BIS Innovation Hub

May 2026

Project Aperta

Enabling cross-border interconnectivity through open finance interoperability

Conclusions from a collaboration with central banks, regulators, international organisations and academia

Project Aperta

Enabling cross-border interconnectivity through open finance interoperability

Conclusions from a collaboration with Hong Kong Monetary Authority (HKMA), Banco Central do Brasil (BCB), Central Bank of the United Arab Emirates (CBUAE), and the Financial Conduct Authority of the United Kingdom (FCA) – including Global Legal Entity Identifier Foundation (GLEIF), the International Chamber of Commerce Digital Standards Initiative (ICC DSI), and the Hong Kong University Standard Chartered Foundation FinTech Academy.

This publication is available at bis.org

Publication date: May 2026

Contents

Glossary, acronyms and initialisms

Aggregator	A TPP that mediates connectivity between multiple parties
AML	Anti-money laundering
API	Application programming interface
Bank	A licensed financial institution that holds customer payment accounts
BIS	Bank for International Settlements
BISIH	Bank for International Settlements Innovation Hub
CA	Certificate authority, a trusted organisation that issues and signs digital certificates to confirm identity and help secure online communications
CFT	Combating the financing of terrorism
Ecosystem, network	Interconnected participants enabling a shared act, ie data-sharing
FAPI	Financial-grade API, an API security model from the OpenID Foundation
FI	Financial institution (also includes banks)
Framework	The governing set of rules, standards and procedures for an ecosystem
GLEIF	Global Legal Entity Identifier Foundation
HKU	University of Hong Kong
ICC	International Chamber of Commerce
ICC DSI	International Chamber of Commerce Digital Standards Initiative
ISO 20022	An international standard for high-value payment messages
Key	A cryptographic key is used by an algorithm to encrypt and decrypt data
KYC; KYB	Know-your-customer; know-your-business (identity verification)
LC	Letter of credit guaranteeing payment to a seller in trade finance
LEI	Legal Entity Identifier, based on the ISO 17442 standard, applicable globally
LFI	Licensed financial institution
MLETR	Model Law on Electronic Transferable Records
NCA	National competent authority, a national-level regulatory body
OAuth 2.0	Open Authorisation 2, a delegated access standard
OIDC	OpenID Connect, an identity layer built on top of OAuth 2.0
OpenAPI	The OpenAPI specifications provide a formal standard for describing APIs
Open finance framework	The rules, standards, governance arrangements, technical specifications and operating models that define how open finance works in a jurisdiction or market
Participant	A catch-all for an entity such as an aggregator, bank/FI or third party
PKI	Public key infrastructure, which manages digital certificates and public keys
Postman	An API platform for developers to design, build, test and collaborate on APIs
Scheme	Governance framework coordinating rules, participants and operations
SME	Small and medium-sized enterprise
TPP	Third-party provider
Trust architecture	The technical and operational systems that enforce the trust framework
Trust framework	The rules, standards and governance that allow participants in an open finance network to share data securely and trust the identities, permissions and security of one another
UNCITRAL	United Nations Commission on International Trade Law

Executive summary

The impetus behind Project Aperta

In today's global economy, people, goods and services move across borders relatively easily, but cross-border finance remains a challenge.

A key reason is the difficulty of sharing financial data across jurisdictions, including information about identity, accounts and credit histories. Differences in technical standards and legal frameworks make it hard for individuals and business to exchange this information consistently.

To address these challenges in a domestic context, standardised technical interfaces (so called application programming interfaces, or APIs[1]) were developed to support these data flows through open banking and open finance[2] frameworks. These frameworks which allow individuals and businesses to consent to sharing their financial data or to initiate services such as payments through trusted third parties via standardised APIs, now exist in around 95 jurisdictions.[3] According to the Bank for International Settlements (BIS) paper *"Opening doors to open finance: evidence from the international experience"* (2026), these frameworks have delivered clear benefits in individual countries, including greater competition, innovation and financial inclusion.[4]

Despite the benefits that domestic open finance frameworks bring, moving financial data and using APIs across borders remains difficult. Technical standards, infrastructure, regulation and governance differ between these open finance frameworks. While a small number of bilateral solutions exist to connect frameworks, they are rare, complex to establish and difficult to scale. As a result, individuals and businesses frequently encounter repeated manual checks, duplicated document submissions and lengthy onboarding processes. This limits their access to overseas accounts, credit and trade finance.

The next evolution of open finance could come from bridging domestic open finance networks, enabling interconnectivity across borders.[5] This is what Project Aperta is about: as an experimental proof of concept, Project Aperta explores the feasibility and potential benefits of cross-border open finance interoperability.

Indeed, Project Aperta demonstrates how cross-border interconnectivity of open finance networks can support objectives that matter to central banks. These include overall safer and more resilient cross-border financial services, greater efficiency in payment systems and enhanced financial stability through broader access to financial services, especially for small and medium-sized enterprises (SMEs). The proof of concept illustrates how technology could help regulated financial institutions serve SMEs engaged in cross-border activity more effectively, while remaining anchored in domestic governance, consent and supervisory arrangements.

Project Aperta is designed as an experimental initiative, with SME banking and trade finance serving as concrete test cases for the prototype. Its relevance for central banks and other public authorities lies in testing whether domestic open finance arrangements can interoperate internationally without requiring each jurisdiction to redesign its own framework, thereby informing future policy choices on interoperability, trust, resilience, governance and access.

Project Aperta's novelty

Project Aperta, launched by the BIS, is a proof of concept "network of networks" for open finance: rather than requiring countries to negotiate separate bilateral linkages, Aperta tests a neutral multilateral interoperability layer that can securely connect existing domestic open finance networks and enable the cross-border exchange of financial data and the cross-border initiation of payments. The experiment specifically explored whether registered participants in one jurisdiction could be discovered and trusted across borders, whether data using technical standards from one domestic framework could be translated into another in real time, and whether these functions could be combined in practical cross-border use cases without altering domestic rules, consent processes or security controls. The project, run by the BIS Innovation Hub (BISIH) Hong Kong Centre, drew on insights and lessons from other BISIH initiatives, such as Project Nexus. That project addressed cross-border interoperability for domestic instant payment systems and faced similar challenges.[6]

Project Aperta is the first public authority initiative to prototype and test the real-time international portability of financial and payment data between different domestic open finance networks.

Aperta is a cross-border project with participants from around the world. The BISIH collaborated with Hong Kong Monetary Authority (HKMA), Central Bank of Brazil (BCB), Central Bank of the United Arab Emirates (CBUAE) and the Financial Conduct Authority of the United Kingdom (FCA) to evaluate the prototype technical design against their domestic open finance frameworks and the potential benefits this could provide. The Global Legal Entity Identifier Foundation (GLEIF), the International Chamber of Commerce Digital Standards Initiative (ICC DSI) and the University of Hong Kong-Standard Chartered Foundation FinTech Academy (HKU) also participated to explore how open finance can be used for novel use cases beyond its current scope, such as trade finance. Collectively, these eight participants formed the project steering committee, which is responsible for setting Project Aperta's strategic direction and making decisions by consensus (see Box 1). Project Aperta also had observing members who were invited quarterly to share project updates and offer advice. These include eight central banks and authorities, seven standard setters and industry bodies, and three international organisations.

The project first explored different ways of connecting domestic open finance networks, considering approaches that varied in how technical responsibilities and coordination would be shared across participants and jurisdictions. Rather than assuming a single solution from the outset, the project experimented through different technical avenues to understand what could realistically work across different domestic environments.

The experimentation examined whether financial institutions in different jurisdictions could securely find and recognise trusted counterparties, exchange information across different systems and standards, and support practical cross-border end user journeys without requiring jurisdictions to redesign their domestic frameworks. Through this process, the project identified approaches that reduced complexity for participants while preserving domestic rules and arrangements. These findings are important because they demonstrate that cross-border interoperability may be achievable through practical adaptation of existing infrastructure rather than requiring domestic systems to be entirely redesigned.

How the prototype works

In simple terms, the Aperta prototype acts as a secure, real-time "translator and directory" for financial data and instructions across existing domestic open finance networks, effectively building a "network of networks".

When a domestic regulatory authority joins the Aperta prototype, it securely shares details of its registered participants, such as banks, fintechs and other third-party providers (TPPs), including aggregators that mediate connections between TPPs and multiple banks through a single technical endpoint. This allows participants in different jurisdictions to find trusted counterparties, verify identities using digital certificates and exchange data safely.

8 project participants

18 observing members (central banks, standard setters and industry bodies)

21 testing organisations

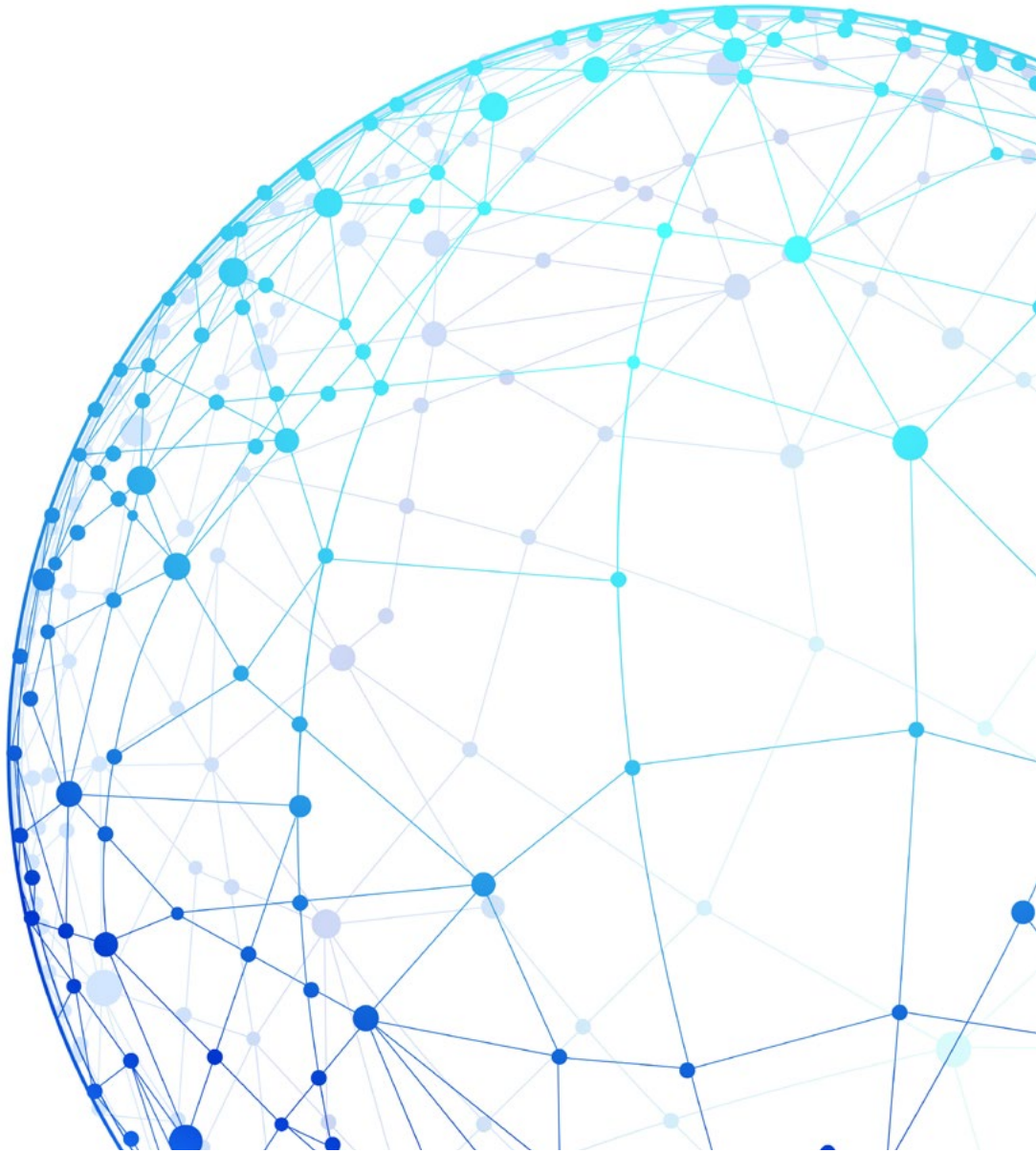
The prototype translates and routes data between jurisdictions in real time by converting financial information and payment instructions from the source jurisdiction's format into the destination format. This can include account balances, transaction histories and instructions to initiate payments using existing domestic technical standards. It not only enables access to data but also supports the execution of transactions, such as making a payment on a bank account in the destination jurisdiction. All data remain protected through strong encryption and user consent remains anchored in familiar domestic processes. End users and TPPs interact only with their domestic networks; Aperta works invisibly in the background.

Use cases tested and benefits demonstrated

The prototype was tested across five countries – Brazil, Hong Kong SAR, the United Arab Emirates, the United Kingdom and India[7] – with participation from all eight steering committee members, as well as private sector test participants comprising six commercial banks and seven third parties. It focused on two practical, SME-focused use cases:

1. **Cross-border business account opening:** A hypothetical SME can securely share its business and owners' profiles along with rich transactional data – including revenue streams, trading history and relationships with counterparties or overseas subsidiaries – directly from its home bank. These data enable the receiving institution to pre-populate application forms and gain a clear, real-time view of the business's legitimacy, activity levels and financial behaviour, thereby significantly increasing confidence and speeding up the overseas account opening process.
2. **Trade finance and payments:** Aperta extends open finance into trade finance, a novel application. The full transaction lifecycle – from contract and letter of credit (LC) issuance through shipping document exchange to final payment execution – is supported by structured digital data flows instead of paper forms. Using Aperta prototype APIs that align with existing technical standards and principles in trade finance, the prototype demonstrates how open finance networks can serve as trusted infrastructure to overcome fragmented, paper-based processes and encourage API-driven processes/data exchange by default.

The project leveraged available domestic open finance and international trade-related API standards to enable the testing of the two use cases. These demonstrations show how Aperta's prototype can potentially reduce duplication, shorten onboarding and processing times, lower compliance costs, build greater institutional confidence and make cross-border financial services more accessible and affordable for SMEs.



Key findings and takeaways

- The project explored and assessed different architectural models (centralised versus federated), each with distinct implications for complexity, governance, and implementation effort. A pragmatic, centralised architectural model was selected for the prototype because it is faster to implement and does not require changes to domestic technical standards or infrastructure. It also enables rapid learning to inform a potential future federated approach, which would require changes across the five jurisdictions tested.
- Testing the two use cases confirmed the technical feasibility of the centralised architecture, demonstrating that domestic open finance networks can be successfully linked on a multilateral basis.
- The project highlighted the power of collaboration among regulators, central banks and technical specialists, delivering a prototype that demonstrates that interoperability requires close alignment across jurisdictions on data standards, translation logic, trade finance data and a common mechanism to identifying and trusting network participants.
- While the prototype was technically successful, real-world challenges would need to be overcome. Deployment would require targeted legal and regulatory changes. Aperta's modular, use case-agnostic design provides a solid, technologically viable foundation for further development of cross-border data-sharing initiatives.

Relevance to central banks and next steps

Project Aperta demonstrates that secure cross-border data portability is feasible within the existing banking ecosystem. By showing what is technically achievable, the project enables policymakers to assess the benefits of interconnecting domestic open finance networks and to refine the architecture for potential real-world implementation. It also serves as a form of regulatory testbed, helping to identify potential legal, governance and technical adjustments needed to support interoperability and secure data-sharing.

Looking ahead, central banks and regulatory authorities could build on these findings to explore practical deployment pathways. One approach could involve small clusters of jurisdictions with advanced open finance ecosystems piloting use cases aligned with central bank mandates, particularly those aimed at improving payment system efficiency and supporting financial stability. Such enhanced tests could generate the operational, legal, regulatory and governance insights needed to inform broader adoption and, over time, support the development of scalable cross-border digital financial infrastructure.

Report structure

This report provides background on the concept of open finance, its benefits, and the main outputs of the project. It explains how Aperta works to enable cross-border data portability through open finance, outlines the prototype's technology components and design considerations, and summarises the key findings as well as possible directions for future development.

All architectural documents, translation protocols, trust and identity system designs, reference code and data models have been developed as shared goods for the central banking community via BIS Open Tech, available for other jurisdictions and network operators to use as a foundation for learning and further development.

Central banks, regulators, governments and network operators interested in the blueprints, prototype assets or further collaboration are invited to contact the Project Aperta team at: hongkong.centre@bisih.org

Box 1: The vision behind Project Aperta

Project Aperta takes its name from the Latin for "open". The vision of the project is to explore a global "network of networks" to enable open cross-border data interoperability between regulated and market domestic ecosystems.

Early discussions identified cross-border SME banking and trade finance digitisation as key innovation opportunities to pursue, whereby Aperta's open approach could encourage data exchange by default, as an alternative to privately negotiated data exchange. This led to engagement with the Global Legal Entity Identifier Foundation, the International Chamber of Commerce Digital Standards Initiative and the University of Hong Kong-Standard Chartered Foundation FinTech Academy.

Further consultative discussion developed high-level principles for the project, balancing the desire for innovation with the pragmatic need to generate interest among potential stakeholders, while minimising the impact (and barriers to adoption) for existing ecosystems.

