDE TTF.⁶

A final aspect of this technological framework is cybersecurity issues involved in designing and operating such infrastructure. For that purpose, the CGIDE TTF analysed the context of an API ecosystem and proposes five guidelines as part of this report in which cybersecurity controls, mechanisms, best practices, and procedures could be grouped. They are summarised in the following and the details are presented as part of Annex D:

1. Asset and risk identification. Be clear about which assets to be protected and against which kind of threats. Accordingly, build a flexible risk management process to assess the identified risks and facilitate decision-making about the measures to be taken to eliminate, mitigate, transfer, or tolerate them. This will assist in anticipating possible impacts on the business.
2. Protection of data and IT assets. Adopt robust authentication and access control mechanisms, strong and up to date data encryption methods and global standards for the development of secure software. Additionally, adopt best practices, processes and procedures for the protection of information.
3. Detection of anomalies and events that may compromise the confidentiality, integrity and availability of information and IT assets. Documented processes for the detection of threats and vulnerabilities, analysis and monitoring tools must be available
4. Incident response in crisis mode. Planning, coordination, and drills can result in less downtime and less data loss. Analysis and planning processes should be conducted to ensure effective response and support for recovery efforts.
5. Incident recovery procedures. We must have in place business continuity strategies and a communications plan to ensure that in the event that the risks identified in the first phase materialise, the operation can continue at a minimum acceptable level.

⁶ CGIDE, op cit.

Annex A: 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

Observers

Bank for International Settlements	Alexandre Tombini
	Jaime Cortina
	Fabrizio Zampolli
	Viviana Alfonso
	Jesse Johal

Annex B: 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

Observers

Bank for International Settlements

Alexandre Tombini

Jaime Cortina

Fabrizio Zampolli

Viviana Alfonso

Jesse Johal

Annex C: Technological requirements identified for a Central Validator's implementation

The purpose of this annex is to provide guidelines on identifying technology elements applicable for implementing a Central Validator (CV).

Neither architectural layers nor technological components are mandatory for a CV 's implementation. However, considering all the proposed layers (and components) they could help to foster efficiency of performance and scalability.

In the next pages the reader will find a brief description and a list of specific components for each suggested layer, along with some trade-offs relating to their inclusion.

Internet -based layer:

This layer is for allocating services offered by the CV which are mainly consumed by third parties.⁷ Accordingly, services allocated in this layer are consumed directly by applications implemented by third parties, and this layer therefore requires high availability and load-balancing schemes, as well as protection against cyber-attacks (i.e., DDoS).

➤ **Technology components:**

❖ **Internet service.** Dedicated and private link is highly recommended for each participant (third-party or financial institution)

- **Tradeoffs.** Despite the high cost associated with the setup and maintenance of a dedicated and private telecommunications infrastructure for the Internet -based layer, availability requirements drive the decision against shared and public links. Dedicated and redundant Internet links will aim to increase possibilities for a good compliance on the business continuity goals established for the operational model. A load-balancing feature on this layer will make it resilient to high transactional scenarios. Finally, an anti-distributed denial of service (DDoS) mechanism is highly recommended to protect the layer against focused attacks and thus avoid availability issues.

- **Main features:**

- Bandwidth 10 times greater than the estimated traffic for the next year based on expected consumption of services and volume of transactions. Estimations must consider expected peak transaction volume.
- Redundant links with different providers with the choice to switch to other providers in the event of the failure of one of them.

❖ **Load balancing system** (traffic management). This refers to the distribution of incoming network traffic across a group of backend servers. Continuity of operation must be guaranteed at high volumes even after the failure of some balancing equipment (failover mode), as well as guaranteeing easy horizontal scalability.

⁷ Some financial institutions may have access to these services through this layer on a regular basis or only for contingency purposes.

- **Tradeoff.** Despite the high cost of load balancers, they ensure reliability and availability by monitoring the health of applications and only sending requests to servers and applications that can respond appropriately.

- **Main features:**

- 2 balancing items of equipment configured in failover mode.
- Mirroring capability with failover to avoid losing operations due to a failure in the main equipment.
- Capacity to process at least 10 times the number of requests per second expected in the following year.
- Elliptic Curve Cryptography (ECC) or Rivest–Shamir–Adleman (RSA) encryption algorithms for Transport Layer Security (TLS) use, guaranteeing the use of robust encryption algorithms that prevent information theft.
- Use of TLS v1.2 or higher for HTTPS, ensuring the use of robust communication channel encryption schemes between third-party participants and the CV.
- Hardware DDoS protection, to guarantee a first containment measure against denial of service attacks that could affect the availability of the system.
- 10 Gbps in multimode optical fibre, to guarantee a high data transmission speed between: internet link, balancer and server pool.

- ❖ **Firewall.** This is a physical device connected between the external network and the internal network of the CV, the purpose of which is to monitor all network traffic in order to identify and block unwanted traffic. It must guarantee a high level of protection that does not affect the performance of the system.

- **Tradeoff.** The use of a firewall reduces the risk of malicious traffic. Investing in a high-performance device will allow the maintenance of a good level of security for the internal network without affecting the performance of the system.

- **Main features:**

- 2 firewall items of equipment configured in failover mode.
- Capacity to process at least 10 times the number of requests per second expected in the following year.
- HTTP and HTTPS support to guarantee complete traffic analysis.
- Federal Information Processing Standard (FIPS) 140-2 level 3 certification to guarantee the safety of the equipment against physical manipulations.
- Should be able to block known exploits, malware and spyware through all ports, regardless of common threat evasion tactics employed.
- Should provide a way to update the firmware in order to stay current on threat developments.

- ❖ **Switch.** This is the logical digital device for interconnection of equipment that works in the data link layer of the Open Systems Interconnection Model. It must guarantee the handling of all traffic within the internal network of the CV by supporting the protocols and network connection technologies employed.

- **Tradeoff.** Despite the cost of a 10 Gbps device relative to a 1 Gbps device, a 10 Gbps device will reduce latency problems within the CV's network.

- **Main features:**
 - 2 rack modules in failover mode.
 - Capacity to process at least 10 times the number of requests per second expected in the following year.
 - Support for 10 Gbps connections to guarantee high-speed data transmission.

❖ **Router.** It is the device that manages the data traffic that is sent within a computer network. It must guarantee the handling of all traffic within the internal network of the CV by supporting the protocols and network connection technologies employed.

- **Tradeoff.** Despite the cost of a 10 Gbps device relative to a 1 Gbps device, a 10 Gbps device will reduce latency problems within the CV's network.

- **Main features:**
 - 2 rack modules in failover mode.
 - Capacity to process at least 10 times the number of requests per second expected in the following year.
 - Support for 10 Gbps connections to guarantee high-speed data transmission.

❖ **DDoS attack prevention system.** A mitigation system that designates the security resources and protocols necessary to mitigate the effects of a DDoS attack.

- **Tradeoff.** Despite the cost and possible decrease in performance compared to not having it, this device guarantees continuity of operation during DDoS attacks, without reducing the service level below the minimum threshold established for the system by the CV.

- **Main features:**
 - 2 rack modules in failover mode.
 - Capacity to process at least 10 times the number of requests per second expected in the following year under normal operation.
 - DDoS protection from active botnets.
 - DDoS protection from active DDoS campaigns based on IP reputation.
 - Advanced web crawler service.
 - GeolP 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 behavioral 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 and connection attacks.

❖ **Hardware security module (HSM).** This is a hardware-based cryptographic device that generates, stores and protects cryptographic keys and often provides hardware acceleration for cryptographic operations.

- **Tradeoff.** Despite the cost and possible decrease in performance compared to not having it, this should guarantee the proper storage and management of the cryptographic keys used by the CV.

- **Main features:**

- 2 rack modules in failover mode.
- FIPS 140-2 level 3 certification to guarantee the safety of the equipment against physical manipulations.
- Symmetric cryptography: Algorithms AES, ARIA and SEED.
- Encryption modes: Cipher Block Chaining (CBC), Galois/Counter Mode (GCM), Counter with Cipher Block Chaining-Message Authentication Code (CCM).
- Asymmetric cryptography: RSA or Diffie–Hellman (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, considering 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, considering 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 of at least 1 Gbps, preferably 10 Gbps in multimode optical fiber.
- Use of roles and users for a correct segregation of operational and administrative functions.
- Multi-factor authentication.

❖ **Server pool.** Set of servers that provide the same services.

- **Tradeoff.** Despite the cost of having equipment with high processing or high storage capabilities, and considering the complexity that the use of cluster schemes may imply, it must guarantee good performance and availability of the services provided by the CV to third-party participants.

- **Main features:**

- 4 rack servers:
128 GB RAM.
- 3 Tb hard disk drive (solid state/ storage area network (SAN)).
- 2x processor 2.30 GHz.
- 2 gigabit network cards (10 Gbps) on failover schema.
- 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:

This layer offers connectivity services between financial institutions and the CV with the goal of maintaining a scheme that has high availability, service stability and protection against cyberattacks.

➤ **Technology components:**

❖ **Private network provider.** Private network between the CV and the financial institutions. It can be set-up using a VPN or a LAN-to-LAN connection.

- **Tradeoff.** Despite the high cost of installing the telecommunications infrastructure, the use of a dedicated link will guarantee privacy and security of communications between the CV and financial institutions.

- **Main features:**

- VPN capability to ensure channel encryption in case communications with financial institutions must be over the internet.
- LAN2LAN capability and scalable up to 10 Gbps by link.

❖ **Load balancing system** (traffic management). This refers to the distribution of incoming network traffic across a group of backend servers. Continuity of operation must be guaranteed at high volumes even after the failure of some balancing equipment (failover mode), as well as guaranteeing easy horizontal scalability.

- **Tradeoff:** Despite the high cost of load balancers, they ensure reliability and availability by monitoring the health of applications and only sending requests to servers and applications that can respond appropriately.

- **Main features:**

- 2 items of balancing equipment configured in failover mode.
- Mirroring capability with failover to avoid losing operations due to a failure in the main equipment.
- Capacity to process at least 10 times the number of requests per second expected in the following year.
- ECC or RSA encryption algorithms for TLS use, guaranteeing the use of robust encryption algorithms that prevent information theft.
- Use of TLS v1.2 or higher for HTTPS, ensuring the use of robust communication channel encryption schemes between third-party participants and the CV.
- Hardware DDoS protection, to guarantee a first containment measure against DDoS attacks that could affect the availability of the system is in place.
- 10 Gbps in multimode optical fibre, to guarantee a high data transmission speed between: internet link, balancer and server pool.

❖ **Firewall.** This is a physical device connected between the external network and the internal network of the CV, the purpose of which is to monitor all network traffic in order to identify and block

unwanted traffic. It must guarantee a high level of protection that does not affect the performance of the system.

- **Tradeoff.** The use of a firewall reduces the risk of malicious traffic. Investing in a high-performance device will allow the maintenance of a good level of security of the internal network without affecting the performance of the system.

- **Main features:**

- 2 items of firewall equipment configured in failover mode.
- Capacity to process at least 10 times the number of requests per second expected in the following year.
- HTTP and HTTPS support to guarantee complete traffic analysis.
- FIPS 140-2 level 3 certification to guarantee the safety of the equipment against physical manipulations.
- Should be able to block known exploits, malware and spyware through all ports, regardless of common threat evasion tactics employed.
- Should provide a way to update the firmware in order to stay current on threat developments.

❖ **Switch.** This is the logical digital device for interconnection of equipment that works in the data link layer of the OSI model. It must guarantee the handling of all traffic within the internal network of the CV by supporting the protocols and network connection technologies employed.

- **Tradeoff.** Despite the cost of a 10 Gbps device relative to a 1Gbps device, this will reduce latency problems within the CV's network.

- **Main features:**

- 2 rack modules in failover mode.
- Capacity to process at least 10 times the number of requests per second expected in the following year.
- Support for 10 Gbps connections to guarantee high-speed data transmission.

❖ **Router.** This is the device that manages data traffic sent within a computer network. It must guarantee the handling of all traffic within the internal network of the CV by supporting the protocols and network connection technologies employed.

- **Tradeoff.** Despite the cost of a 10 Gbps device relative to a 1 Gbps device, this will reduce latency problems within the CV's network.

- **Main features:**

- 2 rack modules in failover mode.
- Capacity to process at least 10 times the number of requests per second expected in the following year.
- Support for 10 Gbps connections to guarantee high-speed data transmission.

❖ **Hardware security module (HSM).** This is a hardware-based cryptographic device that generates, stores and protects cryptographic keys and often provides hardware acceleration for cryptographic operations.

- **Tradeoff.** Despite the cost and possible decrease in performance compared to not having it, this should guarantee the proper storage and management of the cryptographic keys used by the central validator.

- **Main features:**

- 2 rack modules in failover mode.
- FIPS 140-2 level 3 certification to guarantee the safety of the equipment against physical manipulations.
- Symmetric cryptography: Algorithms AES, ARIA, SEED
- Encryption modes: CBC, GCM and CCM.
- 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, considering 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, considering 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 of at least 1 Gbps, preferably 10Gbps in multimode optical fibre.
- Use of roles and users for a correct segregation of operational and administrative functions.
- Multi-factor authentication.

- ❖ **Server pool.** A set of servers that provide the same services.

- **Tradeoff.** Despite the cost of having equipment with high processing or high storage capabilities, and considering the complexity that the use of cluster schemes may involve, it must guarantee good performance and availability of the services provided by the CV to the issuer's banks.

- **Main features:**

- 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) on failover schema.
 - Replication tool for active-passive schema.
 - Failover recovery 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:

This layer provides management capabilities for two types of CV's data: data that requires high processing speed and data that requires storage for persistence and availability.

➤ **Technology components:**

❖ **Dynamic/fast data (active-passive/cluster).** The purpose of this layer is to work with data in very short periods of time.

- **Tradeoff.** The persistence and availability of historical data is not managed in this layer. Therefore, the equipment used must be more specialised in terms of central processing unit (CPU) speed and random-access memory (RAM), leaving aside the issue of handling high volumes of storage. It is suggested to have in place a logical mechanism for recovery in the face of an imminent disruption of service in this layer.

- **Main features:**

- 2 rack servers in failover mode (active/passive) or cluster configuration:
- 512 Gb RAM.
- 2x processor 2.30 GHz (40 cores).
- 2 gigabit network cards (10 Gbps).
- Failover recovery system to prevent losing transactional information.
- Database manager oriented to high performance. It is recommended to use managers that operate on RAM to speed up I/O operations and failover/cluster configuration.

❖ **Static/final data (cluster).** The purpose of this layer is to allow the storage of historical information guaranteeing the availability of the data and the performance necessary for their consumption. Although this layer is not oriented to near real-time responses like the “**high performance data**” layer, it requires that the response times do not affect the systems/users that use the information. Therefore, the equipment used is oriented to deliver good hard disk I/O performance.

- **Tradeoff.** A larger number of nodes is required to maintain a cluster scheme and this is costly, however this will ensure the availability and efficient management of the information.

- **Main features:**

- 2 rack servers on cluster configuration.
- 128 Gb RAM.
- Solid state/SAN (capacity of at least 10 times the estimated data for the following year, considering the number of nodes in a cluster to reach the desired storage space. 10 TB equipment capacity recommended.
- 2 Gigabit network cards (10 Gbps).
- Database manager oriented to handling high volumes of data in cluster with high availability.
- Failover recovering system.
- Backup system to guarantee the recovery of information in the event of loss of information.

Storage layer:

This layer provides scalability in storage space in a simple way in case the computer equipment does not support hard disk growth.

➤ **Technology components:**

❖ **Storage Area Network (SAN).** This is a comprehensive storage network.

- **Tradeoff.** It is a complete architecture that groups the following elements: a high-speed fiber channel or iSCSI network, a dedicated interconnection equipment (switches, bridges etc.) and network storage elements (hard disks). Recommended for transactional data, as it requires lower I/O latency. However, the cost of this equipment is higher compared to other solutions.

- **Main features:**

- Storage capacity: at least 10 times the estimated data for the following 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.