The overarching principle was to limit the impact on domestic open finance infrastructures, standards or regulations while creating a prototype. Several solution options were considered, and the project selected the "centralised aggregator of third-party providers and trust frameworks" approach as it prioritised compatibility with existing domestic regimes and immediate deployment. This choice defined the prototype's operating boundaries.

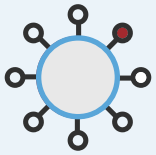
A second principle was a strong desire to create a public good, using open source code and standards where possible and providing a blueprint – including requirements, design, architecture and source code – to foster collaboration and invite both industry and community feedback.

In addition to the prototype implemented and tested applying the centralised approach, the project delivers the high-level design for a potential evolution to a federated solution. This represents an alternative design option, but would require a different architectural commitment and would impose domestic change on local jurisdictions. This federated option would not have met the pragmatic constraints of Project Aperta's prototype phase and would take longer to negotiate and adopt. These approaches are discussed in Section 3.2.

The following report should be read with this in mind: Project Aperta demonstrates that regulated domestic ecosystems can interoperate without structural modification to their underlying trust frameworks, in response to the constraints that were accepted from the outset.

1. The benefits of linking open finance networks

1.1 Key takeaways

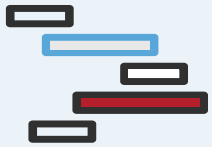


Open finance provides the necessary foundations for cross-border use.

By enabling connectivity, data harmonisation, standardised integration and trusted participation, open finance addresses many challenges of cross-border interaction. It also helps individuals manage their finances seamlessly in a globalised world, simplifying international money movement through synchronised local settlements.

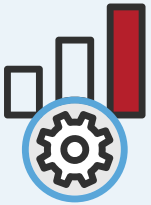
Building upon domestic open finance simplifies cross-border adoption.

Using established domestic infrastructure and common technologies such as application programming interfaces (APIs) reduces barriers to adoption for jurisdictions, building on both participant and user familiarity with open finance interaction.



Multilateral open finance could enhance global trade.

Open finance can serve as a framework with the potential to make trade networks more efficient and easier to operate and connect across borders through trust and data portability.



Open finance could enable inclusive SME and trade finance.

Open finance is geared towards inclusivity for underserved groups by providing a cost-effective platform to scale innovation. Open finance expansion offers strong opportunities in SME and trade finance.[8]

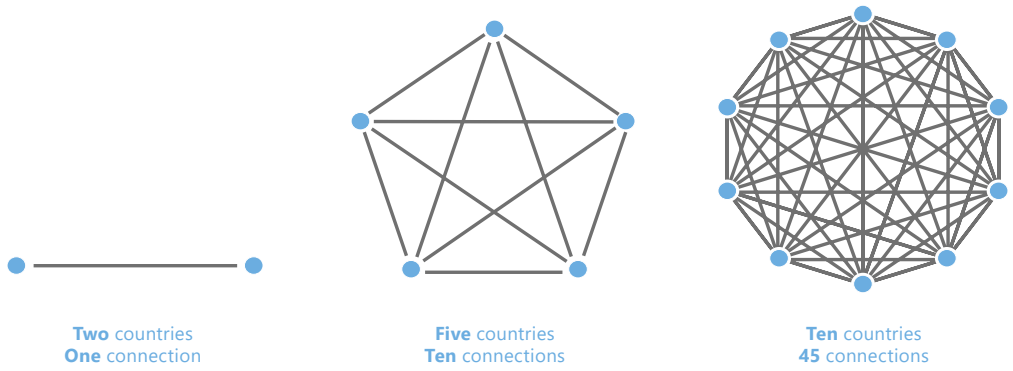
1.2 The challenges of operating across borders

People and goods regularly flow across borders. However, the underlying data and payments that enable this movement do not always flow as seamlessly, as they are subject to regulations designed and enforced at a local level. This creates friction for both individuals and businesses. For example, migrants with credit history in their home country often need to rebuild it from scratch when they arrive elsewhere.[9] Internationally expanding SMEs and multinational businesses face similar barriers, needing to open bank accounts in multiple countries, each bringing additional cost, complexity, currency risk and administrative burden. In addition, businesses face high costs when making cross-border payments, for example when paying invoices abroad in different currencies. For both individuals and businesses, accessing basic financial services becomes difficult due to the lack of a recognised identity, transaction history or trading footprint in the new market.

The establishment of cross-border interconnectivity faces two major challenges: trust and data interoperability. This applies both between counterparties and to the technical infrastructure that underpins financial data portability and includes concerns around security, provenance and portability. Cross-border data portability is complicated by differences in data standards and formats. As a result, moving customer, transaction and logistics data often requires costly manual mapping and translation.

To address some of these challenges, countries often establish trade corridors through bilateral agreements that facilitate the exchange of trade and company data, complementing existing global registries and bureaus, which are often costly and rely on historical data. While effective at a small scale, this approach becomes increasingly complex as the network expands (see Figure 1). Each new country would need to establish individual relationships with existing participants, requiring separate legal negotiation and technical integration. As a result, the number of connections grows faster than the number of countries involved, creating significant operational overhead and barriers to entry.

Figure 1: Bilateral relationships grow faster than the number of countries



This complexity of bilateral relationships is compounded by evolving global trade patterns. International supply chains are becoming more fragmented, driven in part by nearshoring and friendshoring strategies aimed at reducing geopolitical risk.[10] As noted by the United Nations Conference on Trade and Development (UNCTAD), while such diversification "can strengthen resilience and thus stabilise trade, it may also introduce inefficiencies…"[11] These complexities exist at a national level but fall disproportionately on SMEs. SMEs often lack the resources and expertise required to navigate fragmented regulatory environments, placing them at a competitive disadvantage. Although they account for around 90% of companies and more than half of global employment, they remain underserved and face limited access to affordable credit, trade finance and payment mechanisms.[12]

Without effective cross-border data portability, financial institutions (FIs) struggle to deliver even basic services, including customer verification, overseas account opening, credit provision, trade finance and foreign

exchange payments. In practice, SMEs are required to repeatedly submit information through fragmented and manual processes that often rely on PDFs, emails and duplicative data entry for each new foreign FI.

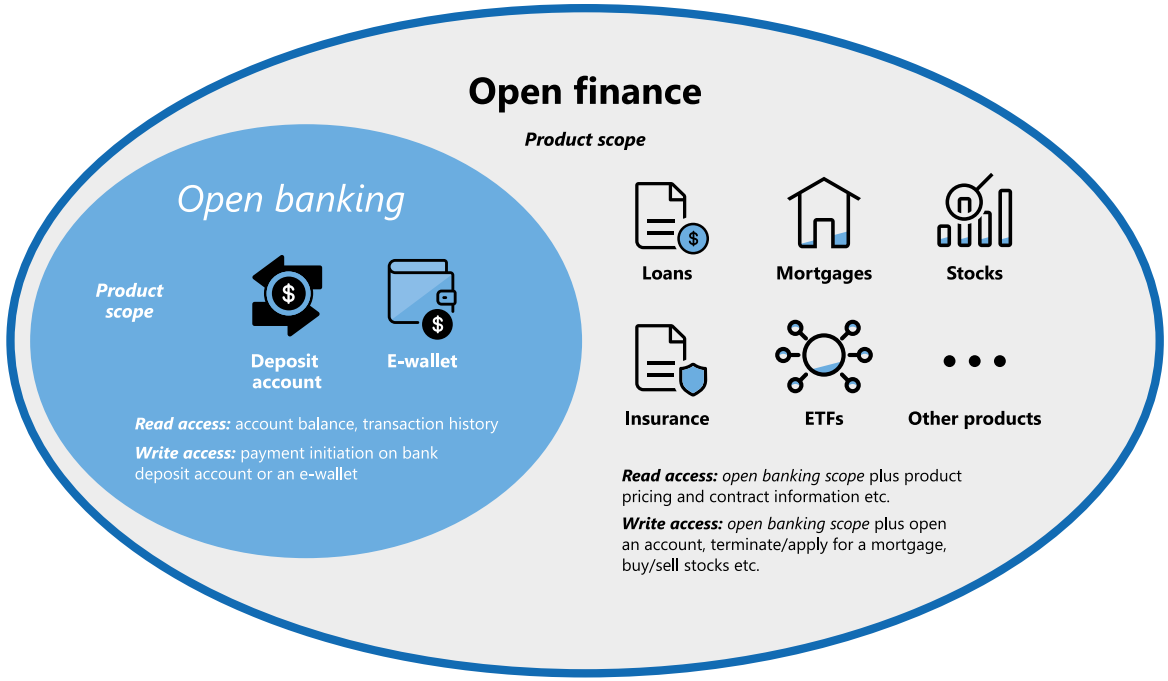
Limited visibility of an SME's track record across jurisdictions further increases perceived risk for FIs, which treat each new cross-border relationship as high-risk and labour intensive, making it uneconomical to serve many smaller businesses. For SMEs, this manifests as weeks-long onboarding, additional collateral requirements and rejected applications, even when their domestic data would clearly demonstrate strong cash flow, reliable repayment behaviour and counterparties if they could be shared in a standardised, machine-readable way.[13]

1.3 The relevance of open finance

An open finance framework that supports secure, consent-based data portability across borders directly addresses these pain points and represents an overlooked opportunity for central banks, which often consider open finance benefits to be domestic, not international. Open finance relies on a means of establishing trust between multiple parties in an ecosystem and uses legal and technical standards to facilitate interoperability, addressing many of the issues present in operating within a network and across borders (see Figure 2). By connecting open finance trust frameworks, building on international standards and linking domestic third-party providers (TPPs), it becomes possible to make cross-border data migration feel almost as smooth and efficient as a domestic open finance transaction (see Figure 3).

Open banking and open finance have demonstrated that standardised, API-based data-sharing ("read access") and initiation of a transaction such as a payment ("write access") can lower barriers to entry and support greater competition in financial services.[14] By allowing customers to authorise banks to share account and payment data with TPPs, open banking has expanded access to credit, enabled alternative payment solutions and fostered a more contestable market structure.[15] In the United Kingdom, open banking now supports 145 TPPs and underpins an ecosystem estimated at around GBP 4 billion, catalysing new provider types such as API aggregators that mediate connections between banks and third parties.[16]

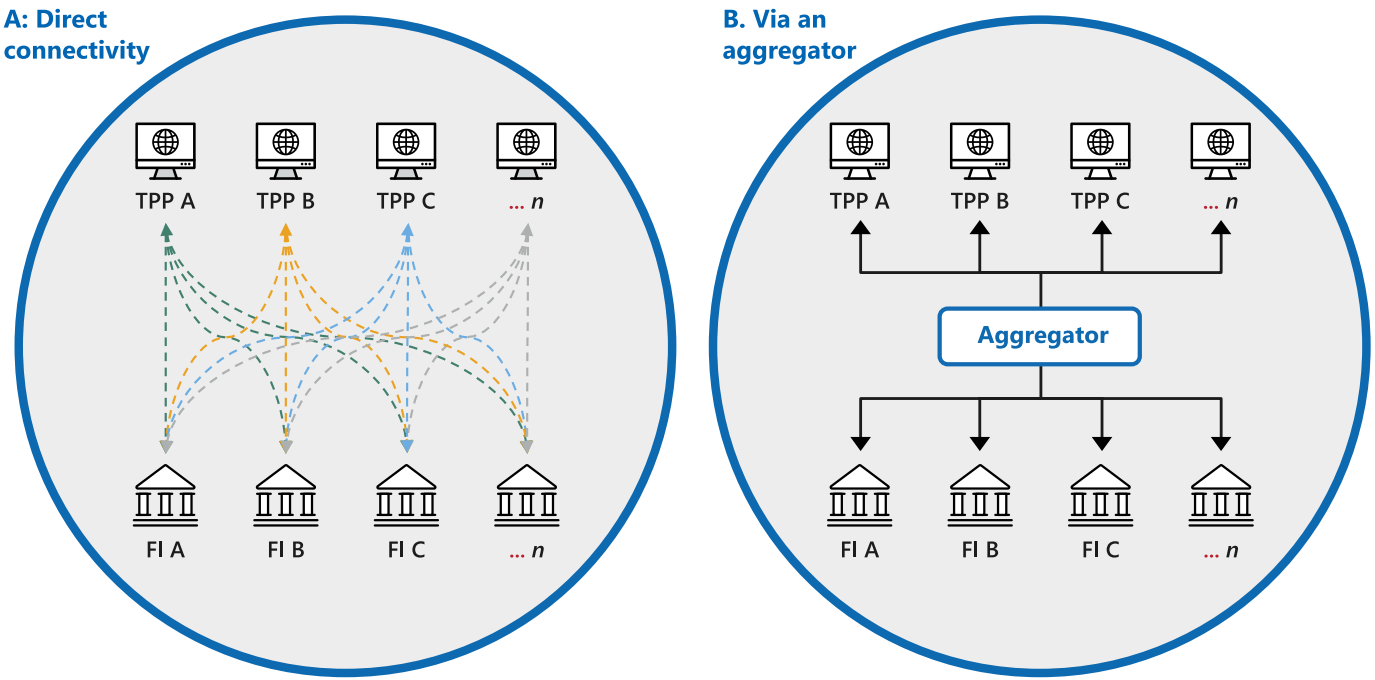
Figure 2: The scope of open banking and open finance



Open banking empowers customers to authorise banking institutions to share their personal and transaction history data and payment account information with third parties via application APIs.

Open finance covers a broader range of financial products, such as loans, mortgages and insurance.

Figure 3: The role of aggregators in open banking and open finance



An **open finance network** contains many **third-party providers (TPPs)**, who – with their customers' consent – need to connect to many **financial institutions (FIs)** to obtain their customers' financial data, typically via APIs.

A. Direct connectivity
One solution is for the TPP to establish **direct connectivity** with each financial institution. This model works but creates many-to-many complexity (a Cartesian join) with potentially hundreds of API-based connections.

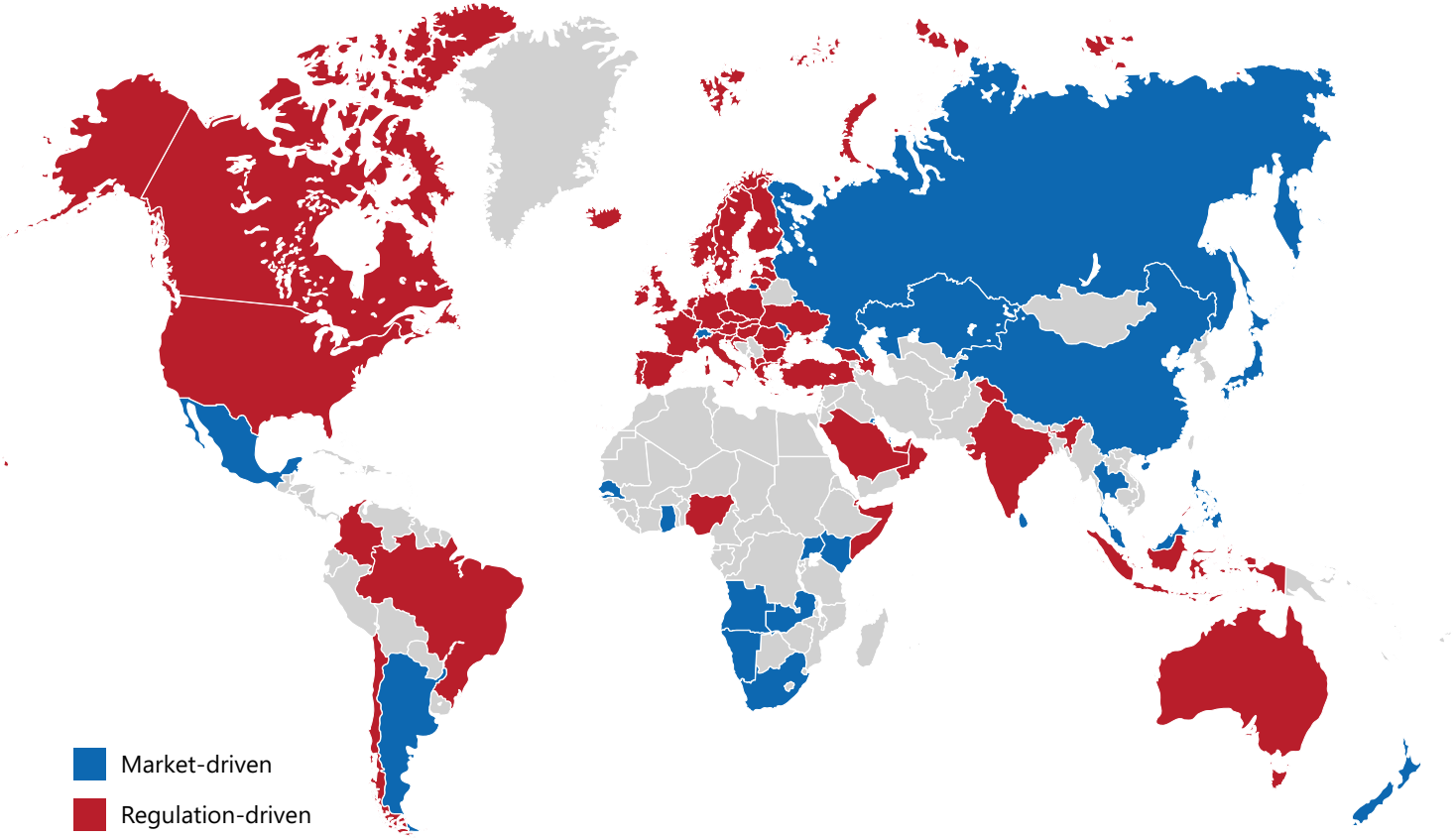
B. Via an aggregator
Many open finance networks contain TPPs that operate as **aggregators**. An aggregator sits as an intermediary between the TPPs and financial institutions, who each only need to connect directly to it. Once the third-party provider or financial institution is connected, all other connected parties are accessible.
Both approaches often coexist within open finance networks, giving a TPP the choice of whether or not to use an aggregator to connect to financial institutions.