Transactions manager layer:

This layer provides a simple integration of communication between applications, oriented to publish-subscribe schemes.

➤ **Technology components:**

❖ **Server pool.** A set of servers that provide the same services.

- **Tradeoff.** Despite the cost of having equipment with high processing or high storage capabilities and considering the complexity that the use of cluster schemes may involve, it must guarantee good performance and availability of the services provided by the CV to the issuer's banks.

- **Main features:**

- 2 rack servers:
 - 512 GB RAM.
 - 5 Tb hard disk drive (solid state/SAN).
 - 2x processor 2.30 GHz. (40 cores)
 - 2 gigabit network cards (10 Gbps) on failover schema.
 - Cluster schema.
 - 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.

Attached "known technology":

Infrastructure	
Operating System	CentOS, RHEL
Version Management	SVN, Gitlab
CI/CD Automation	Jenkins, Ansible
API specification	Open API specification

Application	
Frameworks	Java, Spring, Spring Boot, Netty
Transaction Manager	Kafka
In-Memory Cache (Dynamic/Fast database)	Redis
Cluster Management	Sentinel, Zookeeper

Database	
Static Database (SQL)	PostgreSQL
Static Database (NoSQL)	Cassandra

Security	
Security	HSM Safenet
Agents	FireEye, TrendMicro, CA UIM
API gateway	Zuul

Monitoring	
Monitoring	Kafka Manager, ElasticSearch, Kibana, Logstash, Beats, Elastaalert, Nagios, Flink, Spring Boot Admin.

Annex D: Cybersecurity in the API ecosystem

Due to the evolving cyber threat landscape, participants in API ecosystems must implement cybersecurity guidelines to protect customers' information and IT assets that store, process, and transport such information.

Ecosystems' stakeholders play a role and have responsibilities within the cybersecurity guidelines of the API ecosystem:

- *Central authority.* This is the entity in charge of the centralised infrastructure that provides authentication and payment initiation services. It defines the governance model for compliance with cybersecurity guidelines. It could be a central bank, other authority, or a private entity.
- *Financial institutions.* These are entities that hold money accounts on behalf of their customers, and which grant permission to parties to access their customer data. They can be banks or other financial entities.
- *Third parties.* These are entities that request permission to access or review customers' information from a financial institution in order to initiate or receive payments on behalf of their customers. They can be fintech companies, financial institutions, or big techs.

Cybersecurity governance

Governance involves establishing a decision-making authority and an accountability framework to address cybersecurity risks. Authorities in each jurisdiction could define a governance model that allows monitoring compliance with cybersecurity guidelines through assessment processes. These authorities could also establish a relationship between stakeholders. This would encourage stakeholders to comply with these guidelines. This function could be performed by a central bank, organisations, ministries, committees, companies, financial institutions etc.

Compliance with cybersecurity guidelines in an API ecosystem seeks to achieve the following objectives:

- improve confidence in payment systems managed and operated by central authorities, financial institutions, and third party participants;
- reduce risk of fraudulent transactions and to promote management of control gaps or deficiencies within organisations;
- improve risk management to promote the security and resilience of IT environments; and
- strengthen API ecosystems against cyber-attacks and allow for timely remediation plans in case of breaches or deficiencies.

The scope covered in these guidelines includes IT infrastructure, software and mobile applications installed in users' devices. These guidelines are based on the National Institute of Standards and Technology (NIST) cybersecurity framework,⁸ the Open Web Application Security Project Foundation (OWASP)⁹ and the Payment Card Industry (PCI) Mobile Payment Acceptance Security Guidelines.¹⁰

⁸ www.nist.gov/cyberframework/framework

⁹ owasp.org/www-project-api-security/

¹⁰ www.pcisecuritystandards.org/documents/Mobile_Payment_Acceptance_Security_Guidelines_for_Merchants_v1-1.pdf?agreement=true%26time=1483228800336

All guidelines in this document are established as suggestions. Topics in this document are addressed in a high-level context. The application of these guidelines is left to the discretion of each stakeholder.

Cybersecurity guidelines

1. Identifying assets and risks

1.1 Asset management

Technological asset inventory is populated through a process of discovery. This process, which may be manual or automated, involves obtaining information about the components that comprise the information systems within financial institutions, third parties and the central authority.

The use of automated tools for discovery, analysis and management of component inventories is generally a more effective and efficient means for maintaining component inventories. Nevertheless, even with automated inventory management tools, it may still be necessary to enter some component inventory data elements manually.

Tools that support inventory management are usually database-driven applications that track and manage information system components within a given environment. Once an inventory is established, automated tools are often used to detect the removal or addition of components. Some inventory management tools allow for expanding the monitoring of components through the use of built-in hooks in the Operating Systems (OS) or the installation of agents on each component. With this functionality, the inventory management system can monitor changes in the component's configuration and report the results to specified staff.

An inventory adds real value when each item in the inventory is associated with information that can be leveraged for determining approved configuration baselines, configuration change control/security impact analysis and for monitoring/reporting. Some data elements typically stored for each component in the inventory include, but are not limited to:

- Unique identifier and/or serial number.
- Type of component (e.g., server, desktop, application).
- Manufacturer/model information.
- Type of operating system and version/service pack.
- Presence of virtual machines.
- Application software version/license information.
- Physical location (e.g. building/room number).
- Logical location (e.g., IP address).
- Media Access Control (MAC) address.
- Owner.
- Operational status.
- Primary and secondary administrators.
- Primary user (if applicable).

Some additional data elements may also be recorded, such as:

- Status of the component (e.g., operational, maintenance, spare, disposed etc.)
- Relationships/dependencies to other components in the inventory.
- Identification of any Service level agreements (SLA) that apply to the component.
- Applicable common secure configurations.
- Security controls supported by this component.
- Identification of any incident logs regarding any of the components.

Including diagrams that reflect data flows among components is also suggested in order to improve troubleshooting and have a better understanding of the architecture and operational functions. The diagrams are useful to understand the relationships between the different IT infrastructure components and services and to support information when a cybersecurity incident occurs.

1.2 Risk assessment

Risk assessments address potential adverse impacts on organisational operations and assets, individuals and other entities arising from the operation itself and the use of information systems and information processed, stored and transmitted by those systems. Organisations conduct risk assessments to determine risks that are common to the organisation's core business processes, common infrastructure/support services, or information systems. Risk assessments can support a wide variety of risk-based decisions and activities.

Risk assessment is a process that includes:

- identifying vulnerabilities, threats, and risks that can cause any sort of damage to the organisation
- estimating the probability of risk materialisation
- defining mitigation priorities by risk severity and likelihood of occurrence
- determining risk tolerance.

There is a wide range of security practices and approaches that can be applied to risk assessment. The most popular is penetration testing.

1.2.1 Penetration tests

Penetration tests simulate an attack on the organisation's cybersecurity systems and applications using a wide range of manual techniques and automated tools. During this process, testers determine possible ways of exploiting vulnerabilities and estimate the potential damage they can cause. Pentests may also include vulnerability scanning. The main goal of pentesting is to determine and assess all cybersecurity threats and risks facing the organisation.

Organisational missions and business functions, supporting mission/business processes, information systems, threats and environments of operation tend to change over time. It is therefore suggested that financial institutions and third parties execute tests for the identification of vulnerabilities in both a static and dynamic source code. The organisation should test on every occasion when a new API version is released, and a third-party test is suggested every 3 years.

The frequency of penetration tests should be determined based on factors such as system criticality and system's exposure to cybersecurity risks. For systems that are directly accessible from the internet, a pentest is suggested at least once a year, whenever these systems undergo major changes or updates, and whenever new threats that may affect them are discovered. Stakeholders should consider the following types of pentests:

- White box. Full network and system information is shared with the tester, including network maps and credentials.
- Grey box. Only limited information is shared with the tester, such as credentials.
- Black box. No information is provided to the tester at all.

1.2.2 Vulnerability assessments

Vulnerability assessments are recommended based on publicly known information-security vulnerability and exposure sources such as the Common Vulnerabilities and Exposures (CVE) System¹¹ and/or the US National Vulnerability Database.¹²

It is suggested that both financial institutions and third parties have a workplan to resolve vulnerabilities by prioritising those with high-level and medium-level associated risks.

Threats should also be identified, assessed and documented. Internal and external threats need to be considered and a defined workplan setting out roles and responsibilities needs to be developed in order to implement corrective actions.

1.3 Business impact analysis

Stakeholders should execute and document a methodological approach for developing a business impact analysis (BIA). A BIA predicts the consequences of disruption to a business function and process and gathers information needed to develop recovery strategies.

Identifying critical operational processes should be the first step to take into consideration when executing a BIA. After that, identifying and classifying the impact of risks should be done according to the operational risk methodology. At this point, it is important to have identified the recovery time objective (RTO) and the recovery point objective (RPO). RTO refers to the time it takes for functional restoration of a business process, to a level of functionality similar to before the disruption. For stakeholders, an RTO close to zero would be the best, since a zero RTO would be almost impossible in the short term, but not in the long term. RPO defines the maximum acceptable data loss that a business process can stand to lose within individual applications before it is critically impacted. In other words, it is a data-loss metric expressed in time (e.g., minutes, hours, or days) directly related to applications. RPO is used to determine the point in time at which data needs to be recovered after a disruption, this is usually a matter of minutes or hours.

A BIA should identify critical human and material resources involved in the operation.

1.4 Providers and partners' risk management

There are many situations that can cause disruptions within providers and partners. To avoid these potential service disruptions, many organisations use supply chain risk management. This allows stakeholders and supply chain managers to recognise threats and determine a corrective or protective course of action. Implementing legal agreements with providers and partners is suggested so that they can meet cybersecurity standards. These legal agreements could be confirmed through audits or other types of assessments. Some certifications could be used as a reference for compliance.

¹¹ See cve.mitre.org.

¹² See www.nist.gov/programs-projects/national-vulnerability-database-nvd.

2. Protecting data and IT assets

2.1 Authentication and access control

When planning an access control system, access control policies and mechanisms should be considered. Access control policies are high-level requirements that specify how access is managed and who may access what information and under what circumstances. In general, access control mechanisms require security attributes to be maintained for users and resources. User security attributes can consist of categories such as user identifiers, groups and roles to which users belong. Alternatively, they can include security labels reflecting the level of trust bestowed on the user. Resource attributes can take on a variety of forms. For example, they can consist of sensitivity labels, types or access control lists. When determining a user's ability to perform operations on a resource, access control mechanisms compare the user's security attributes to those of the resource.

It is suggested that financial institutions, third parties and central authorities have defined controls and procedures in place to create, modify or delete users and profiles, and assign privileges and permissions to them. Assigning a specific group to verify, modify and authorise access privileges, and to modify these users and profiles, is recommended. It is important to have a segregation of duties between the different groups of users, mostly between those in charge of user management and the others.

Either for operational facilities or for data centres, stakeholders should restrict access to designated operational areas where critical activities are executed. They must develop, approve and maintain a list of individuals with authorised access to the facility where the system resides, issue authorisation credentials for facility access, review the access list and remove individuals from the facility access list when access is no longer required.

Electronic controls to access restricted areas are recommended. Physical access authorisations apply to employees and visitors. Individuals with permanent physical access authorisation credentials are not considered visitors. Authorisation credentials include ID badges, identification cards, and smart cards. Stakeholders determine the strength of authorisation credentials according to applicable laws, executive orders, directives, regulations, policies, standards and guidelines.

Each organisation should implement control access systems with roles and responsibilities to request, review and authorise access. All access should include information such as reason, detailed activities, period and personnel information. Physical access authorisations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

2.1.1 Implementing authentication for users and passwords in the back office

With respect to back-office operations, it is suggested that stakeholders employ passwords, physical authenticators or biometrics to authenticate users or, in the case of multi-factor authentication, some combination thereof. When using passwords, it is strongly suggested that stakeholders have a password policy that considers complexity requirements as well as their validity and updating periods.

In addition, use of the following rules is recommended as guidance for the creation of strong passwords:

- Complexity rule. Complexity makes a password strong. It ensures unpredictability and resistance to brute-force attacks. Complexity is a combination of password length and diversity of content.
- Uniqueness rule. This means that every password is exclusive to a particular system and distinct as compared to all other passwords. For instance, never reuse the same password, especially among different systems. Uniqueness also refers to uniqueness over time. A good practice is to update passwords every three to six months.

- Secrecy rule. Always maintain the secrecy and confidentiality of a password to ensure its integrity as an authentication resource. Do not share passwords with others. Use one password while setting-up and configuring a system and then change the password when the setup is completed.

Stakeholders may require the re-authentication of individuals in certain situations including when roles, authenticators or credentials change, when the system's security categories are adjusted and when the execution of privileged functions occurs.

Whether for backoffice authentication or mobile application authentication, the recommendation is to implement mutual transport layer security (TLS) authentication so that the client is assured that it is being connected to the right server and not to a malicious fake.

Using OAuth 2.0¹³ for access delegation in API ecosystem is also recommended, as it has become the *de facto* standard for mobile application authentication. In an OAuth-based authorisation, a user requests access to resources under the control of a resource owner. To access these resources, the user is provided with a different set of credentials. This can be used when accessing APIs from multiple endpoints including mobile apps, desktops etc.

There are multiple grant types in OAuth 2.0. A grant type defines how a user can obtain an authorisation grant from a resource owner to access a resource on his/her behalf. While using OAuth 2.0 to access APIs from a native mobile application, an authorisation code grant type is recommended, along with a proof key for code exchange (PKCE).¹⁴

The PKCE protects the native apps from a code interception attack. This is defined in *Request for comments (RFC) 7636* as a technique to mitigate the threat of a code interception attack in a mobile environment.

A code interception attack is where a malicious user intercepts the authorisation code returned from the authorisation endpoint and uses it to obtain the access token.

2.1.2 Implementing authentication on mobile applications (endpoints)

Use of current and strong multi-factor authentication methods are highly recommended. Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as something you know (e.g., a personal identification number (PIN)), something you have (e.g., a short message service (SMS) text or a one-time password (OTP)), or something you are (e.g., a biometric).

Stakeholders may require re-authentication of individuals in certain situations, including when changes in profile information and security options are involved.

If the use of passwords is considered, stakeholders are encouraged to follow the strong password creation rules explained in the backoffice section.

2.1.3 API gateway

API gateways might be considered. These management tools sit between clients and the back-office services (between PSTs and CV's internet-based layer). It is common for API gateways to handle common tasks that are used across a system of API services, such as user authentication, rate limiting and statistics.

At its most basic, an API service accepts a remote request and returns a response. API gateways are useful when you host large-scale APIs. They offer the following benefits:

¹³ See oauth.net/2/

¹⁴ See Prabath Siriwardena, "API Security: OAuth 2.0 and Beyond", Apress, 2019 (doi.org/10.1007/978-1-4842-2050-4_2).

- They protect your APIs from overuse and abuse, so you use an authentication service and rate limiting.
- They allow you to understand how users use your APIs (analytics and monitoring tools).
- They allow you to connect to a billing system if you have monetised APIs.

2.2 Protected communication network

We suggest stakeholders ensure they have a protected communication network. Network segmentation is recommended in order to limit the level of access to sensitive information that individuals have and to separate the development and testing environments from the production environment. Stakeholders should establish access control policies for each environment such as white lists to establish a connection to an environment and to implement controls to request, review and authorise access. All connections from the back office to the internet should be justified.

Authentication, authorisation and accounting (AAA) management for users should be implemented by stakeholders. The AAA features allow stakeholders to verify the identity of, grant access to, and track the actions of users including:

- authentication, including login and password dialog, challenge and response, messaging support and encryption depending on the security protocol that stakeholders select; and
- authorisation providing access control.

Accounting provides the method for collecting information, logging the information locally, and sending the information to the AAA server for billing, auditing and reporting.

Secure communication protocols should be implemented to provide the appropriate confidentiality, authentication and content-integrity protection. Depending on the access, protocols such as HTTPS, FTPS, SCP, WebDAV, SSH2, radmin, RDP etc. should be implemented.