For policymakers, open banking and open finance ecosystems are governed by rule-based frameworks and technical standards that confer trust on participating TPPs and reduce market fragmentation.[17] Membership in the ecosystem requires compliance with common data, security and operational requirements. Once a provider is connected, other members are able to trust that provider and share data or initiate payments with confidence, as well as scale innovation across multiple institutions.

Jurisdictional approaches to open finance

From a policy perspective, a key decision is how to implement open banking and open finance frameworks. Implementation ranges from regulation-driven mandates to facilitative or market-driven approaches (see Figure 4). The United States has historically relied largely on market-led data-sharing arrangements between FIs and third parties, although regulatory developments are increasingly shaping this landscape.[18] International experience suggests that regulation-led approaches with standardised APIs can support faster and more coordinated adoption, particularly where competition, innovation and financial inclusion are policy objectives.[19] For example, Brazil and India have combined open finance regulatory frameworks with broader digital financial infrastructure initiatives. In these jurisdictions, instant payment networks such as Brazil's Pix and India's Unified Payments Interface (UPI) have expanded digital payments and generated transaction data that can support financial services innovation and inclusion.[20] Pix processed more than 7 billion transactions in Brazil in December 2025 and was used by around 175 million consumers and over 22 million companies.[21]

Figure 4: The global extent of open banking and open finance



The use of this map does not constitute, and should not be construed as constituting, an expression of a position by the BIS regarding the legal status or sovereignty of any territory or its authorities, the delimitation of international frontiers and boundaries and/or the name and designation of any territory, city or area.

Note that the overview does not cover all known open finance frameworks, and classifications may change over time. Source: CCAF (2024).

Open finance is evolving to include integration with other sectors. Australia's Consumer Data Right is a multi-sector data-sharing framework, with banking one of the first sectors to implement it.[22] The United Kingdom is progressing open banking and accelerating open finance and, through the Data (Use and Access) Act 2025, extending into smart data and interoperability between different sectors such as property, energy and retail.[23]

From a cross-border perspective, various jurisdictions are exploring bilateral cross-border data-sharing opportunities, such as the Hong Kong Monetary Authority (HKMA) and the Financial Services Regulatory Authority (FSRA) of the Abu Dhabi Global Market (ADGM) signed a memorandum of understanding to deepen partnership on cross-border trade-related data exchange and business collaboration.[24]

Project Aperta seeks to go further, to remove the need for bilateral agreements (or connections) by providing interoperability between existing infrastructure, data and frameworks in order to enable trust between any jurisdiction (see Figure 5). In Project Aperta's prototype, the focus is on the existing open finance networks and infrastructure in the jurisdictions included in this project, including India.

Figure 5: Jurisdictions within scope for Aperta's prototype

	Country	Approach	Scope	Regulating authority	Standard setter; Coordinator	Type of infrastructure	Architecture
	**Brazil**	Mandated, standardised APIs	Open finance, payment initiation	Central Bank of Brazil (BCB)	Open Finance Brazil Association	Market built and run	Centralised, via Open Finance Trust Framework
	**Hong Kong SAR**	Collaborative, standardised APIs	Open finance, payment initiation	Hong Kong Monetary Authority (HKMA)	Hong Kong Association of Banks (HKAB)	Market built and run	Bank-implemented, HKMA-guided and facilitated
	**United Arab Emirates**	Mandated, standardised APIs	Open finance, payment initiation	Central Bank of the UAE (CBUAE)	CBUAE, coordinated by Nebras Open Finance	CBUAE built and run	Centralised, via CBUAE trust framework
	**United Kingdom**	Mandated, standardised APIs	Open banking (account information, payment initiation)	Financial Conduct Authority (FCA) and Competition and Markets Authority (CMA)	Open Banking Limited (OBL)	OBL built and run	Centralised trust and governance framework operated by OBL
	**India**	Standardised APIs	Open finance	Reserve Bank of India (RBI): Securities and Exchange Board of India	RBI, coordinated by Sahamati Account Aggregator (AA) scheme	Market built and run	Centralised using central registry

1.4 Opportunities from open finance interoperability

Open finance is increasingly seen as a platform for both domestic and international economic growth. Often starting with a focus on retail consumers, interest rapidly moves to SMEs and business-to-business services as a standardised API interface lowers innovation costs and makes it economical to serve SMEs. The United Kingdom's Financial Conduct Authority (FCA) notes how "reducing operational costs and enhancing consumer experience, particularly for SMEs and merchants" is a clear benefit.[25]

The FCA also notes the role that open finance has, beyond domestic efficiency gains, in unlocking export-led growth and innovation.[26] This aligns with World Economic Forum (WEF) research into global value chains, which notes that "competitive advantage now depends not on end-to-end control, but on orchestrating value, trust and data across networks far beyond direct ownership".[27]

International open finance interoperability would enable an SME to provide real-time access to foreign financial data or payment service providers, across accounts, lenders, accounting software and tax services, supporting digitisation and automation

in trade finance. Open finance has a powerful opportunity to transform cross-border APIs that exchange financial data and payment instructions from a hidden barrier into a driver of SME growth, enabling SMEs to operate efficiently across a wider range of regional hubs.[28]

1.5 How Project Aperta's open finance "network of networks" benefits cross-border trade

This intersection of domestic open finance trust infrastructure, SME needs and the increasing complexity of trade value chains is the focus of Project Aperta. Project Aperta's prototype demonstrates the technical feasibility of using open finance as a trusted conduit for cross-border data-sharing via APIs. Importantly, its application to trade finance is novel within the open finance space, extending the use of open finance infrastructure beyond retail financial services to support cross-border SME trade and onboarding.

Aperta connects existing open finance networks, using domestic trust frameworks and their established registries of TPPs, and provides a translation capability to enable data interoperability between domestic standards. Within these registries are TPPs that operate as aggregators, which already provide connection to multiple FIs. By supporting aggregators, Aperta does not need to integrate with each individual FI in a jurisdiction; instead, it can also enable connectivity through aggregators that already provide access to multiple institutions within the network.

By bridging these established data standards and trust layers across jurisdictions, the blueprint removes the need for numerous bilateral integrations and instead creates a multilateral network of networks. Open finance makes this possible because:

- **Open finance is already a reality in multiple jurisdictions**. Project Aperta is able to reuse existing, tested infrastructure, enabling easy participation of banks and TPPs which are already registered in their home jurisdictions. It builds on consumer familiarity with open finance concepts and services such as consent-based data-sharing.
- **Open finance typically uses familiar, standard technical capability.** Project Aperta's solution building blocks are also familiar and within the technical competence of most developers of SME solutions. They include API-based interfaces, existing frameworks for public key infrastructure (PKI) and certification for trust capability.[29] Payment initiation is also a familiar, standard feature of open banking and open finance in all jurisdictions in scope for the prototype.
- **Trust frameworks reduce the need for bilateral arrangements**. Project Aperta respects local regulatory, trust and security frameworks. The project's overarching principle was to limit the impact on domestic open finance infrastructures, standards or regulation while creating a prototype to ease the path for adoption.
- **A potential direction of open finance and trust is towards federation.** Project Aperta evaluated several technical design options, including federation of trust, which preserves regional autonomy and reduces centralisation risks. Federation would require the adoption of a common data standard and typically involves policy and change coordination across jurisdictions. The prototype built by Project Aperta instead relies on existing standards in order to avoid the need for immediate policy change, while still supporting expansion.

Project Aperta reinforces global efforts in open finance and trade

Project Aperta complements other cross-border data-sharing efforts in general, and particularly in the context of its trade finance use case; it should not be viewed in isolation. Project Aperta's stakeholders included the Global Legal Entity Identifier Foundation (GLEIF), and the project sought input from experts in the United Nations Commission on International Trade Law (UNCITRAL) to assist with and advise on cross-border harmonisation – though Project Aperta sets out to work with existing standards, not define them. The Project Aperta prototype includes the global Legal Entity Identifier (LEI) in the data specifications of the use cases to support global identity and verification best practice.[30] The project benefited from insights and lessons learned from other BISIH projects, such as Nexus, which addressed cross-border interoperability for domestic instant payment networks and encountered similar challenges.[31]

The prototype and templates built as part of the project used open, widely adopted standards wherever possible. For the trade finance use case, Project Aperta built upon the International Chamber of Commerce Digital Standards Initiative (ICC DSI) and SWIFT's collaboration on trade API standards, feeding insight from Project Aperta back into the ICC DSI through mutual stakeholders.[32] These definitions future-proof adoption, as they align with SWIFT message type standards and future ISO 20022 compliance to minimise disruption to existing trade networks.[33]

Globally, over 120 initiatives are under way to digitise trade finance. Of those, just under 50 are examining trust frameworks.[34] Trust frameworks include private networks such as the Trade Worldwide Information Network (TWIN), which uses distributed ledger technology to make global trade efficient.[35] Persistent obstacles that can hinder adoption include technical incompatibility or concerns around lock-in. Aperta's ambition is to create an open framework – using open standards where possible – to encourage data exchange by default, as an alternative to privately negotiated discrete solutions.

PKI is frequently used to enable trust between parties and in trade trust frameworks. Project Aperta extends this to enable multilateral trust between existing trust frameworks. Project Aperta aims to complement existing networks, but is unique as it also brings with it the benefit of interlinking open finance capability with the benefits of digitised trade. This can be seen as an implementation of an interoperability layer, defined as "a virtual umbrella of shared assets (schemas, code lists, APIs, conformance tests)", which aims to break the pattern of application-based bilateral interoperability services.[36]

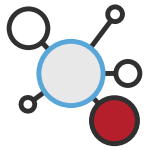
Project Aperta's prototype and templates are built with extensibility in mind in order to further accelerate the opportunity for public and private sector progress in enabling cross-border data transfer and finance interoperability. Using open banking and open finance as a starting schema extends applicability to over 90 economies already with – or contemplating – open finance. Project Aperta is also designed to be flexible and enable other use cases within open finance, with the possibility for extensibility to other open data or smart data networks and industry sectors.

1.6 Progress to date

In 2025, the BISIH Hong Kong Centre developed a solution design for Aperta through multiple design workshops with central banks, regulators, global foundations, trade organisations and universities. The Project Aperta team built a working prototype to test the proof of concept and enable the onboarding of TPPs from five established open finance frameworks, adding India to the scope of testing alongside Brazil, Hong Kong SAR, the United Arab Emirates and the United Kingdom.

This prototype was tested by banks, regulators and TPPs from five jurisdictions (including testers from India) and confirmed the technical viability of the Aperta model.

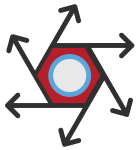
The work has been structured around the following goals:



Evaluate approaches to open banking and open finance across five jurisdictions and identify synergies and best practices, contributing to policy discussions on open finance, trust frameworks and data portability;

Recommend an approach to prototyping an interoperable, multilateral open finance framework that securely connects domestic open finance networks across the participating jurisdictions;

Develop technological architecture options, designing a prototype as well as a blueprint and extensible framework using insights from the prototype, scalable to additional jurisdictions, use cases and product types for potential later phases; and

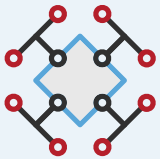


Prove the model through a prototype and private sector testing using trade finance use cases, building upon existing domestic open finance frameworks and standards in trade finance, augmented with new interoperable infrastructure.

This report summarises the output from this work. Section 2 gives a high-level understanding of how Aperta works to enable cross-border data portability using open finance, as well as the scope of the prototype use cases. Section 3 goes in depth into the architectural options, design considerations and technical components for the prototype and reusable design. Section 4 outlines the main findings from the project and considerations for future extensibility for Aperta, including potential for further use cases for development.

2. How Aperta works

2.1 Key takeaways

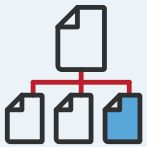


A network of networks for open finance:

The Aperta prototype is designed to act as an interoperability layer connecting domestic open finance networks, demonstrating how banks, fintechs and TPPs in different jurisdictions could interact. Aperta does not replace existing structures.

Trust and API interoperability:

A common trust framework, data translation layer and encryption layer is designed to enable participants using different technical standards to securely exchange financial data across borders, including payment instructions for initiating payments in another jurisdiction.



Support for any use case:

The prototype demonstrates how interoperable trust frameworks can support cross-border use cases such as account opening and trade finance. By testing a diverse range of examples, it shows potential applicability beyond SMEs, including retail consumers and additional financial products or sectors.

Transparency to the end user:

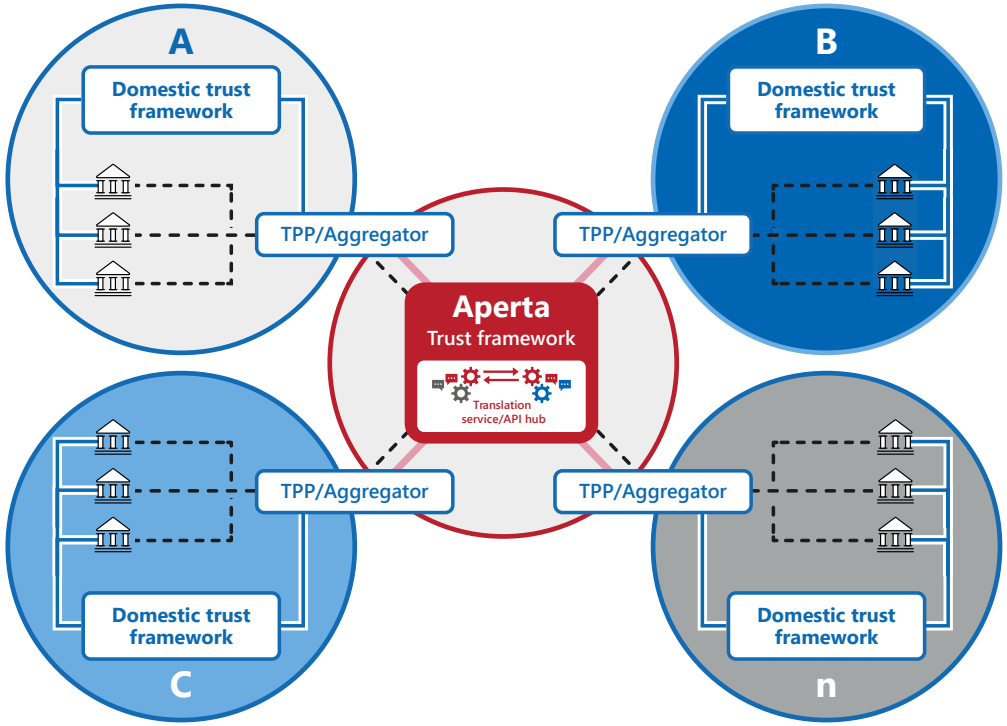
Users do not interact with Aperta directly; instead they interact via the TPPs, banks and fintechs in their own domestic environment. The only discernible change would be having a wider choice of overseas TPPs from which to select services.

2.2 Aperta's interoperability approach: the network of networks

Within the Project Aperta prototype, Aperta functions as a network of networks, bridging domestic open finance frameworks (see Figure 6). This is achieved by mirroring the registration of all domestic open finance participants across the open finance frameworks participating in the Aperta prototype. When a jurisdiction chooses to join, the local registrations of all participants are copied from the domestic trust framework into Aperta's central trust framework registry and subsequently synchronised.

Because of this, end users are not interacting with Aperta directly. They interact via the TPPs, banks and fintechs in their own domestic environment, who would ultimately be responsible for the end user experience and for obtaining consent for the requested service. Aperta's trust framework and translation service run in the background, accessible via a set of functional APIs.

Figure 6: How Aperta connects domestic frameworks as a network of networks



1 **Connecting network participants**
Aperta facilitates seamless interaction between domestic TPPs and domestic trust frameworks. The TPP could be a bank (directly registered on Aperta as a TPP), an aggregator (a special type of TPP which offers one-to-many connectivity to multiple domestic banks) or a fintech such as a trade finance solution provider.

2 **Framework integration**
Domestic trust frameworks achieve cross-border scope by registering directly with the Aperta trust framework through automated, semi-automated or manual onboarding of their respective registered TPPs. If a TPP acts as an API aggregator, the list of connected FIs is also recorded in the Aperta trust framework. This creates a standardised environment in which local rules are respected while enabling global connectivity.