2.3 Protected computer system

Since it is the first code that is executed by a main CPU, the basic input/output system (BIOS) is a critical security component of a computer system. The BIOS system is a potentially attractive target for attack. Malicious code running at the BIOS level could have control over a computer system. It could be used to compromise any components that are loaded later in the boot process. It is thus important that stakeholders secure the BIOS with a password as a minimum and restrict any loading from external devices. It is suggested that all unused physical ports are disabled, and those that are not, should be justified.

2.4 Software restrictions

Any service, application or software not needed in the IT infrastructure should be restricted. Stakeholders must review what software programme(s) a particular application is often bundled with, and determine if an application is known to pose a substantial security risk.

2.5 Processes to protect information

It is suggested that configuration change management should be implemented in order to determine, document, review, implement, monitor, coordinate and provide oversight for configuration change control activities. Roles and responsibilities must be defined to request and approve changes in the IT infrastructure and software. Any requested change must contain justifications, impacts and results.

Backups of information should be conducted, maintained and tested by stakeholders. Establishing and documenting what type of information should be backed up, and from which system(s), and determining how long this information will be stored.

Secure procedures to erase information from any component should also be implemented in order to dispose of hardware in such a way that information cannot be retrieved from them.

2.6 The role of human resources

It is strongly suggested that cybersecurity be included in human resources practices, including:

- Personnel screening. Checking the background of a potential hire such as education, experience, certification/license, criminal record and financial status.
- Raising periodic cybersecurity awareness and education among the organisation's personnel.
- Deprovisioning. Deleting all user credentials and any other access the user had.

2.7 Software Development Life Cycle (SDLC)

When developing, stakeholders should consider a software development life cycle (SDLC) methodology with clearly defined processes in which confidentiality, integrity and accountability are considered. The following stages must be kept in mind:

- requirements
- design
- development
- test
- deploy
- change management

Mobile applications should be submitted to an evaluation process in order to get the central authority's approval for their development. This process should be considered after every software release.

It is important that stakeholders consider industry-accepted secure coding techniques (e.g. OWASP Top 10 and SANS 25)¹⁵ and OWASP best practices.

2.7.1 Third-party provision

It is suggested that an agreement is put in place with software providers to complete a verification process on delivered items. This verification might include an integrity assessment for each file delivered from the software provider to the stakeholder. The primary goal of this task would be to monitor every possible modification on the stakeholder's side, while bearing in mind that some files would change because of local configurations.

2.8 Audit logs

It is recommended that log information be included, for both applications and infrastructure, when designing every component. Including consideration of the following types of information as a minimum:

- timestamps
- users
- users and systems' activities
- IP addresses (origin and destination)

¹⁵ See <https://www.sans.org/top25-software-errors/>.

Logs should not contain sensitive information and this information must be stored for a determined period of time in case logs need to be audited for any reason. In the event that a log includes sensitive information, it is recommended to keep it encrypted based on the encryption methods described in the data security section.

2.9 Data security

Data at rest are data that are not actively moving from one component to another or from network to network. Data protection at rest aims to secure inactive data stored on any component or network. While data at rest are sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion. The risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state.

Data in transit, or data in motion, is data actively moving from one location to another. Data protection in transit is the protection of this data while it is traveling from one network to another or while being transferred between components.

Data can be exposed to risks both in transit and at rest and requires protection in both states. There are multiple different approaches to protect data in transit and at rest. Encryption plays a major role in data protection, both in transit and at rest. For protecting data in transit, stakeholders can choose to encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc.) to protect the contents of data in transit. Stakeholders should be aware of considering only communication protocols that guarantee the integrity and confidentiality of information. Implementing mechanisms to check integrity such as digital signatures issued by a certificate authority must also be considered. For protecting data at rest, stakeholders can simply encrypt sensitive information prior to storing it and/or choose to encrypt the storage component itself. While at rest, all data related to digital signatures must be secured and stored in HSM infrastructure.

2.9.1 Cryptography requirements

JavaScript Object Notation (JSON) is a notation that uses printable characters and nowadays is deployed for storing and exchanging data, and it is heavily used for data exchange in APIs. JSON has already become the de facto message exchange format for APIs. Thus, understanding security in combination with JSON plays a key role in securing APIs, it is appropriate to mention as well that JavaScript Object Notation (JSON) has these main advantages:

- Lightweight and more compact style than XML.
- Uses less data overall improving the parsing speed.
- Simplifies the code by increasing its readability.

It is also necessary to define how to secure JSON messages at the message level.

Confidentiality is fulfilled under encryption schemes. The JSON Web Encryption (JWE) described in *RFC 7516* can be used for this purpose. Data integrity and non-repudiation can be achieved by using signature schemes. The JSON Web Signature (JWS) described in *RFC 7515* shows how to reach this goal.

To transport data between stakeholders' parties in a cryptographically safe manner, the use of the JSON Web Token (JWT) is recommended. The privileges of JSON Web Tokens can be used to propagate user identity as part of the authentication process between an identity provider (central authority) and a third-party. JWT is an internet engineering task force (IETF) standard defined in *RFC 7519*.

In addition to the JSON format, we must also consider secure algorithms and its security parameters.¹⁶

If digital certificates are used, a public key infrastructure (PKI) should be considered to guarantee the authenticity of such certificates and the uniqueness of the public keys involved.

2.9.2 Data security in mobile applications (endpoints)

Regarding mobile applications, it is suggested that stakeholders adopt a principle of informed consent. Users should clearly understand the authorisation they are being asked to provide, including:

- who they are providing authorisation to;
- what they are providing authorization for;
- how long the authorisation will last;
- the permissions mapped to one or more API calls; and
- what information the third-party is storing.

It is suggested that stakeholders disable keyboard caching for any potentially sensitive field. Keyboard caching increases risk of exposure of sensitive information. Sensitive information that is input for the application may be saved in the device and accessed later. All sensitive information shown through the user interface on mobile applications should be masked in order not to expose it. Screenshots should be restricted.

It is suggested that disabling USB debugging and using code obfuscation should be enforced by stakeholders, making it more difficult for an attacker to modify or reverse engineer the software by reducing the attack surface.

It is further recommended that stakeholders provide secure means for keeping mobile applications updated through patch management – as well as other means – to prevent compromising the mobile device due to vulnerable software. Controls should include, but are not limited to:

- notifying new updates to the user; and
- validating versions continuously to ensure that the latest is installed.

Controls should be implemented to prevent the escalation of privileges on the device (e.g., root or super admin). Bypassing permissions can increase the number of possible attack vectors. The device should therefore be monitored for activities that defeat operating system security controls – e.g., jailbreaking or rooting – and, when detected, the device should be quarantined by a solution that disables the mobile application. Offline jailbreak and root detection and auto quarantine are key since some attackers may attempt to put the device into an offline state to further circumvent detection. It is also suggested that stakeholders restrict installation on unauthorised platforms.

3. Detecting anomalies

3.1 Anomalies and events

It is recommended that all changes in the IT infrastructure and software are detected by stakeholders. Automated tools or systems that allow monitoring of all changes should be utilised, allowing for a timely response in case of atypical, anomalous or unauthorised changes. It is suggested that stakeholders define actions in case of atypical, anomalous or unauthorised changes. Roles and responsibilities should be

¹⁶ See Arjen K. Lenstra and Eric R. Verheul, "Selecting Cryptographic Key Sizes" (Journal of Cryptology, vol. 14, pp. 255-293, 2001, (<https://www.keylength.com/>))

See NIST Special Publication 800-131A

defined when monitoring changes and a follow-up of atypical, anomalous or unauthorised changes should be established. Procedures to communicate atypical, anomalous or unauthorised changes, including those by the security officer, should be documented. All actions to be taken in case of atypical, anomalous or unauthorised changes should be documented as well.

3.2 Continuous monitoring

Stakeholders should monitor communication networks at all times in order to detect potential cybersecurity events. The use of anti-malware software is recommended as well as setting up daily automatic scans with an update at least every week. All corrective actions should be taken in case of anomalies' detection.

Live logs should be the primary input in order to have an effective and active monitoring response when events are detected. Events can occur in a single component or have a correlation between components.