3 **Data translation and routing**
Aperta acts as the intelligent, secure routing engine of the network. The prototype translates data formats in real time and encrypts and routes requests to the destination bank via the relevant TPP or aggregator. Aperta demonstrates how banks and fintechs could speak the same language even if they use different technical standards. The data exchanged can include financial information or transaction instructions, such as initiating a payment or updating the status of an LC.

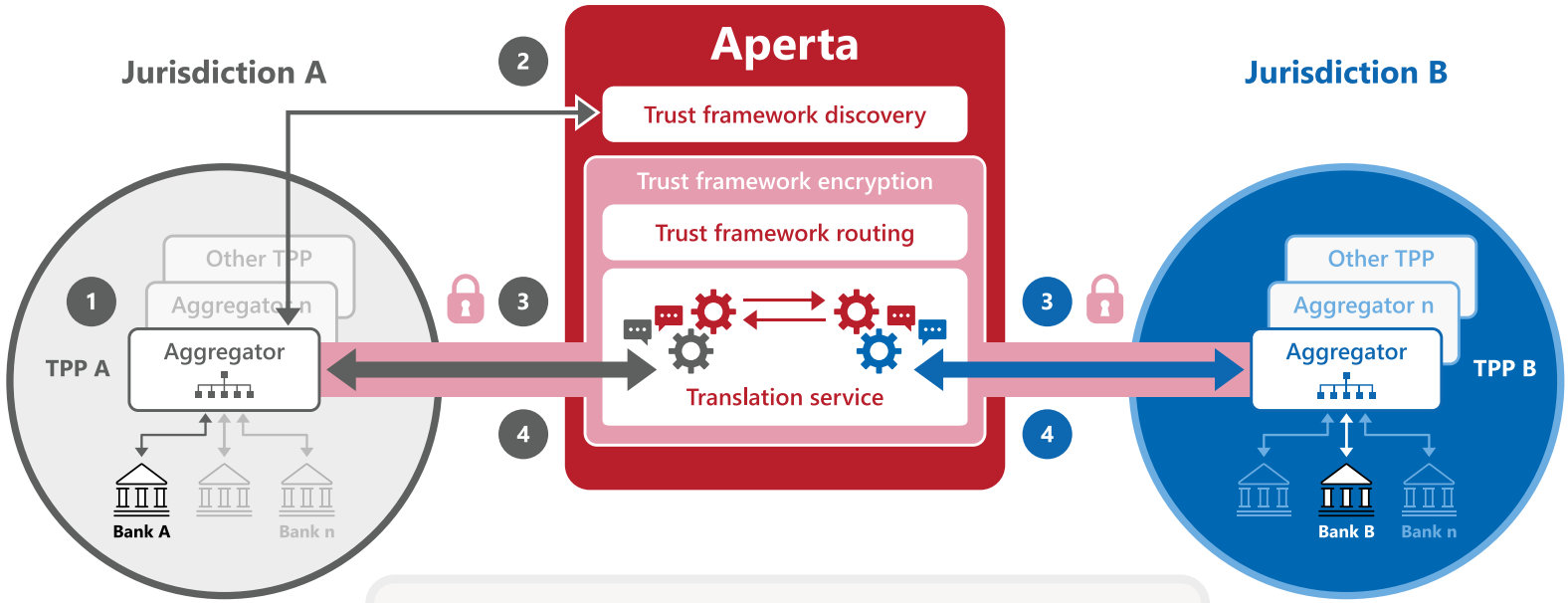
Project Aperta drew on practical lessons from Project Nexus, which explored multilateral interoperability between domestic instant payment systems. Nexus highlighted that bilateral connectivity models become increasingly difficult to scale, as each additional participant requires new technical and legal arrangements. It also demonstrated the value of enabling interoperability while preserving domestic infrastructures and regulatory frameworks.

The prototype solution

The Aperta prototype solution consists of a common trust framework, data translation layer, encryption engine and the APIs required to interact with it. Aperta maintains a single, central directory listing all registered TPPs, their roles and the addresses for their APIs so users from different countries can discover them and trust who they are dealing with.

When a TPP in one jurisdiction intends to request data from a TPP in another, it first queries the trust framework discovery service to identify the appropriate counterparty and determine the most efficient way to reach it (see Figure 7). The counterparty in the other jurisdiction may also be accessible through another TPP acting as an API aggregator. Aperta recognises the role of each TPP, and can identify whether it functions as an API aggregator or another type of intermediary TPP, and presents the user with options if there are multiple routes to reach a counterparty.

Figure 7: How Aperta operates as a network of networks



1 User in jurisdiction A grants consent to TPP A to share data from bank A to bank B. TPP A could be either: (a) a standalone TPP; (b) an aggregator with a TPP role; or (c) bank A with a TPP role. Regardless of type, TPP A needs to be registered with the Aperta trust framework.

2 TPP A requests from Aperta the list of TPPs in jurisdiction B that can connect to bank B. These TPPs could be either; (a) standalone TPPs; (b) aggregators with a TPP role; or (c) bank B with a TPP role. Regardless of type, each of these TPPs needs to be registered with the Aperta trust framework.

3 TPP A selects TPP B, establishing a trusted relationship using certificates issued by the Aperta trust framework PKI. TPP B receives the relevant information about TPP A within the request forwarded by Aperta and does not need to call the Aperta trust framework.

4 TPP A transmits data to bank B via TPP B, where this data is routed and translated using the Aperta translation service.

Types of data and services

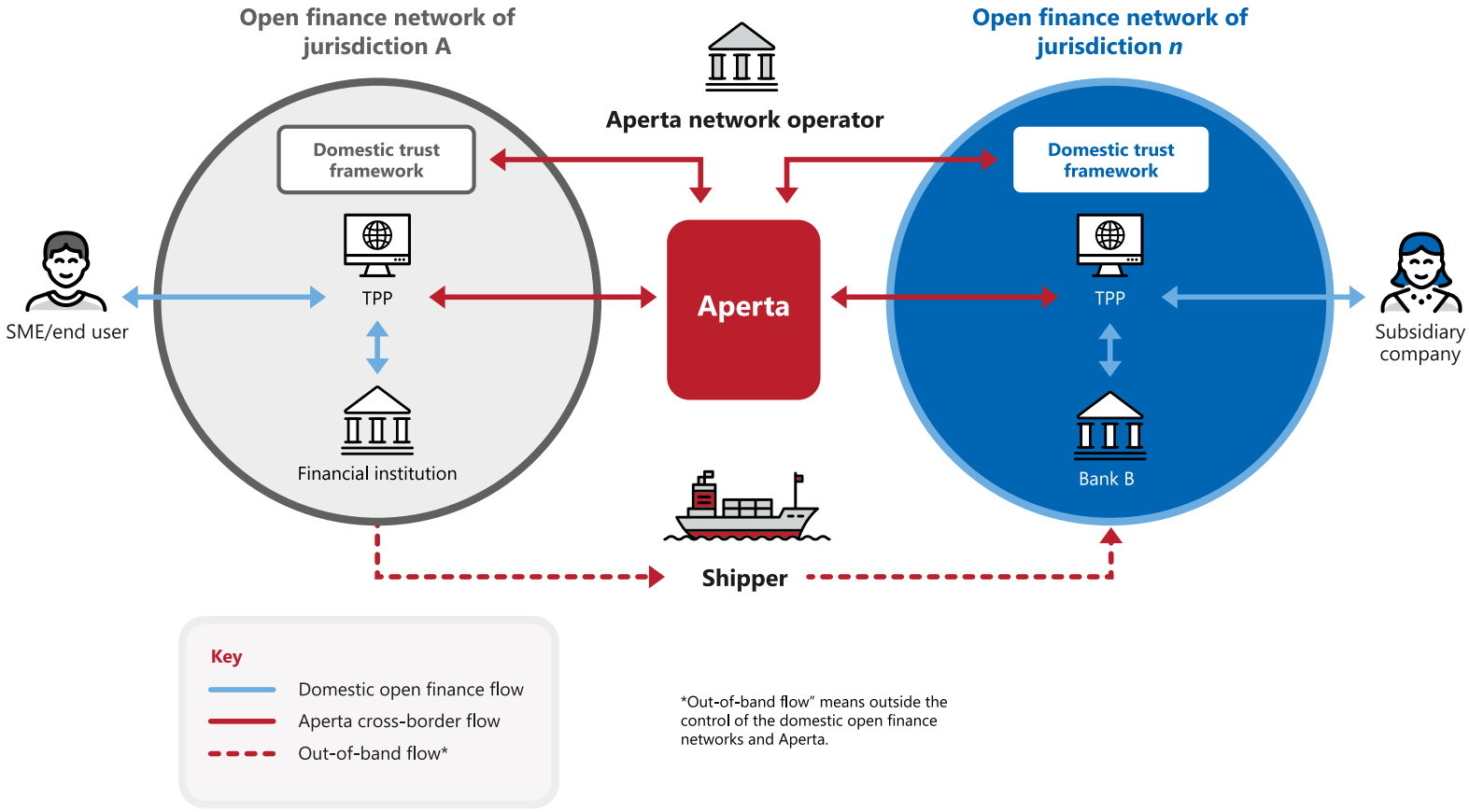
1) Bank account data

The prototype supports cross-border sharing of financial bank account data using open finance standards, with data either "pushed" from the source jurisdiction or "pulled" on request from the destination. It is technically feasible to extend this model to other open finance data, such as investments, pensions or mortgages, where equivalent products exist in both jurisdictions, and later to other standardised open or smart data (eg telecoms, energy or property).

2) Trade finance instruments and documents

To enable the trade finance use case the prototype follows the principles of the SWIFT trade finance APIs, the API standards of the ICC DSI and UNCITRAL's Model Law on Electronic Transferable Records (MLETR), adding the LEI, to support the objectives of using open standards, simplifying adoption and maximising applicability. The Aperta prototype also enables international payment initiation, with the technical potential to offer liquidity bridging services, subject to agreements between participating parties.

Figure 8: Actors in Aperta



2.3 Actors in Aperta and how they benefit

Aperta's novelty lies in extending the scope of open finance and bringing in new participants alongside actors traditionally recognised in open finance. For a potential real-world implementation, this would require regulatory acceptance of these additional actors and TPP types within local jurisdiction frameworks. In a real-world implementation, an Aperta network operator is needed to govern the ecosystem and run the infrastructure components. Aperta could technically enable other sectors or network operators to interoperate with other jurisdictions, sectors or industries with compatible trust frameworks, subject to harmonisation work on standards and legal frameworks. Aperta's actors (see Figure 8) include:

SMEs/End users

These are companies/subsidiaries/buyers/sellers/retail account holders, including businesses that want to open accounts abroad or obtain trade finance, authorised individuals acting on behalf of a business and retail account holders whose consumer accounts may be checked for know-your-customer (KYC)/know-your-business (KYB) purposes. They do not interact with Aperta and are served via TPPs registered with Aperta.

Financial Institutions (FIs)

These are open finance API providers. Licensed financial institutions (LFIs) such as banks hold accounts, perform KYC/KYB and anti-money laundering (AML) checks and expose open finance APIs in their domestic networks. In the SME context, they may provide verified information relevant to fraud prevention, trading legitimacy and indicators such as revenue receipt or turnover, subject to applicable regulatory frameworks. An FI is either directly registered as a TPP with Aperta or accessible via a domestic aggregator that is registered as a TPP with Aperta, reducing the need for separate bilateral trust framework integrations.

TPPs

These are FIs directly connected to Aperta, aggregators, fintechs and trade finance intermediaries. Licensed open finance participants that obtain customer consent, connect to FIs' APIs and initiate or broker cross-border data and service flows (including trade finance flows). They can connect once to Aperta's common cross-border trust platform to reach multiple jurisdictions, simplifying integrations and enabling new value added services for clients. They are directly registered as TPPs with Aperta.

Domestic trust frameworks

These are national infrastructures and authorities that define open finance frameworks, license open finance/banking participants and oversee compliance in each jurisdiction. Often managed by regulators or central banks, they could also be private sector trust frameworks. Through participation they obtain a demonstrable model for secure cross-border data portability that respects domestic rules while informing future policy and standard-setting. They register to participate, then integrate their framework with Aperta's network of networks.

Aperta network operator

This is the central entity and governance body responsible for setting the rules that define the transnational trust framework, managing and operating central services and coordinating participating jurisdictions. It could serve as a potential global network operator, providing a viable prototype and template for how global open finance interoperability, standards and best practices might be organised to create an interoperability network of its own.

Indirect actors

To enable trade finance, the prototype includes parties such as shippers or logistics firms acting as licensed TPPs.

Shippers

International shipping companies and/or other logistics parties that manage the physical movement of goods and the presentation of shipping documents in trade finance flows. In the prototype, they operate outside the influence of Aperta ("out-of-band flow") as current open finance frameworks do not include this type of TPP within their frameworks.

2.4 The focus of the prototype: the two implemented use cases

Project Aperta and its project participants tested cross-border interoperability through two SME-focused use cases implemented on the prototype: (i) cross-border business account opening and (ii) a multi-stage trade finance journey.

During a transaction, the end user interacts with the TPP, who is responsible for the user experience and user interface during the process. In both cases, TPPs act as the operational conduits, requiring consent (captured as a "consent object", a structured digital record of what data can be shared, with whom and for how long) before exchanging data between domestic networks, while Aperta enables cross-border interoperability without requiring changes to existing open finance standards and regulatory frameworks (see Figure 9).

Figure 9: Core design features: Trust, consent and secure data handling across jurisdictions

Trust

Third party providers are registered in both the domestic and Aperta trust frameworks.

Aperta must validate both parties' roles and permissions before any connection is established and data can flow.

Aperta's PKI allows authorization and assurance throughout the process.

Consent

Consent is created, managed and enforced entirely within domestic networks using existing open finance mechanisms.

Aperta only processes data permitted under that consent and never stores or transfers the consent object itself.

Data and encryption

Data is translated between domestic schemas and transmitted via secure, encrypted channels without central storage.

This preserves confidentiality, integrity and auditability while allowing interoperability across jurisdictions.

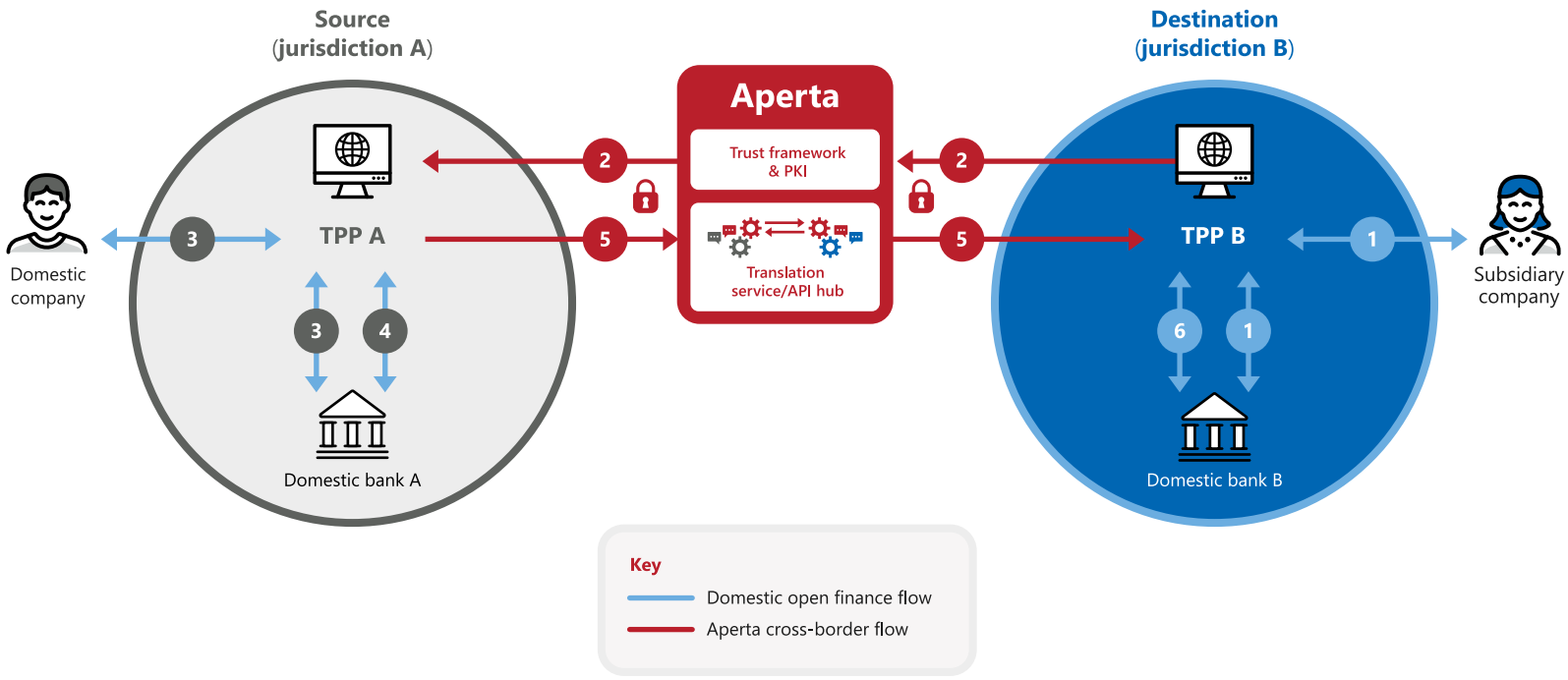
Both TPPs (the counterparties) are required to be registered with both Aperta and their domestic trust frameworks. This dual registration enables Aperta to bridge the cross-border connection and keeps elements of the process within the domestic trust framework. The prototype demonstrates that these interactions can be executed using existing infrastructure, keeping trust, consent and data handling anchored in domestic networks and preserving auditability through a verifiable, time-stamped record of data access, permissions and participants across jurisdictions.

Use case 1 – Cross-border account opening

Use case 1 is tested to demonstrate how an SME can open a business account in another jurisdiction by sharing verified financial and KYC/KYB data from its domestic bank relationship.

This scenario uses a request-initiated data-sharing model, in which a TPP actively requests access to the user's financial data from the data holder on the user's behalf. The destination-side TPP – such as a trade finance intermediary, a business bank account comparison marketplace or a directly registered bank – requests access to the SME's domestic account data via a domestic TPP, either the directly registered domestic bank or an aggregator that enables access to that bank. The SME authorises the initial request with the destination-side TPP and then consents to sharing the relevant data through familiar open finance consent journeys.[37] The data shared may include account details, transaction history and other relevant financial information, which can be used to support use cases such as account opening. The same process can also be used to connect to a retail bank account to verify named account holders, owners or ultimate beneficial owners (UBOs) of the business. The TPP receives all relevant financial data to process the SME account application. These data are also used for credit scoring, enabling faster decision-making, approvals and account openings.

Figure 10: Opening an overseas business bank account via Aperta



At a high level, the flow is as follows (see Figure 10):

1. The SME applies for an account with a foreign bank, typically via a destination-side TPP.
2. The destination TPP requests access to KYC/KYB and financial data from the source TPP via Aperta, using digital certificates and a digital pass, then verifies the business owners and UBOs. The SME authenticates and authorises this request via its domestic open finance interface.
3. A domestic TPP or bank retrieves and prepares the requested data, having captured consent.
4. Data are transmitted cross-border via Aperta between the participating TPPs. During this step, Aperta uses the Aperta data translation protocol as outlined in the "Interoperability and data services" subsection to translate the data from source to destination format.
5. If the destination TPP is a directly registered bank, this is the end of the flow; if the third party is an aggregator or a marketplace intermediary, there is an additional step in which the destination-side TPP delivers the data to the foreign bank to support onboarding and verification.

This approach allows the destination bank to define its data requirements while relying on trusted, pre-verified information sourced from the SME's domestic financial relationships. It also enables onboarding decisions to be made using structured, machine-readable data rather than manual document collection, while keeping the SME within a familiar domestic consent user experience.

Use case 2 – Trade finance

Use case 2 extends the same cross-border interoperability approach to a trade finance lifecycle involving multiple parties, documents and stages.

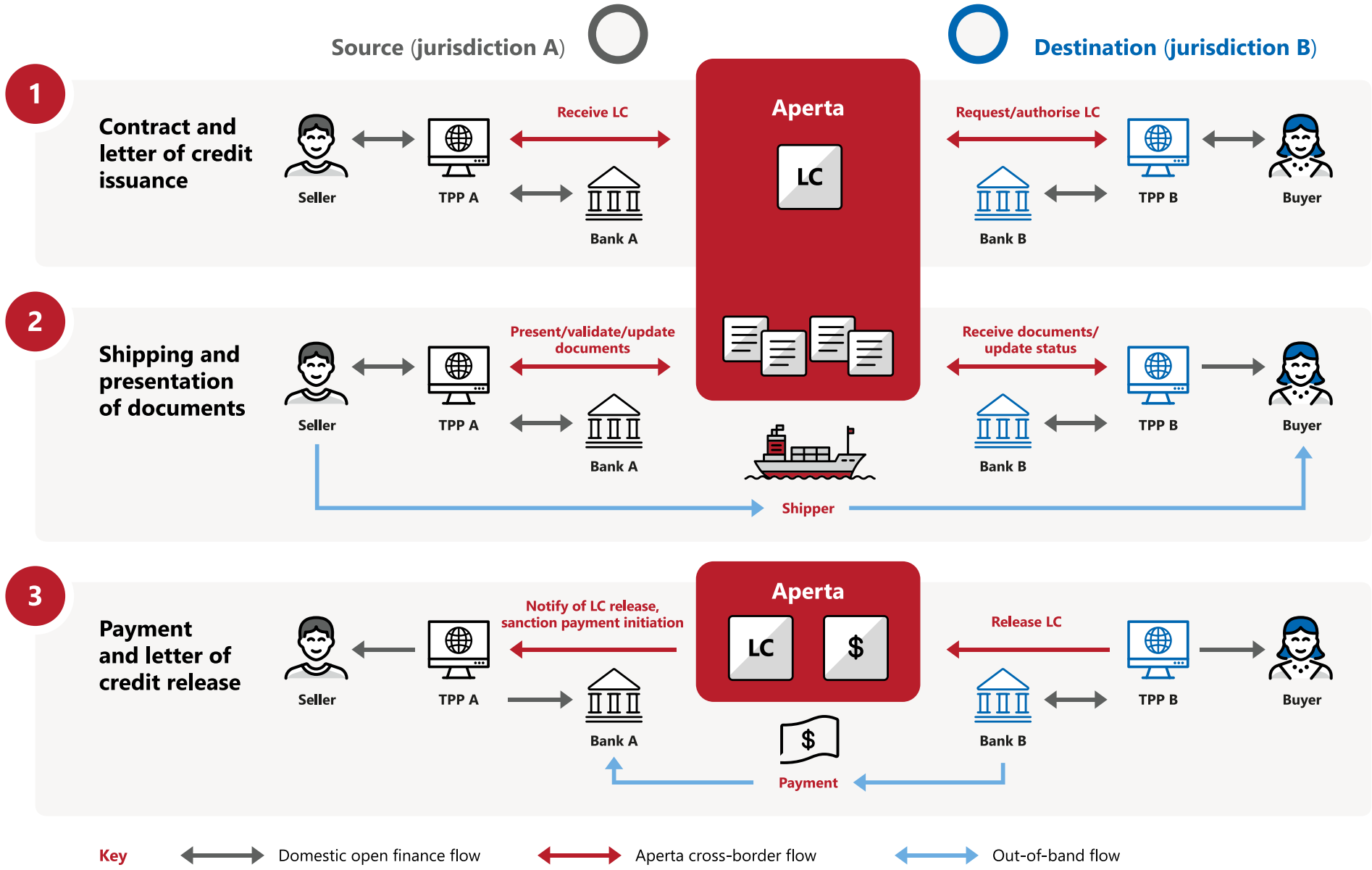
As with use case 1, TPPs or trade-focused intermediaries play a key role in orchestrating the exchange of data and documents between institutions using standardised APIs, acting as integration points or "bridges" alongside participating banks and platforms. As detailed in "Types of data and service", the prototype follows SWIFT and ICC DSI trade API standards and UNCITRAL's MLETR and incorporates the LEI. Aperta also supports international payment initiation, with the technical potential to offer liquidity bridging services triggered by invoices or letters of credit (LCs).

Unlike account opening, this scenario involves a combination of request-based and event-driven data exchanges, reflecting the more dynamic nature of trade finance processes. Data may be requested on demand or shared at defined points in the transaction lifecycle. Aperta tracks and provides audit data on the progress of each trade finance case within the Aperta translation service and API hub.

Box 2: Testing use case 2: integration with a blockchain-based trade finance platform

During testing, a participating bank was able to integrate the Project Aperta prototype into its existing blockchain-based trade finance platform by leveraging API connectivity and aligning with ISO 20022 standards already embedded in its architecture. Using an "open connector" layer, the KYB functionality was incorporated as a modular, off-chain service that could interface seamlessly with tokenised trade finance workflows. This enabled Aperta to act as a trusted validation layer at the outset of the trade finance process, verifying the identity and legitimacy of traders before contract execution. As a result, onboarding integrity was strengthened and counterparty fraud risk significantly reduced without requiring major changes to the core platform.

Figure 11: The three stages of use case 2 – Trade finance



The prototype simplifies this into three stages (see Figure 11):

1. **Contract and LC issuance**

   Buyer and seller agree on terms and an LC is issued. TPPs facilitate the exchange of contract and issuance data between institutions across jurisdictions.

2. **Shipping and presentation of documents**

   Trade and shipping documents are created and shared between parties. TPPs manage the structured exchange of documents such as invoices, bills of lading and certificates of origin. Shipping occurs outside the influence of Aperta (ie outside its data and messaging layer), reflecting physical trade execution that is not processed within the network. The status of the transaction (eg shipped, received etc) can be updated in real time.

3. **Payment and LC release**

   Documents are reviewed and validated. TPPs support the standardised, secure transmission of verification outcomes and payment initiation instruction data between parties, including invoices. Payment occurs outside Aperta (ie settlement is executed through external financial networks, with only related instructions and status updates exchanged via Aperta).

After contract fulfilment, financial and trade data may be reused, where appropriate and with the right consent, to support future risk assessment and credit decisions, again facilitated through TPP-mediated access.

While this use case introduces additional participants, document types and process steps, it follows the same underlying approach demonstrated in use case 1: TPP-mediated, consent-enabled data exchange across jurisdictions, facilitated by Aperta without requiring changes to domestic networks.

While the diagrams present a simplified view for clarity, the underlying trade finance process is significantly more complex, spanning multiple actors, document flows and cross-border dependencies, all of which are fully detailed in the solution design documents.

Role of Aperta across both use cases

Across both scenarios, the Aperta prototype is positioned to operate as an interoperability layer between TPPs and participating institutions in different jurisdictions, rather than as a participant in the transaction itself, using data only for the purposes of processing.

It enables participants to:

Discover and identify trusted counterparties and their endpoints;

Verify roles and credentials prior to interaction;

Translate between different domestic data models and API standards; and

Route data securely between TPPs without long-term central storage.

What the prototype demonstrates

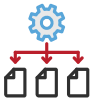
The two use cases demonstrate that interoperable intermediaries can connect domestic financial data networks via APIs, avoiding the need for all institutions to integrate identical technical standards (see Box 2). Once a jurisdiction has joined the Aperta prototype, a TPP registered with the joining jurisdiction's domestic trust framework will be able to offer cross-border services with any other jurisdiction present in the Aperta network. Aperta provides a low-barrier way for participants to expand into new markets and strengthen their domestic economies.

The use cases demonstrate that:

Domestic TPPs can act as "bridges" across jurisdictions;

Different interaction patterns such as request- and event-based data exchange can be supported within a common framework;

Trust, consent and regulatory accountability can remain anchored in domestic regimes; and



Interoperability can be achieved via translation, without the need to standardise underlying networks.

The prototype focuses on technical feasibility. Legal, regulatory and policy considerations remain within the scope of individual jurisdictions (see Box 3).

Box 3: Considerations for the two use cases

Project Aperta has focused primarily on demonstrating the technical feasibility of cross-border data-sharing through open finance infrastructure. Policy harmonisation, licensing regimes, supervisory approaches and the legal recognition of digital trade documents remain matters for individual jurisdictions.

Participation in an Aperta-type ecosystem would require a degree of regulatory alignment across participating jurisdictions, particularly in the licensing and oversight of TPPs involved in cross-border data-sharing. Jurisdictions may also need to establish legal frameworks that support the digitalisation of trade and the recognition of electronic records. In this context, the adoption of internationally recognised frameworks such as UNCITRAL's MLETR could play an important role in enabling the cross-border use of electronic trade documents.

While Aperta demonstrates how such networks can interoperate from a technical perspective, decisions on regulatory alignment and legal adoption ultimately rest with participating jurisdictions.

3. Technology considerations for Aperta

This section describes the technology components of the Aperta prototype, which is intended to test feasibility rather than serve as a final solution.

3.1 Key takeaways

- **Comparison of architecture options.** Project Aperta compared jurisdictions' open finance frameworks and evaluated four architectural options, selecting a centralised model for the prototype and a federated option for potential future alternative implementations.
- **Designed to bridge – but respect – boundaries:** The prototype preserves jurisdictions' domestic open finance frameworks, adding central services for discovery, encryption and translation, in order to minimise change and ease adoption pathways.
- **Designed with layered security:** Security is embedded across the design, combining transport-level protection, message-level assurance and strict identity governance. Data are not persistent or visible within Aperta, which operates as a data processor, not a controller**.**
- **Common interoperability and data services:** The Aperta data translation protocol translates from source format into an Aperta format for cross-border transmission, and then into destination format so participants can retain their native standards while interoperating. Beyond facilitating data translation, it also supports the execution of transactions.
- **Built with open, widely adopted standards:** To avoid vendor lock-in in a potential future production solution and to ease adoption, the solution uses open standards and creates reusable artefacts to support public and private sector extensions of the Aperta solution or to allow a potential Aperta network operator to take over.

3.2 Architectural options and decisions

Project Aperta assessed various solution design options, with two notable approaches: a centralised model, used as the practical basis for the prototype, and a federated alternative, considered to support a foundational and repeatable framework.

A common set of evaluation criteria was defined for the prototype design. The overarching principle was to minimise impact on local ecosystems, including both framework and standards considerations as well as the technical and implementation burden on participants. The Aperta prototype design sets out a common set of evaluation criteria that any architectural option should satisfy.

3.3 Evaluating the options

Project Aperta compared four architectural options using a common set of decision criteria based on its objectives and constraints. The criteria balanced short-term needs for the prototype, eg regarding speed, feasibility, participant complexity and cost, with longer-term goals such as interoperability, scalability, standardisation and security. This helped ensure that the chosen architecture supported both Aperta's role as a prototype and its potential as a blueprint for future cross-border open finance infrastructure (see Box 4). Options were assessed as follows:

Interoperability and network alignment readiness criteria assessed how easily heterogeneous domestic networks can connect in practice, given their current standards and regulation. This was central to Project Aperta's intent to demonstrate cross-border SME use cases using existing infrastructures rather than hypothetical future regimes.

Complexity for participants criteria evaluated the technical and operational burden on FIs, TPPs and aggregators (such as the number of formats, security models and integrations to support). Minimising this complexity is key to lowering barriers to entry for TPPs and users in order to make the prototype realistically deployable.

Security and trust criteria compared the strength and consistency of security baselines, trust anchors and governance (such as fragmented certificate authorities versus federated trust). A robust, demonstrable security posture is essential to build confidence in cross-border data portability.

Scalability and future-proofing criteria looked at how models behave as the number of jurisdictions and participants grows, and whether they encourage convergence on global standards (eg OpenID Connect (OIDC) Federation, ISO 20022). This directly supports Project Aperta's intent: a practical prototype now, with a pathway to decentralised, federated testing later.

Implementation speed and feasibility criteria considered how quickly each model could be established given the current heterogeneity of networks and regulatory frameworks. This was important in the context of the prototype's fixed timelines and its objective to demonstrate SME account opening and trade finance flows.

Total cost and central cost to operate criteria were used to distinguish distributed network costs, such as participant-level implementation, from central operational costs, such as the trust framework and translation service. This aligns with Project Aperta's objective to explore a financially sustainable model with the potential to scale beyond a prototype.

Project Aperta included a cost evaluation, recognising that the cost of enabling cross-border interoperability can vary significantly depending on the architecture selected. The comparative analysis estimated indicative annual costs for each model, taking into account development, infrastructure, and operational considerations, as well as how these costs might be distributed across participants and a centralised network provider. The following architectural options were each evaluated against the evaluation criteria:

1. **Option 1 – Native standards:**

   A decentralised architecture in which TPPs communicate directly using their existing domestic standards. Each jurisdiction's TPPs interconnect directly using their existing local API, data and security standards, with Aperta providing only a minimal central discovery service. TPPs are required to implement translation and routing for every other network's format and profile, including trust framework variants and certificate authorities.

2. **Option 2 – Common messaging protocol:**

   This option introduces a shared messaging protocol (eg ISO 20022) for all TPPs within the Aperta network. It enables unified communication between jurisdictions, but all participants are required to implement and maintain the common format in addition to local standards. Jurisdictions retain their domestic standards but add support for a single Aperta common messaging protocol and converged security profiles. TPPs operate a dual stack: a local standard for domestic traffic and the Aperta data translation protocol for cross-border traffic.

3. **Option 3 – Centralised aggregator of TPPs and trust frameworks:**

   Aperta operates a central trust framework and a centralised translation layer that converts messages between each jurisdiction's native standard. TPPs integrate once to Aperta using their domestic formats, with Aperta handling translation, encryption, routing and enforcement of common security policies.

4. **Option 4 – Federated trust with OIDC Federation:**

   This model envisages a fully decentralised, standards-aligned federation in which domestic trust frameworks and participants interoperate directly using common discovery, registration and security protocols (eg OIDC Federation, aligned Financial-grade API (FAPI) profiles). Aperta functions as a trust anchor and policy coordinator rather than as a message intermediary or translator.

Box 4: The architectural options

1 Native standards

- Decentralised architecture where aggregators communicate directly using local protocols and standards.
- Each aggregator must support inbound/outbound translations for all connected jurisdictions, driving high implementation overhead.
- Aperta acts as a directory and discovery service, not an intermediary in message processing.