3.3 Documented detection processes

Roles and responsibilities for detection should be clearly defined to ensure accountability. All information related to an event detection should be communicated accordingly to a defined procedure. Stakeholders should keep in mind that detection processes have to be tested at regular intervals and the result of these drills will serve as an input to continuously improve detection processes.

4. Incident response

An analysis should be conducted to ensure effective response and support recovery activities. It must include at least the following actions:

- notifications from detection systems must be investigated;
- the impact of an incident must be understood by the business area to raise awareness;
- forensics must be performed for the external area;
- a process must be established to receive, analyse, and respond to the vulnerabilities disclosed from internal and external sources (e.g., internal testing, security bulletins or security researchers);
- newly identified vulnerabilities must be mitigated or documented as accepted risks; and
- to mitigate vulnerabilities, a change control process needs to be implemented including, as a minimum, the stages of testing, authorisation, implementation and roll back.

It is suggested that stakeholders consider the following stages with defined roles and responsibilities in addition to the listed scenarios (playbooks). All communication plans with both internal and external parties should be considered.

Stages:

- prepare
- detect
- analyze
- contain
- eradicate
- recover
- post-incident handling

Scenarios:

- malware outbreak (malware is running rampant on the network)
- phishing (someone is trying to take advantage of users)
- data theft (data is being extracted by external or internal parties)
- denial of service (system performance or availability is compromised)
- unauthorised access (user gains access to network illegally)
- elevation of privilege (credentials of system users have been compromised)
- improper usage (abuse of network's permissions and tools)

As a procedure, drill exercises should be executed at least once a year to identify any situation that may affect the participants' ability to maintain acceptable levels of services, critical functions and activities. Stakeholders should evaluate the results of the exercises and make improvements in the process according to the deviations and lessons learned.

5. Recovering from incidents

5.1 Business continuity strategies

The development of a business continuity policy with strategies and procedures to be followed is strongly recommended so that, if a contingency scenario identified in the risk analysis materialises, the operation could continue at a minimum acceptable level.

The business continuity plan should establish that, at least for the following scenarios, continuity strategies related to the operation are fully implemented:

- inability to use primary operating facilities due to natural, social, political or infrastructure causes;
- inability of the personnel responsible for the operation to regularly attend the primary and secondary operating facilities due to various situations (for example, health alert due to pandemic threat);
- impact on computing infrastructure;
- impact on telecommunications infrastructure;
- impact on software supporting operations; and
- impact on the central authority's infrastructure.

The personnel responsible for the continuity strategies should be trained to execute them by themselves, without depending on suppliers or third-party partners.

It is suggested that stakeholders identify and prioritise strategies associated with contingency scenarios according to the level of risk.

Roles and responsibilities for business continuity strategies should be established, including those regarding the approval, implementation, execution, testing and evaluation of the business continuity plan.

Documented procedures for reviewing, updating and communicating continuity strategies to stakeholders should be considered.

We suggest executing drills every at regular intervals (at least once a year) in such a way that the continuity strategy can be updated and reviewed based on the lessons learned.

It is important to consider that in any business continuity plan stakeholders should know which data are business-critical and protect it. This "golden copy" of data is a simple, cost-effective way of complementing a traditional disaster recovery plan. The "golden copy" must be available at any time and geographically distributed. Synchronous replications of the "golden copy" should be considered.

5.2 Communication plan

Stakeholders must consider a public relations plan so that the reputational damage caused by an incident can be repaired, providing timely information on the causes and magnitude of the damage, the actions implemented and the preventive measures to avoid damage.

Recovery activities should be communicated to the internal and external stakeholders as well as to the executive and management teams.

5.3 Sharing information

Stakeholders should consider communicating with outside parties in the event of an incident. This may include contacting law enforcement agencies, fielding media inquiries and seeking external expertise as appropriate.

They should also discuss incidents with other involved parties such as internet service providers (ISPs), vendors of vulnerable software and other incident response teams.

Stakeholders may proactively share relevant incident indicator information to improve the detection and analysis of incidents. The incident response team should discuss information sharing with the organisation's public affairs office, legal department and management before an incident occurs to establish policies and procedures regarding information sharing.

Annex E: Industry outreach learnings

In line with the early work done by the CGIDE TTF, there was agreement on the need to deepen the analysis to identify challenges, standards or potential innovations in the open finance ecosystem from the stakeholder perspective. To achieve this goal, the CGIDE TTF held several industry outreach sessions. The intention was to hold sessions dedicated to all actors involved in the system: developers, third parties and financial institutions.

Stakeholders analysed

Figure 6

Developers	Financial institutions	Third parties
Generate the infrastructure to make payments through an API.	The operators of users' records, in addition to their expertise in the payment system.	The ones who interact with the user and connect with both developers and financial institutions.

Firstly, developers are usually the entities which generate the infrastructure to make payments through an API. For this reason, CGIDE TTF held a meeting with representatives of UPI-NPCI which involved a presentation titled *Digital retail payments as a public good for the world*. CGIDE TTF also held a meeting with the Gates Foundation, who gave a presentation about the Mojaloop system and the open-source identity platform (MOSIP). In both cases, developers and CGIDE TTF members discussed developments relating to centralised infrastructure and the challenges that the CV may have.

Secondly, from a third-party point of view, the CGIDE TTF met with Google to discuss *Google Pay – open banking recommendations*; and with Amazon to discuss Amazon's general views on APIs were discussed. Third parties are the ones who have interactions with users. Their perspective is essential for the implementation and acceptance of APIs in the payment system.

Finally, financial institutions are the operators of user's records, in addition to their expertise in the payment system. They are a key player in the development of the API infrastructure for payment initiation. In order to gain insight on the perspectives of these participants, CGIDE TTF met with Citi in a presentation titled *Citi connect API: the invisible bank for digital treasury*; and also, with BBVA who presented their *Perspective on open finance*.

It is worth highlighting that all three roles described above are not completely separate. That is, a financial institution can also play the role of a developer or third-party and these stakeholders, in turn, can also act as a different stakeholder. The objective of this annex is to address the key aspects identified by the industry about the use of APIs for the open finance ecosystem. The topic is addressed in two sections. First, the general perspective for the ecosystem. Second, the individual perspective of each stakeholder: developers, financial institutions and third-party stakeholders. This last part serves to deepen insights gained as a result of outreach to the industry. In addition, public versions of the presentations are available on the following website [to be included].

General perspective

As a result of analysing the sessions, CGIDE TTF identified five issues that institutions are constantly facing: (i) adaptability to the technology-changing environment; (ii) use of APIs as publicly available club good; (iii) user experience (iv) risk management and liability; and (v) regulation. Each issue is described below, along with the main perspectives of each stakeholder.

Adaptability

Due to rapid innovation in technology and the entry of new players in the financial system, adaptation is emerging as a key issue in the payments ecosystem. Companies are increasingly looking for payment solutions that enable them to manage their processes digitally and reach underserved or completely underserved sectors. As a result, there is a widespread trend exhibited by all participants to implement schemes that are sufficiently scalable to keep up with changing digital transformational trends. For example, one such trend is that faster and smaller payments are increasingly being demanded by consumers. Developers must implement technologies that support these types of payments and their continuous increase; financial institutions must keep up with the evolving needs of users and provide sufficient continuity; and third-party participants face increasing competition in the ecosystem. Another example is that payments are not carried out separately but are increasingly interconnected and form ecosystems and networks.

As part of this adaptability process, participants agree that flexibility is a key challenge to address, mainly in the instances in which users can use an API infrastructure. For example, flexibility in the payment models that are designed is necessary, and flexibility to ensure accessibility and ease for users in operating such a scheme when instructing transactions is also required. In this way, the stakeholders described challenges of implementation on multiple schemes and use cases.

From the financial institution's perspective, challenges of a smooth transition and innovation requirements to offer flexibility and adaptation were identified. They have also faced the challenge of digitising their infrastructure and seeking to avoid importing problems from legacy systems. Therefore, although they offer wider experience and greater trust from users than the new competitors, they also accept soaring costs to a greater extent, and higher risks. From the perspective of the third-party participants, there is increasing competition for innovation and efficiency to gain the trust and commitment of customers. From the developers' perspective, the technology infrastructure provided to users must be sufficiently capable to meet every customer's requirements, as well as guaranteeing users' information and security.