2 Common messaging protocol

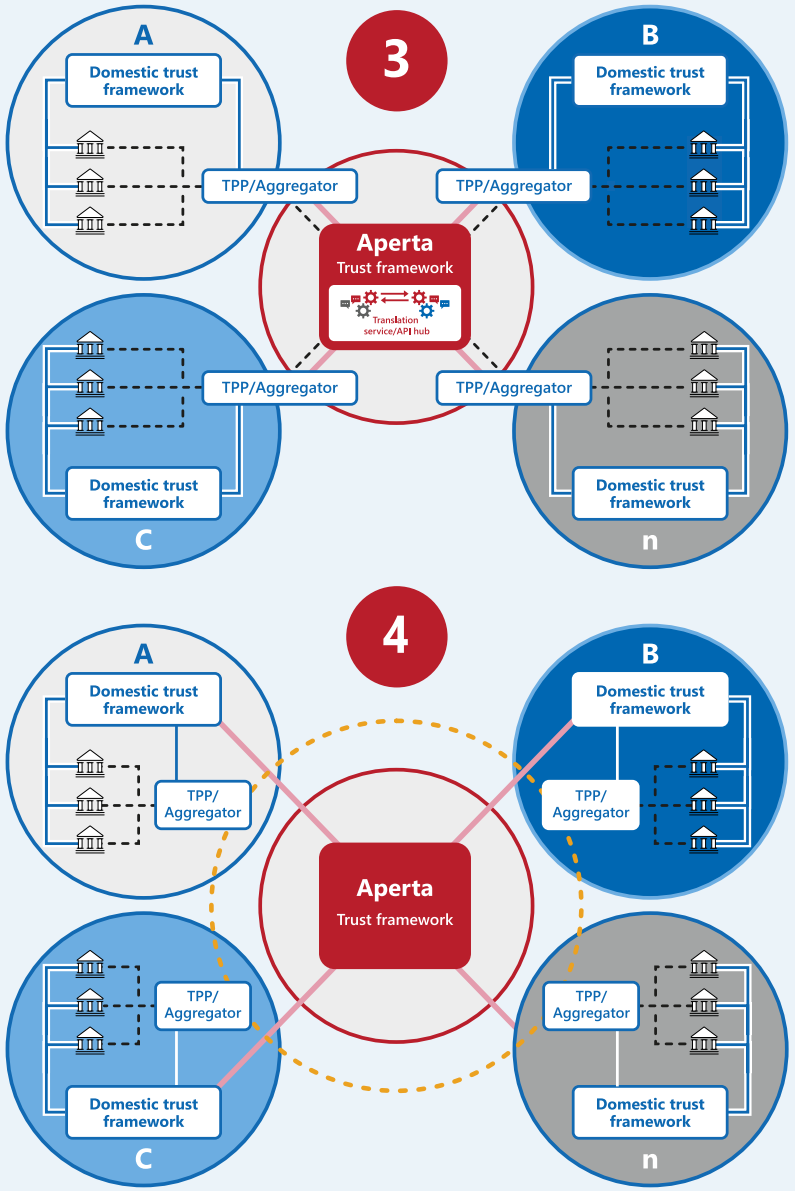
- Aggregators translate domestic formats into a single, shared protocol (eg derived from ISO 20022) for all cross-border communications.
- Aperta acts as a discovery and validation layer but is not responsible for translation.
- Efforts for developing the protocol must be maintained and governed centrally by Aperta.

3 Centralised aggregator of TPPs & trust frameworks

- Aperta handles all message translation and routing between networks using a central translation engine.
- Aggregators send and receive messages in their domestic format, simplifying their integration.
- Aperta bears responsibility for security compliance, message mapping, and protocol adaptation.

4 Federated trust with OIDC Federation

- Each network uses OIDC Federation protocols to dynamically discover, trust, and communicate with others using signed metadata and a common messaging data protocol.
- Aperta operates as a neutral trust anchor, facilitating federation without acting as a message relay.
- Fully decentralised model requiring significant regulatory and infrastructure alignment.



Key

- Registration/connection to Aperta trust framework
- Registration to local trust framework
- Participant communications using domestic standards
- Participant communications using common message protocol

Evaluative comparison of the architectural options

Option 1: Native standards

This creates high complexity, onboarding costs and operational burden as the number of networks grows and increases the attack surface due to fragmented security and trust anchors. Scalability and extensibility are weak as integrations are bilateral and each new participant adds many dependencies. Standardisation is poor, limiting convergence on global practices. Governance is diffuse with low central coordination, preserving local autonomy but undermining consistent policy and risk management. Direct interaction requires translation and routing logic implementation at each TPP, creating barriers to entry.

Option 2: Common messaging protocol

This substantially reduces the multi-standard complexity of Option 1, improves scalability and interoperability and enables clearer security alignment via a single cross-border profile. However, it requires coordinated development, maintenance and governance of the common messaging data protocol. All participating networks must implement this additional technology stack, slowing initial rollout. There is no centralised translation service; resilience is stronger, but onboarding and evolution depend on sustained multilateral standards governance.

Option 3: Centralised aggregator of TPPs and trust frameworks

This greatly reduces complexity and change for participants, accelerating implementation and simplifying onboarding of new markets and use cases, but at the cost of higher central operational expenditure and a potential single point of failure. Harmonisation is only moderate because domestic heterogeneity persists, but the model is evolution-ready: networks can later converge on shared protocols without disrupting the initial prototype. Governance is strong, with Aperta centrally managing message flow, trust and metadata.

Option 4: Federated trust with OIDC Federation

This offers high scalability, strong security and future-proofing, since networks share the same federation and discovery protocols. However, it requires extensive upgrades to many domestic networks, including regulatory alignment, and technical migration to federation protocols, making implementation very slow and costly in the current heterogeneous environment. In addition, all participating networks need to agree on a common messaging data protocol. For the prototype horizon it was assessed as strategically desirable but not yet practical.

Evaluation criteria	Option 1	Option 2	Option 3	Option 4
Ecosystem alignment readiness				
Standardisation				
Complexity for participants				
Scalability				
Governance				
Implementation speed				
Future-proofing				
Security				
Central cost to operate				
Total cost				

Key ○ Minimal ◔ Low ◑ Moderate ◕ High ● Very High

The decision on the centralised approach of the prototype:

Option 3 (Centralised aggregator of TPPs and trust frameworks) was chosen from the four options considered (see Box 4). It is a pragmatic, near-term model in which Aperta provides a central trust, discovery and translation layer so each TPP can keep using its existing domestic APIs and standards while interoperating cross-border. It minimises implementation effort, fits more easily within current regulatory frameworks and allows for rapid onboarding of new markets and use cases by concentrating complexity in the central service. It offers strong interoperability and a prospect for nudging ecosystems towards more standardised data models and security profiles over time. The centralised approach could be a viable option for future implementation if Aperta is adopted quickly.

The decision on an alternative approach for a long-term development model:

Option 4 (Federated trust with OIDC Federation) points towards a fully decentralised, standards-based model that enables networks to discover and trust each other directly without a central translation hub. It offers strong long-term interoperability, security, scalability and sustainability, while supporting harmonisation across jurisdictions. However, it requires substantial technical and regulatory change, making it less feasible for initial implementation in the current heterogeneous landscape.

Selecting Option 3 established the broad architectural direction for the prototype. The objective was to both determine whether a centralised model could support cross-border interoperability and to explore which implementation choices within that model could realistically operate across heterogeneous domestic open finance ecosystems. The prototype was therefore developed as an iterative exercise, examining alternative approaches across a number of core capabilities before converging on a practical design.

Several implementation avenues were explored within Option 3. The project assessed alternative architectural configurations and evaluated different approaches to trust framework design and participant onboarding. For the purposes of the prototype, a single centralised trust framework was selected, while multiple participant onboarding methods were incorporated to accommodate the diversity of domestic ecosystem arrangements and levels of maturity across jurisdictions. Different approaches to interoperability and data services were also considered, including methods of translating data formats between domestic API standards, ultimately leading to the use of a central API hub, translation and routing capability. A key technical challenge was to design a translation protocol that could map data fields from various source formats to different destination formats while preserving their meaning, and that could be modular, extendable and scalable so that new jurisdictions could be added over time without redesigning the core.

The project also explored the role of aggregators as a distinct type of TPP: rather than replacing them, the "network of networks" aims to connect aggregators (ie networks) across borders, thereby enabling them to expand their reach.

Security and consent were treated as design considerations throughout the experimentation process. The project evaluated different approaches to identity, authentication, encryption and consent handling, while preserving the principle that consent should remain embedded within familiar domestic open finance journeys.

A consistent lesson emerging from this experimentation was that concentrating interoperability functions within shared services reduced implementation burdens for participants and aligned more closely with the project's overarching principle of minimising changes to domestic infrastructures. This process reinforced that successful interoperability depends not only on technical capability, but also on balancing operational practicality, adoption considerations and compatibility with existing networks.

Lessons from Project Nexus

Lessons from Project Nexus informed several aspects of Aperta's decision on Option 3. Similar to Nexus, Aperta adopts an "integrate once" multilateral model intended to reduce onboarding complexity. Aperta also follows a principle of minimising changes to domestic ecosystems, concentrating interoperability functions within shared services rather than requiring jurisdictions to adopt a single common standard. Unlike Nexus, which focused on payment system interoperability, Aperta extends these concepts to open finance by introducing trust framework interoperability, participant discovery and cross-border translation of financial and trade data.

A more detailed description of Aperta's technology design principles and decisions is provided in Appendix A.

3.4 Testing Aperta - how Aperta works in practice

The testing phase validated the prototype design and engaged testers from **21** public and private sector organisations across **five** jurisdictions to test the Aperta prototype. These included **six** banks, **seven** TPPs and in addition **eight** steering committee members, providing coverage across data providers, service providers and governance stakeholders.

Experimental changes can create risk; for testing, the Aperta prototype did not connect to live open finance frameworks or bank or third-party APIs. Tests were conducted in a dedicated user acceptance test (UAT) environment with synthetic test data for each of the five jurisdictions in order to avoid using real customer information or sensitive data.

The prototype simulated the full Aperta trust framework, routing and translation service, providing a mock bank and demo third-party app per jurisdiction to enable testing of the two use cases. The API specifications and data standards of each jurisdiction's open finance standards were used for the testing of the API hub and data translation component.

Testing focused on three elements: (i) interoperability and the translation layer and APIs; (ii) the Aperta trust framework; and (iii) the two cross-border business use cases, account opening and trade finance.

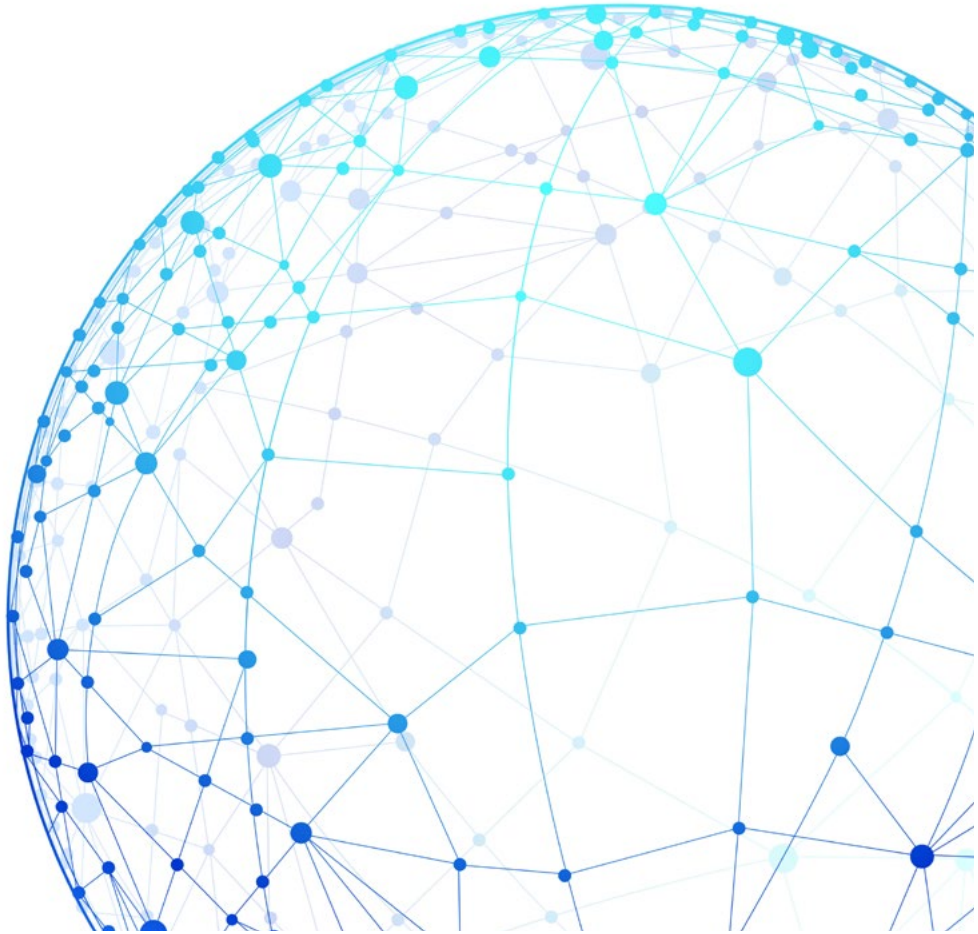
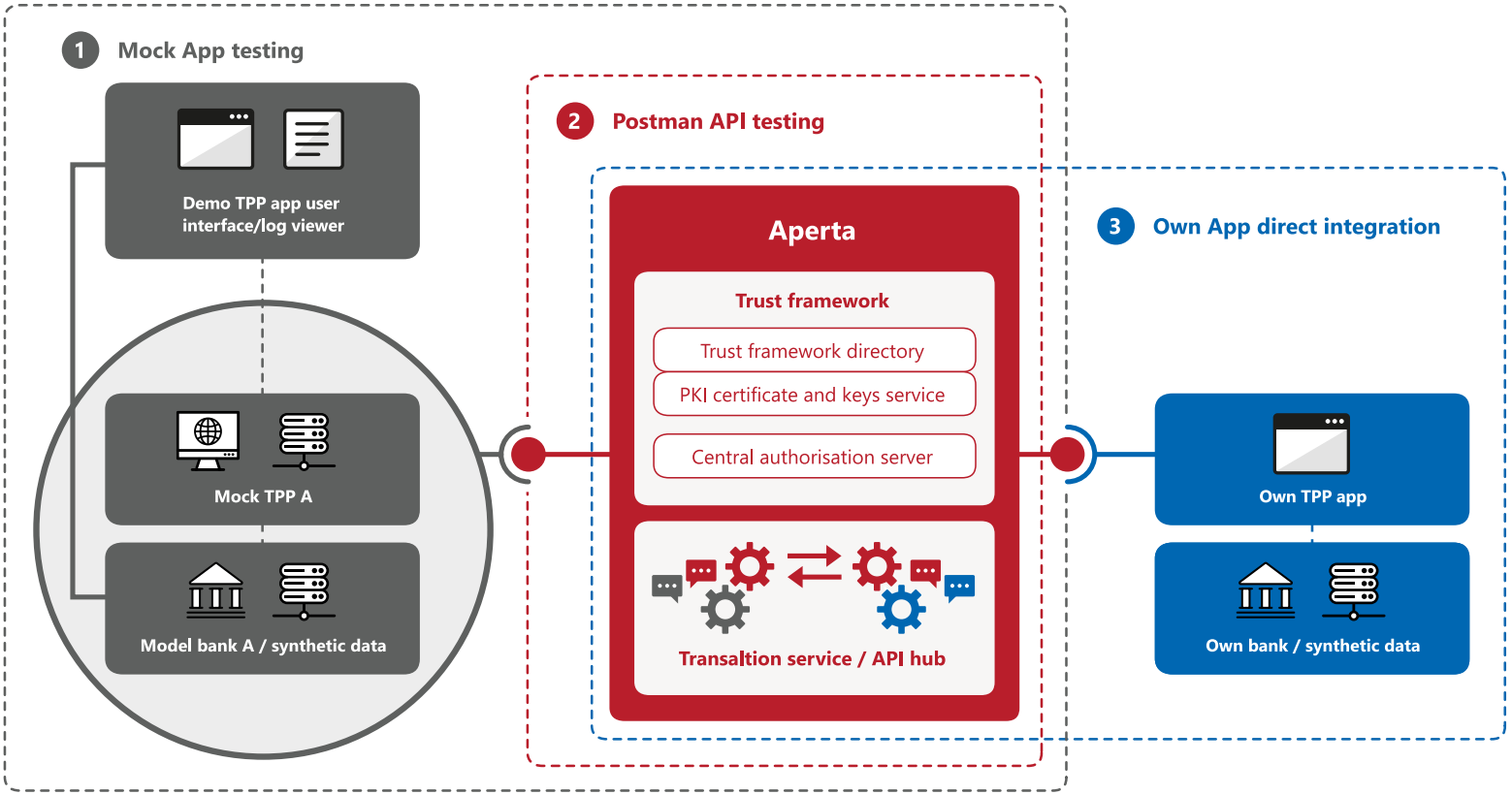


Figure 12: The three testing options within the prototype

The Aperta prototype supported three test approaches

1. via the prototype's user interfaces with mock TPP and model bank applications, with in-built log-viewer;
2. via Postman-based API collections for API-based testing; and
3. via direct integration with the Aperta APIs using their own mock application source.



Participants were able to test via three approaches: (1) via user interfaces with mock TPP and model bank applications; (2) via Postman-based API collections; and (3) via direct integration with the Aperta APIs using their own mock application source (see Figure 12).

A mock jurisdiction trust framework enabled unit testing of Aperta's functional APIs for semi- and fully automated onboarding in order to validate the performance of the automatic population of TPPs and registered APIs within Aperta's trust framework. It was also possible for a tester to integrate their own app via Aperta's APIs and specify their own synthetic data, which one organisation chose to do.

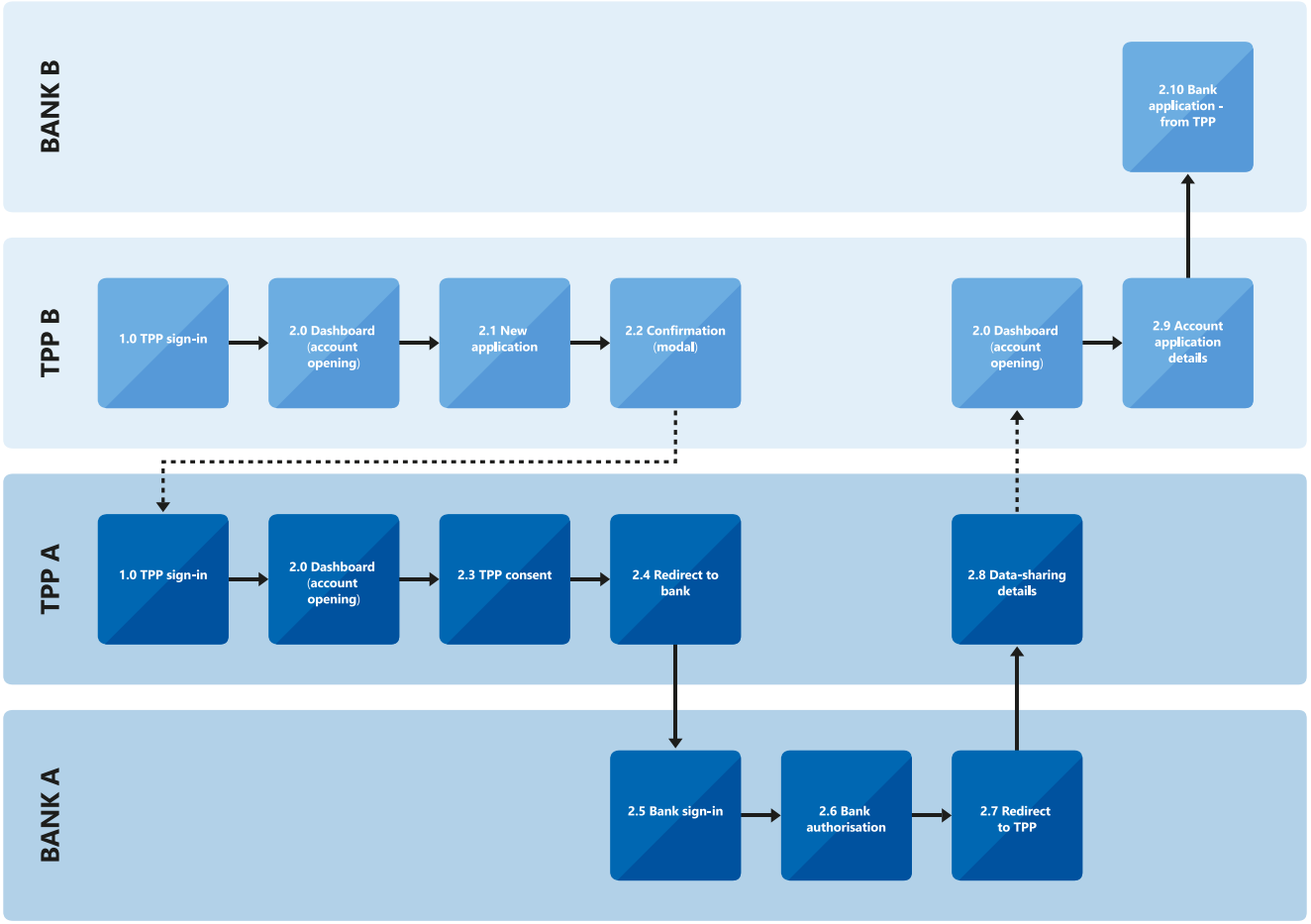
The prototype: what testers see

Most testers interacted through five demo TPP apps, each simulating a partial bank or third-party user journey to reflect real end user interactions. Complementing these apps, the test infrastructure included a developer portal featuring documentation, examples, synthetic test data and test scripts, providing teams with the necessary resources to evaluate the prototype effectively.

To further simplify testing, the app user interface incorporated a log viewer. This tool exposed the API calls exchanged between each app and the Aperta platform, offering clear insight into how Aperta's trust framework validated identities and established secure connections.

The wireframe flows in the prototype, meaning simple sketches of the user journey and screen sequence adopt a standardised, redirect-based consent journey (TPP consent screen > redirect to bank for sign-in and authorisation > redirect back to TPP for confirmation) (see Figure 13), while recognising that domestic guidelines differ and that real-world deployments may impose additional authentication factors.

Figure 13: The user experience flow for the prototype app for use case 1



Trust framework and translation services flow

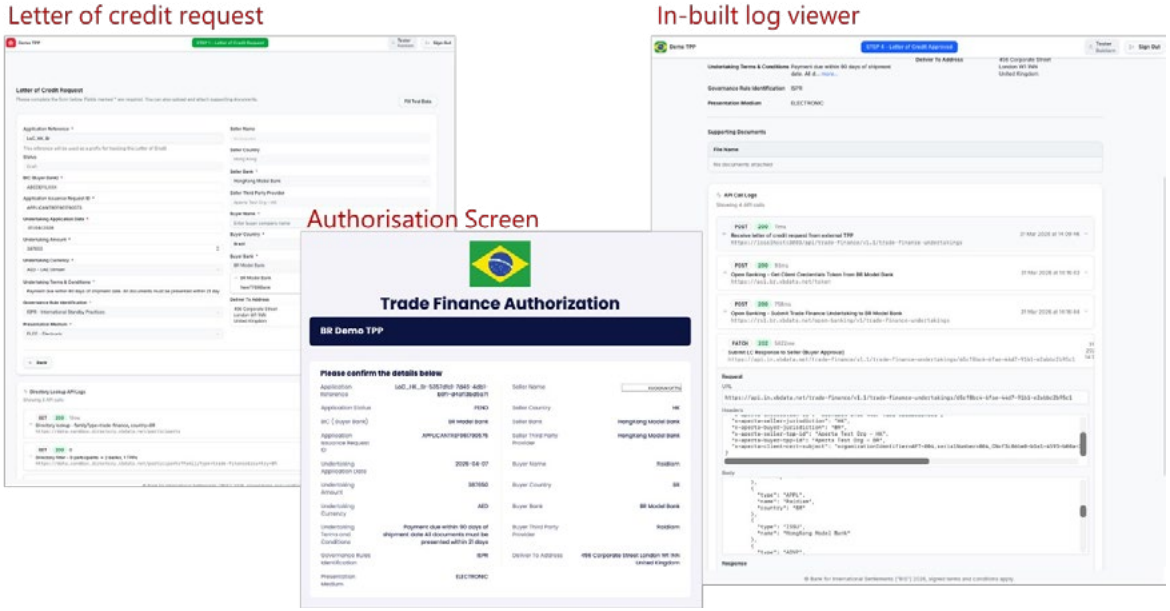
This flow shows how the user (eg a tester) will navigate through screens between the **TPP demo app** and **model bank** in **jurisdiction B** and the **TPP demo app** and **model bank** in **jurisdiction A** to complete the end-to-end account opening process for use case 1.

During testing, the Aperta prototype functioned as outlined in the blueprint. One bank integrated its own blockchain-based trade finance solution directly with Aperta's KYC/KYB capability within the account opening use case, using synthetic test data to verify the supplier's authenticity as a critical – and previously missing – step in its trade finance process. The bank was able to incorporate far greater security and assurance using Aperta to build a global "confirmation of payee" solution.

Testing demonstrated under controlled conditions that multilateral open finance interoperability is technically feasible and shows potential operational viability across multiple jurisdictions. The Aperta prototype was shown to support secure, consent-based cross-border data exchange, interoperability between different open finance standards and multi-party workflow orchestration without requiring fundamental change to domestic infrastructures.

The results underscore the need to expand the range of cross-jurisdiction participant and framework interactions; deepen data model alignment and formalise governance relating to trust, certification and cross-border data portability. Participants suggested improvements such as clearer certificate management guidance across jurisdictions; earlier sandbox access and more role-specific documentation, particularly for API configuration and testing. These insights offer actionable direction for any future scale-up alongside the established technical design.

Figure 13 continued



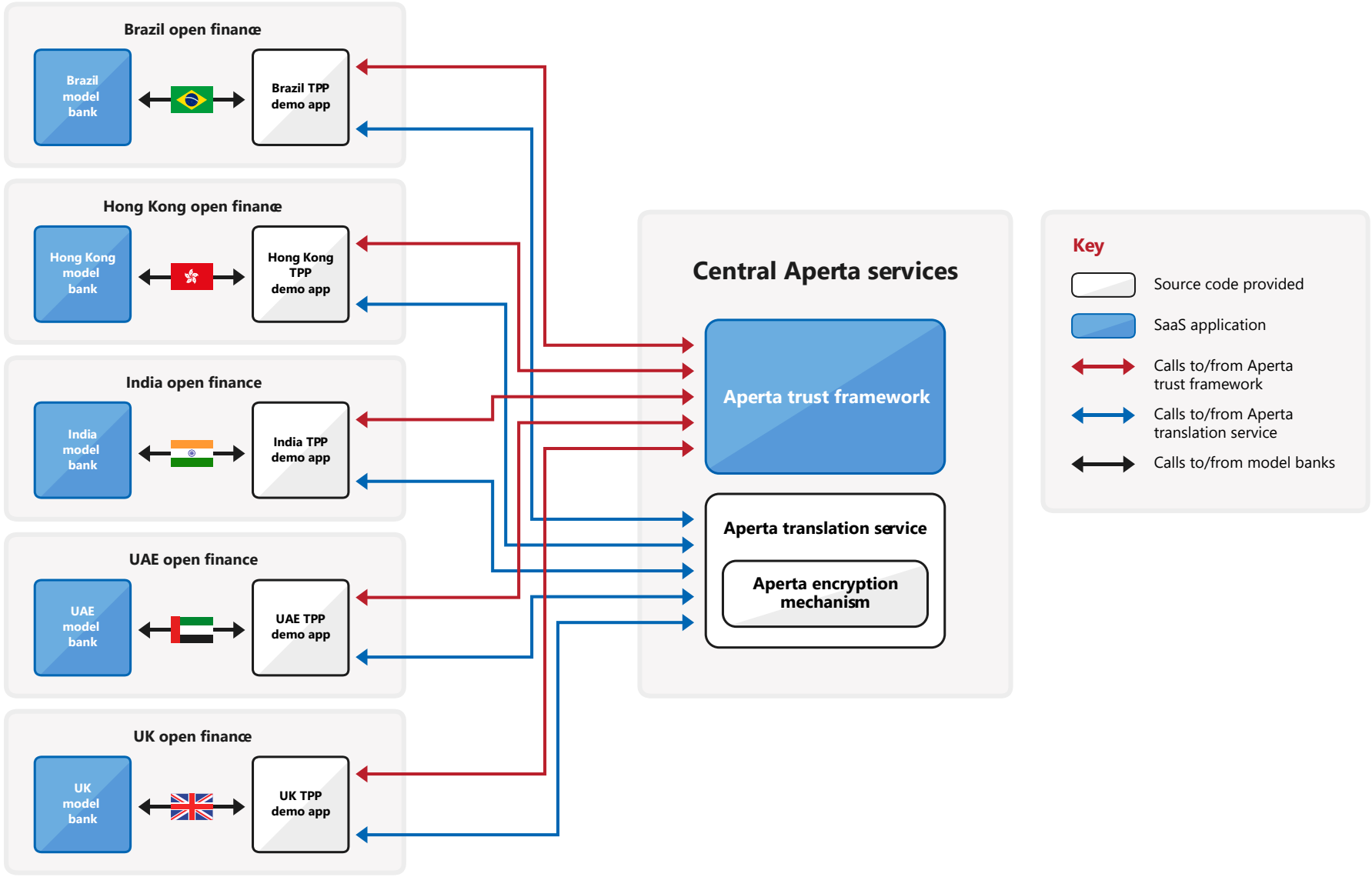
3.5 Reuseable artefacts

Project Aperta made a deliberate choice to build on open standards and construct the prototype as a public good to encourage other network participants to learn and build similar prototypes for their own solutions. Project Aperta's standards, protocols and blueprints are designed as reusable, non proprietary assets that any jurisdiction or provider could use these artefacts as a foundation to further development or adoption. See Appendix B for more detail.

Project Aperta's reusable artefacts come in three forms:

- **documentation and designs**, ie the requirements, architectural options, solution designs and technical architectures for both Option 3 (Centralised aggregator of TPPs and trust frameworks) and Option 4 (Federated trust with OIDC Federation);
- **reusable technical frameworks**, ie the trust framework and security model architecture, API translation specifications and reference source code for the two SME use cases, including mapping approach and common data model guidance; and
- **prototype assets for future reuse**, ie the translation capability, reference source code and API specifications for the two use cases, along with five model banks, test apps, synthetic data and guidelines to replicate Aperta with any API hub and trust framework provider. This capability is supported by a developer portal containing API documentation, usage manuals, sample payloads, downloads and test collections that can be replicated or adapted by other initiatives, as depicted in Figure 14.

Figure 14: The reusable artefacts of Project Aperta live beyond the technical proof of concept



4. Outcomes

4.1 Simplifying the complexities of cross-border data flow

Project Aperta's prototype was intended to test feasibility rather than serve as a final solution but it demonstrated a novel way to materially reduce cross-border SME friction, particularly duplication in verification and manual handling of trade documents. TPPs were able to exchange financial data and trade documents via standardised APIs and a central trust framework that validated participant identity, ensured secure connectivity and performed real-time translation between domestic data formats, all while preserving local licensing, governance and supervisory arrangements. For central banks and policymakers, this points to the importance of setting clear interoperability requirements, shared technical protocols and trusted participation rules so that open finance can scale without undermining domestic supervisory control.

Testing confirmed that domestic banks and fintechs already registered in their home open finance networks could connect to Aperta's transnational trust framework with modest integration effort. Beyond planned testing, one bank successfully integrated a blockchain-based trade finance solution directly with Aperta's KYB/KYC capability, using the platform to verify supplier authenticity before loan approval, demonstrating how cross-border trust infrastructure can unlock new commercial applications without requiring comprehensive regulatory harmonisation. Central banks and policymakers may therefore consider how to support cross-border data portability while avoiding fragmented regimes that create uneven access, compliance burdens or market distortions between incumbent institutions and new entrants.

Project Aperta also surfaced structural challenges. Achieving data interoperability required collaborative agreement on a minimum viable data set and dynamic translation between five jurisdictional standards. While technically straightforward, early convergence on common semantic models was crucial to reducing translation complexity and dependency on central services. For testing, the prototype operated with synthetic data, which offset legal and regulatory constraints on cross-border data. Real-world scenarios and deployments with live data would require targeted regulatory adjustments by central banks and policymakers, particularly regarding consent portability, a legal basis for cross-border data-sharing, data controller and processor roles, cross-border liability and supervisory cooperation across several markets.

While the prototype demonstrated the technical feasibility of cross-border payment initiation and liquidity bridging in both trade finance and account opening use cases, practical realisation is limited by jurisdictional scope differences (not all open finance networks include payment initiation); transaction value caps; and the need for robust governance and complaint and dispute resolution arrangements within the operator network.

4.2 Possible roadmap for further development

The mandate of the BISIH is to build technical prototypes and derive insights and learnings from them. All project artefacts will be shared with central banks via BIS Open Tech. This section explores potential future pathways for Project Aperta, outlining how central banks could advance the prototype towards a more refined architecture to increase adoption or transition it into a production-ready solution.

Project Aperta's modular prototype architecture and use case-agnostic design position it as a foundation for a wide range of cross-border applications beyond the initial SME account opening and trade finance flows. Potential candidates could include cross-border exchange of credit data to support better risk assessment for cross-border customers; integration with digital public infrastructures such as instant payment networks, digital identity networks or customs and trade documentation

platforms; and application to other smart data sectors, such as telecommunications, energy, health or property.

While the prototype demonstrates technical feasibility, a live multi-jurisdictional deployment may require architectural adjustments and an incremental implementation pathway. Lessons from other cross-border interoperability initiatives, including Project Nexus, suggest that technical interoperability alone is not sufficient for large-scale deployment. Sustainable operation may also require a common governance model, legal framework, technical protocols, operating rules and an operational entity responsible for coordinating and managing shared infrastructure across jurisdictions.