API as a publicly available club good

From the sessions with the industry, it is implied a broad agreement among stakeholders that the implementation of APIs may contribute to the improvement of the financial system and potentially represents a greater welfare for all participants, once relevant and properly addressed risks it may represent.¹⁷ In this sense, even when there is a tendency to affirm that APIs contribute to society, it does not necessarily imply that APIs should be called a "public good", instead they have characteristics that are more associated with the definition of a club good.

On the one hand, public goods are non-excludable and non-rival products. This means that no one can be prevented from consuming them (non-exclusivity) and that individuals can use them without reducing their availability to other individuals (non-rivalry). Under certain circumstances, these goods are usually provided by a public entity or government. Examples of public goods are clean air, knowledge, national defense, public lighting among others. In that sense, with the centralised scheme proposed above, the API infrastructure for payment initiation does not match the definition of a public good because exclusion does exist.

On the other hand, club goods are excludable but non-rival goods. Thus, individuals can be prevented from consuming them, but their consumption does not reduce their availability to other individuals. Club goods are also sometimes called artificially scarce resources and are usually supplied by private entities or natural monopolies. Examples of club goods are cable television services, cinemas,

¹⁷ For more details of involved risks related to APIs, please consult: Bank for International Settlements. (2019, November). Report on open banking and application programming interfaces; <https://www.bis.org/bcbs/publ/d486.pdf>

wireless internet, toll roads etc. The API infrastructure for payment initiation coincides with the exclusivity of the good, but the difference is it is desirable to make it publicly available so that anyone who wants to be part of the ecosystem can do so.

Types of goods Figure 7

	Excludable	Non-excludable
Rival	Private goods (food, clothing)	Common goods (Public Parks)
Non-rival	Club goods (cinemas, streaming service)	Public goods (national defence)

For this reason, CGIDE TTF has termed APIs as publicly available club goods. There is also a widespread intention to promote financial inclusion and serve sectors of the population without access to banking services. Considering this intent, there is a common concern about how to ensure accessibility of services without diminishing security and user authentication. In other words, participants want a robust and secure infrastructure, for which it is necessary to correctly identify users. One way to authenticate securely is the use of biometrics. However, some users do not have access to devices with biometric detection and it does not always guarantee secure authentication. Secure authentication can also be achieved without using biometrics such as by combining multiple security factors depending on the context of the authentication. For example, impossible to clone possession factors that requires confirmation of the real owner’s physical presence to grant access. Even so, the question remains and there is no precise solution for it.

User experience

One of the elements that all players are inclined to develop is an improved user experience. If the user experience (UX) is satisfactory, users will enjoy the service offered by the companies, as well as each of the possible extensions and updates that may come later. On the other hand, when UX is not pleasant, it will create a seamless and ineffective perspective that will make users not want to use it and not return to it, and they will also tell their friends and family about it, with network effects. This, related to technological trends in which interconnected networks and complete ecosystems have been formed. As mentioned above, these networks have changed the user experience and made it smoother.

Thus, all participants have strived to implement real-time transactions through a simplified and easy-to-implement user experience for businesses. In this way, they not only offer better services and have more customers, but also contribute to welfare by facilitating the use of financial services and making them very easy for customers to use. The developers have made sure that the interface is sufficiently accessible to third-parties and physical customers such that use cases are very intuitive. Third parties must be able to capture and serve customers' needs and banks must offer sufficient alternatives for transactions. Banks are constantly competing to create the best experience possible for users and it is therefore essential for them to offer the best user experience available.

There are differences of perspective in the standardisation of processes and technology. Standardisation allows the creation of standards or norms that define the common characteristics with which products must comply and which are respected in different parts of the world. This facilitates the creation of ecosystems, the extension of networks, interoperability and accessibility to APIs. However, it makes it difficult for participants to differentiate their products and can hamper innovation and internal change. CGIDE TTF has observed this concern on the part of some financial institutions seeking to have a distinctive role in the payment ecosystem. This is because, with standardisation, they must adhere to standards and norms for compatibility with the rest of the system. It is worth mentioning that having one API, but each stakeholder promoting a completely different data model will not solve the acceptance and

interoperability issues. It is worth noting that maintaining a reduced number of variations (simplification) is a goal for the API.

Risk management and liability






There is a broad consensus on the importance of the security of customer information and everyone agrees with developing and implementing systems with that in mind. The differences lie in what type of system to implement and what technology best secures everyone's information. Although there are technological and implementation differences, it is very important to highlight that there is an industry view in favor of implementing layered systems to guarantee the transmission and safeguarding of information.

Likewise, traceability has become fundamental for tracking of risks and implementing of accountabilities. To minimise the likelihood of fraud or transaction failures, all participants have invested in implementing the necessary traceability mechanisms. An example of this is the constant use of two or more factors of authentication, encrypted and secured in a relevant way. This establishes trust relationships intrinsic to the procedure and interactions within the ecosystems. Thus, involved participants have also explored the possibility of establishing other types of relationships with thirds, e.g., contractual relationships. Another example is the challenge that participants face in the identification of end users within an enterprise. This is because participants must find a way that does not rely on physical signatures, but a digital alternative could help them to correctly identify users. Regulation

All participants consider regulations required for the implementation of the APIs. However, some participants feel that heavy regulation could lead to disadvantages or barriers for certain stakeholders. Regulation includes operating rules, participation rules, as well as brand guidelines and operating circulars. From the developers' perspective, there is a broad initiative to maintain a relationship with the authorities in order to seek to foster a competitive environment and better development of the API ecosystem. As far as third-party participants are concerned, there is agreement that inter-connections can be facilitated when countries have similar regulatory regimes and made more difficult when there is a great variation in the characteristics of regulatory regimes in different countries.

Finally, there are polarised views among financial institutions. At the beginning of the direct data and open finance revolution, some financial institutions felt compelled to distribute their transactional data. This perspective changed as participants tracked the role, they can play in the API ecosystem to initiate payments. On one hand, there is a view that clear rules outlining entitlement, rights and obligations promote a level playing field for all who wish to participate. On the other hand, there is also the view that strong regulation can hurt traditional financial institutions, if they are not able to adapt to new ecosystems standards. It is necessary to emphasise that clear rules help all users to know the responsibilities of each participant and, above all, to know to whom liability shift corresponds in different circumstances.

In this way, the sessions that the CGIDE TTF has had with the industry have been very valuable and have aided understanding of the API ecosystem for payment initiation. Many elements were considered and raised in this analysis and there is a table summarising the perspectives of participants.

Aspect	Developers	Financial institutions	Third parties
<p>Adaptation</p> 	<p>From the developers' perspective, the technology infrastructure provided to users must be sufficiently capable to meet every customer's request.</p>	<p>Traditional financial institutions face the challenge of having to upgrade and digitise their infrastructure.</p>	<p>From the point of view of third parties there is increasing competition in terms of innovation and efficiency in order to gain the trust and commitment of customers.</p>
<p>APIs as publicly available club goods</p> 	<p>While there is a consensus among all stakeholders that APIs contribute to the general welfare, they cannot be classified as public goods. Therefore, this text proposes the categorisation of APIs for payment initiation as a publicly available club good.</p>		
<p>User experience</p> 	<p>Developers have gone to great lengths to make the user experience simplified so that it increases user engagement and makes it easier to perceive multiple use cases.</p>	<p>Different views regarding standardisation of processes and technology vs. innovations that differentiate products. But they converge in that the experience must be fast and simplified.</p>	<p>This is one of the factors that third parties compete for, as a better user experience helps improve user confidence and financial viability levels. In addition, a standardised connection makes it easier for third-parties to provide accessibility for users.</p>
<p>Risk management</p> 	<p>Layered ecosystems that enable intrinsic risk and liability management, along with efficient use of two or more authentication factors.</p>	<p>General agreement on the importance of protecting user information</p>	<p>Ensuring that user information and accounting record operators are secure, along with the handling of authentication factors.</p>
<p>Regulation</p> 	<p>Common agreement to have a close relationship to establish clear rules together with direct association with the central bank and/or entity authorised by the central bank to collaborate.</p>	<p>Opinions are divided as there is a perception that strong regulation may lead to disadvantages for financial institutions compared to other unregulated companies. But there is consensus in favour of the establishment of clear rules.</p>	<p>Third parties agree with the establishment of a level playing field in the payments ecosystem as they compete more on user experience, trust and other services.</p>

Stakeholder perspective

Following this general analysis of the industry sessions, CGIDE TTF presents the perspective of each stakeholder below. First, from the developers' perspective, CGIDE TTF delves more deeply into the technological aspects and the developed structure. Second, from the perspective of the financial institutions, CGIDE TTF analyses the differences of opinion which became apparent and the possible roles that these institutions will play in the payment ecosystem. Finally, CGIDE TTF sets out at the perspective of third-party participants who implement APIs to initiate payments directly with users.

Developers

Among the developers, there was a concurrence of opinion regarding modular design. Modular design is based on the placement of functional and universal modules, which together form more substantial structures that can be assembled in alternative ways or arrangements. Modules allow developers to transform and adapt their structure to modern technological developments or to overcome problems. In addition, they can address risk management, ecosystem responsibilities, scalability and interoperability.

Also, in respect to scalability, it was observed that identical modular design fosters standardisation and innovation for multiplayer solutions. Innovation represents a fundamental challenge for any company. Aware that it is a substantial competitive advantage in a more globalised and competitive environment, all of these organisations are trying to innovate in alternative ways. Areas for innovation include manufacturing products, redefining processes or promoting organisational models that have a direct impact on the company's performance, whether it be increased turnover or improved efficiency.

As a result of high volume transaction requirements and large-scale adoption, the implementation of new paradigms of architectural design are widely considered relevant to the achievement of performance and user experience objectives. Design considerations include:

- distributed data transmission for load-balancing and high-availability purposes;
- NoSQL distributed databases for speeding up data access and response time on information repositories;
- in-memory key-value data store for in-transit transactions and non-final data; and
- idempotency and immutability.

Regarding security and risk management, CGIDE TTF found that there is a trend towards a model with multiple layers of protection. As in the payment initiation schemes discussed in this text, developers have acknowledged the need to find a way to ensure that payment information reaches the accounting operators without necessarily giving all stakeholders access to that information. Thus, a layered system results in the creation of a series of private key files designed to protect and share the information. In addition, this results in an anti-fraud scheme which is intrinsic to the developed ecosystem. That is to say, payment information will not reach the accounting registry operator if it has not already passed all the tests and signatures that those involved in the previous steps have reviewed.

This model is efficient together with a multi-factor authentication system. It is possible to make payments so that the bank and user information is secure. The case of modular open-source identity platform (MOSIP) presented by the Gates Foundation is very interesting because it is a robust, scalable and inclusive foundational identity platform. MOSIP supports governments and other user organisations to implement a foundational digital identity system cost-effectively. Nations can independently use MOSIP to build their identity systems. Being modular in its architecture, MOSIP provides flexibility to nations in how they implement and configure their systems, and helps avoid vendor lock-in. This equivalent system makes it possible to find faults or fraud that may be generated in a transaction. Still, MOSIP documentation is very extensive and is under constant development along with other technological alternatives for authentication. It is worth mentioning that the use of biometrics is only one way to perform secure

authentications and that there may be strong regulation of the use and handling of user information. Nevertheless, institutions have also explored the idea of generating contractual relationships with third-party initiators. The idea is to establish sufficient relationships of trust to generate what they dub "the bus of trust" or what CGIDE TTF refers to as "the onion".

Finally, it is widely recognised that partnerships and collaborations are vital to the implementation of APIs. From the creation of aliases and third-party relationships to the establishment of rules, together with direct partnerships with the central bank and/or an entity authorised by the central bank to collaborate.

Financial institutions

From the perspective of financial institutions, it is often believed that broad reach and expertise in the payments system produces competitive advantages for financial institutions. However, these participants expressed concerns about the costs of digitising internal legacy systems to open up to APIs, being able to innovate fast enough compared to other non-regulated players, moving from big to small and turning industries into intact ecosystems.

Unlike developers, in financial institutions there are divided opinions on the usefulness and benefits of standardization. Unlike developers, financial institutions are divided on the usefulness and benefits of standardization. Indeed, without standardization, financial institutions could develop meaningful user experiences and compete with third parties that are often able to offer differential user experiences by leveraging the greater amount of user data to which they have access. In the long run, this can greatly improve many aspects of open banking, from financial inclusion to transparency of the criteria and data used to deliver better services to end users. With respect to regulatory issues, there is a fear that regulation will be excessively rigid and harm the development of APIs for these players. This is because financial institutions are regulated in multiple ways that third-party participants and unknown players in the payment ecosystem are not. Even so, they agree that it is necessary to establish explicit rules for each type of participant. In addition to ensuring that payment users are equally protected regardless of which party they interact with to initiate payments or which stakeholder they seek recourse from if there is a problem with a payment. They also agree that the implementation of secure systems for users is fundamental, although there are differences of opinion about the technology and implementation mechanisms.

Ultimately, CGIDE TTF notes that financial institutions have envisioned two ways in which they can be part of the APIs. The first of these is to join an ecosystem developed by a third party. The second is based on developing their ecosystem. By being participants in an ecosystem developed by third parties they have the advantage of having even more reach but they would have to adapt to the mechanisms and technology that have already been implemented. On the other hand, developing their ecosystem can be more complicated since it requires the creation of standards and relationships with others involved when the institution already has its own standards and relationships. When adopting either of these two ways of participating in the ecosystem, there is the possibility of the financial institutions becoming invisible to users. This is as a result of enabling customers to carry out transactions in a simpler, faster and barrier-free way. In this role, financial institutions act only in the back office. Even so, users must have all the necessary information to recognise who is responsible for the management of their resources and which institution to turn to in case of a problem.

Third parties for payment initiation

Third-party participants, within the outlined API ecosystem, are typically those that retain a direct relationship with the customer and face the most competition in the user experience arena. Accordingly, it is reasonable for them to be business-focused. That is to say, these participants focus on the business model and the specific or multiple services they can offer. Payment initiators can be viewed either as simply

a payment initiator or as a merchant offering variety in payments. To achieve this, third parties must ensure security, traceability, flexibility and continuity of service to users.

In this regard, one of the most daunting challenges they face is user trust. To gain the trust of consumers, it is essential to offer them different payment options so that they can select the one they trust the most or the one that best suits their needs. The shopping experience must be more secure, varied, and with more guarantees, if possible, than in a physical store. Of course, third-party initiators must ensure KYC procedures and the linking of the user's accounting records with the operators.

Accordingly, it is easy for third-party payment initiators to connect to a standardised and centralised scheme instead of having to establish multiple lines of connection to different established umbrellas. In addition, these participants should be alert for fraudulent activities when offering the option to personalise an account with aliases or other elements. For these reasons, authentication and the use of multiple authentication factors and information sources – such as linking to bank accounts – helps to correctly identify both the commerce user and the physical user. Another challenge they experience is to offer an inclusive ecosystem to develop the digital payments ecosystem. Third-party payment initiators frequently address this by creating innovative products and services and creating value propositions for merchants.

Annex: Definitions

- **user:** a person interested in using financial services such as payments through a payment app.
- **payment app:** third-party app enabled to offer payment initiation services User. We refer to this participant as payment initiation application, third-party application, and PST in the text.
- **payment app server:** backing server or middleware providing functionality to Payment app.
- **CV auth-app:** app provided by a central validator to perform secure management of authentication factors for User.
- **issuer bank:** financial institution providing financial services, such as payments, to User.
- **cipher block chaining:** it is a block cipher mode in which each ciphertext block is dependent on all plaintext blocks processed up to that point, it is considered safer than previous modes.
- **cluster:** It is a group of inter-connected computers or hosts that work together to support applications and middleware
- **NoSQL:** It means non-SQL and refers to a non-relational database that stores and accesses data using key-values, storing items/objects individually with a unique key associated.
- **middleware:** software that has an intermediary function between at least two applications.