A governance model should consider transparency; accountability; and balanced representation of jurisdictional, institutional and user interests; and establish clear policies for participant onboarding, technical protocols, data protection, dispute resolution, incident management and the ongoing evolution of the network. Moving beyond a prototype would also be likely to require identification of a responsible operating entity and associated governance arrangements to support ongoing network management and coordination across participating jurisdictions.

Project Aperta's extensibility also depends on strategic choices about governance, ownership and funding for any future networks, as well as the identification of an Aperta network operator. Similar to the evolution of other multilateral interoperability initiatives such as Project Nexus, a future Aperta network operator could potentially coordinate participant onboarding and accreditation, certificate and trust infrastructure management, incident and dispute handling, funding and cost recovery arrangements, and coordination with supervisory authorities. Potential operating models may range from central bank- or regulator-led arrangements to industry consortia or commercial operators.

Rather than attempting immediate broad participation, an initial deployment could potentially begin with a small coalition of jurisdictions with open finance ecosystems and overlapping policy objectives. A limited group of participating central banks and authorities could enable a test under realistic operating conditions while limiting coordination complexity, with tests focusing on use cases closely aligned with central bank and regulatory mandates.

Insights from Project Aperta and this report could help participating jurisdictions to identify practical areas requiring further work, including cross-border legal recognition of TPPs, liability framework, supervisory coordination, trust and certificate management, and data governance requirements. The findings may also help to inform decisions regarding the degree of harmonisation needed between jurisdictions and where interoperability mechanisms can reduce reliance on broad regulatory convergence.

Recent multilateral initiatives, including World Trade Organization (WTO) members progressing a joint implementation pathway for the E-Commerce Agreement, reinforce the shift towards harmonised, standards-based cross-border digital frameworks and highlight the critical role of governance and network operator models in enabling scalable deployment.[38]

Other exploratory considerations

Near-term exploratory considerations could include the following:

- expanding and enabling the prototype for other open finance use cases, such as retail customer services; cross-border lending and credit assessment; multi-jurisdiction reporting and SME treasury, supply chain finance and working capital solutions;
- designing and testing an international confirmation of payee service using Aperta to strengthen cross-border payment assurance and fraud prevention;
- joint work with standard-setting bodies and regulators to define sector-specific legal and data governance requirements, including roles and liabilities; redress mechanisms and alignment with ICC DSI, SWIFT trade APIs, digital identity standards and LEIs;
- developing and evaluating governance models and funding options with potential network operators, central banks, regulators, regional institutions, industry consortia and commercial providers,

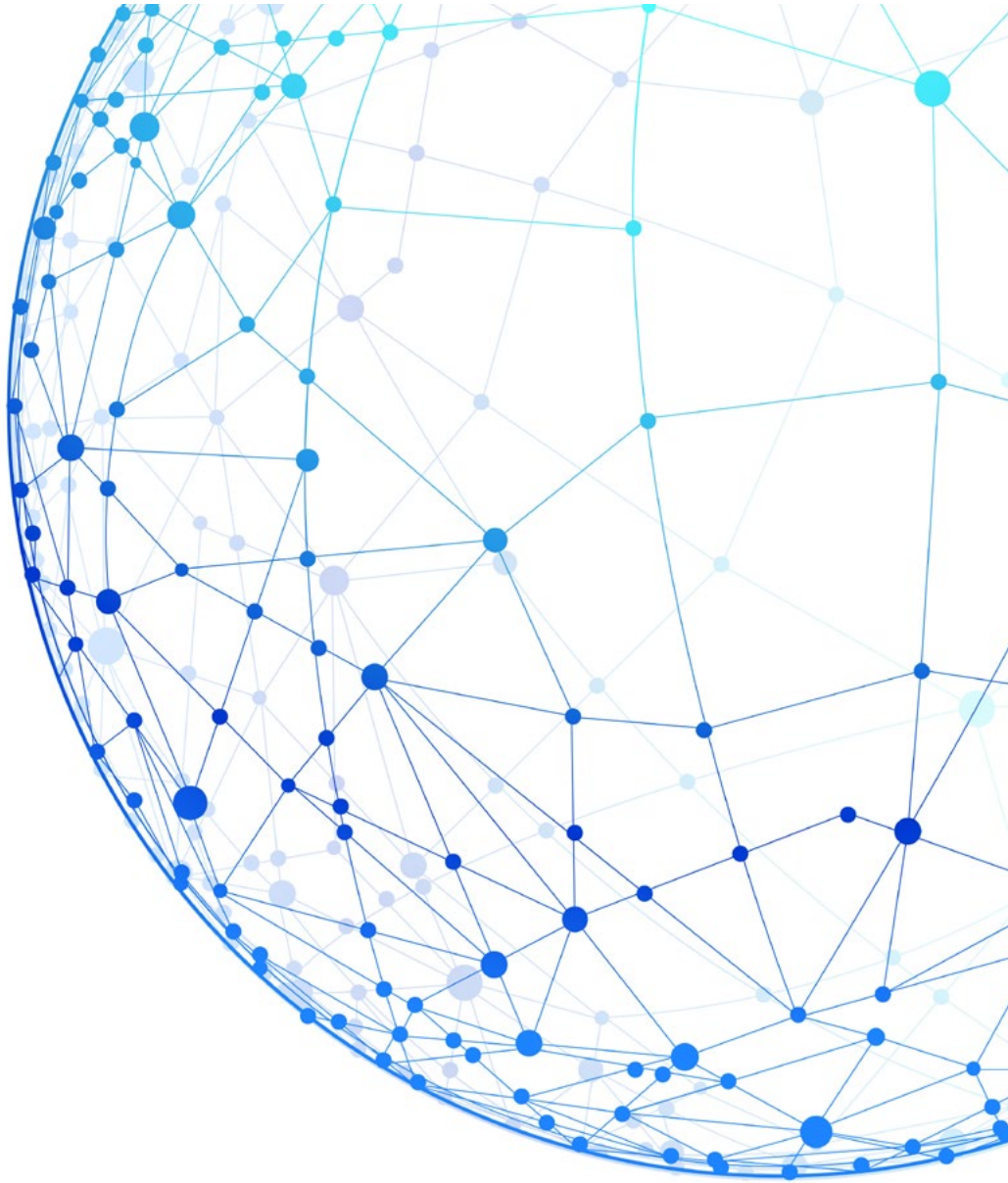
including policies for onboarding, technical standards, data protection and incident management;

- initiating a federated trust model pilot with a coalition of advanced open finance jurisdictions, using Option 4 as the technical baseline, to validate operational feasibility and quantify benefits from reduced central translation and stronger convergence on global standards; and
- automating Aperta services with agentic AI, eg to detect changes in API standards and adapt the translation service, onboard new jurisdictions by automating inclusion in the Aperta data translation protocol, and update specifications and related documentation.[39]

Medium- to longer-term exploratory considerations could include:

- extending Aperta to support tokenised finance and digital asset networks by enabling cross-border exchange of verified legal entity and account data between FIs, digital asset platforms and supervisors;
- applying the architecture to additional complex, document-heavy institutional workflows such as guarantees, trade documentation and cross-border insurance underwriting as jurisdictions broaden open finance scope to relevant data and participants; and
- using these deployments to build a scalable, interoperable foundation for global data portability, fostering competition and innovation while maintaining robust safeguards for transparency, accountability and user protection. Achieving cross-border data portability would require regulatory consideration regarding data localisation and sovereignty as well as data translation and/or harmonisation.

The BISIH welcomes feedback on the findings, design choices and outcomes set out in this report and remains committed to supporting international efforts to enhance cross-border data portability; reduce barriers to SME finance and trade; and promote inclusive, interoperable digital financial infrastructure.



Contributors and acknowledgments

Project participants

Bank for International Settlements (BIS)

Benedicte Nolens (Centre Head, BIS Innovation Hub Hong Kong Centre)

Hakan Eroglu (Project and Open Finance Lead, Technical Adviser and Author, BIS Innovation Hub Hong Kong Centre)

Jack Lee (Project Adviser, Co-Author, BIS Innovation Hub Hong Kong Centre)

Andrew Chau Chun Sing (Technical Advisor, BIS Innovation Hub Hong Kong Centre)

Italo Borssatto (Technical Advisor, BIS Innovation Hub Hong Kong Centre)

Hong Kong Monetary Authority (HKMA)

Terry Chan (Fintech Director, Fintech Facilitation Office)

Ada Kwok (Associate Fintech Director, Fintech Facilitation Office)

Sue Wong (Associate Fintech Director, Fintech Facilitation Office)

Central Bank of the United Arab Emirates (CBUAE)

Paul Kayrouz (Chief Fintech Officer)

Jonathan Holman (Head of UAE Open Finance and CEO of Nebras Open Finance LLC)

Central Bank of Brazil (BCB)

Matheus Rauber (Head of Open Finance)

Veruska Rocha de Aragao (IT Senior Advisor)

Financial Conduct Authority of the United Kingdom (FCA)

Simone Plances (Manager, Smart Data Accelerator)

Ekaterina Borisova (Technical Specialist, Smart Data Accelerator)

Global Legal Entity Identifier Foundation (GLEIF)

Alexandre Kech (Chief Executive Officer)

Xue Tan (Head of Business Development for Asia)

Nuria Vegas (Head of Business Development for LATAM)

Yanzhao Zhang (Country Representative for China)

International Chamber of Commerce Digital Standards Initiative (ICC DSI)

Pamela Mar (Managing Director, Digital Standards Initiative)

Oswald Kuyler (Advisor, Digital Standards Initiative)

Hong Kong University Standard Chartered Foundation FinTech Academy (HKU)

Douglas Arner (Professor, HKU / Cambridge Centre for Alternative Finance / Queen Mary University of London)

Wenglu Wang (Research Fellow, Centre for Banking and Finance Law, National University of Singapore)

Project observing members (in alphabetical order)

Australian Treasury

Bangko Sentral ng Pilipinas (BSP)

Bank of Thailand (BOT)

Berlin Group

European Third Party Providers Association (ETPPA)

Korea Financial Telecommunications & Clearings Institute (KFTC)

National Bank of Georgia (NBG)

Norges Bank

Open Banking Limited (UK)

Open Finance Association (OFA)

OpenID Foundation (OIDF)

Reserve Bank of India (RBI)

Sahamati

Sveriges Riksbank

Swift

World Economic Forum (WEF)

and others...

Acknowledgments

The authors are grateful to Tommaso Mancini-Griffoli (Global Head, BISIH), Karmela Holtgreve (Deputy Head, BISIH), Miguel Diaz (Deputy Head, BISIH), Beju Shah (Centre Head, BISIH Toronto Centre), Balu Babu (Adviser, BISIH Singapore Centre) and Henry Holden (Adviser, BISIH Swiss Centre) for reviewing the report and their insightful feedback, and to Oscar Borgogno (Senior Policy Officer, Bank of Italy) for his invaluable feedback to the report.

Appendices

A. Technology design principles and decisions

Project Aperta developed a detailed solution design for Option 3. The functionality, capabilities and architecture were designed around principles that directly reflect its mandate to deliver a practical, usable cross-border open finance prototype (see Box 5).

Aperta infrastructure

Within the Project Aperta prototype, organisations would be required to register under the Aperta trust framework and to comply with applicable licensing requirements set by regulators in their domestic jurisdictions. The Aperta prototype combines trust and security services with data translation, encryption and routing services so that participants in different jurisdictions can securely discover each other and authenticate and exchange data in a controlled test environment while continuing to use their domestic standards (see Figure 15). The platform acts as a trust anchor that two parties – eg a fintech application and a bank – can each use to establish trust between themselves. The prototype includes:

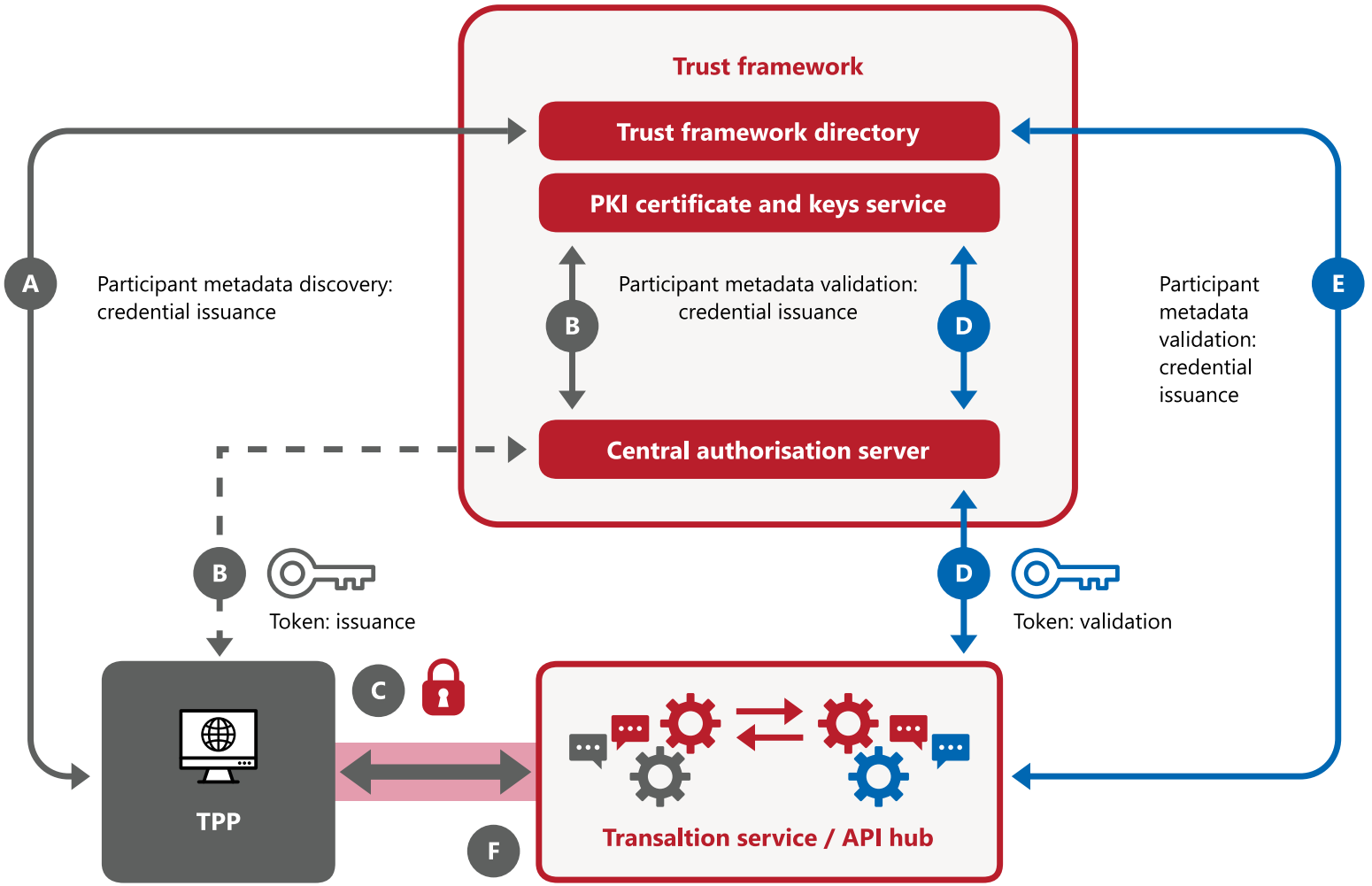
- **a trust framework directory** for participant discovery and registration;
- **PKI** for certificate and key management;
- **a central authorisation server** for authentication and access token issuance;
- **translation and routing services (API hub)** for interoperability between domestic APIs, with case management workflow support; and
- **demo banks and TPP applications** to support end-to-end testing.

Box 5: Design principles

Aperta developed in accordance with the following principles:

- **Build on existing domestic open finance**, adding only what is necessary for cross-border interoperability: This enables prototype feasibility within current regulatory and technical constraints and grounds the prototype in real-world SME journeys rather than a purely academic environment.
- **Use open, widely adopted standards wherever possible:** This avoids lock-in and eases adoption. From the outset, the prototype functions both as a working system for SME account opening and trade finance and as a template that potential network operators can adopt or adapt.
- **Centralise trust and discovery and decentralise value delivery**, leaving account servicing, customer relationships and data provision with domestic institutions: This principle reflects Project Aperta's role as a neutral convener, strengthens cross-border trust and security and keeps competitive and customer-facing activity within national frameworks.
- **Minimise change and complexity for participants** so that TPPs may continue using local APIs and security profiles, with Aperta performing cross-jurisdiction routing, encryption and translation: This simplifies adoption, supports inclusion of less-resourced participants and increases chances of moving beyond proof of concept.
- **Prioritise security, consent and data minimisation**, applying strong security profiles, PKI and explicit consent and treating regulatory gaps as design inputs rather than constraints: This demonstrates feasibility without compromising privacy, financial integrity or supervisory expectations.
- **Enable an extensible path to future federation**, designing for scalability so the prototype and initial use case architecture can support additional jurisdictions, use cases and products without major redesign: This aligns with Aperta's ambition to inform globally scalable, decentralised open finance infrastructure and/or incorporation of other sectors.

Figure 15: Conceptual overview of design components



Trust framework directory:
Provides a registry of authorised TPPs, their scope and their products within the network.

Trust framework PKI certificate and keys service:
Provides a centralised PKI for issuing, validating, and revoking certificates and keys.

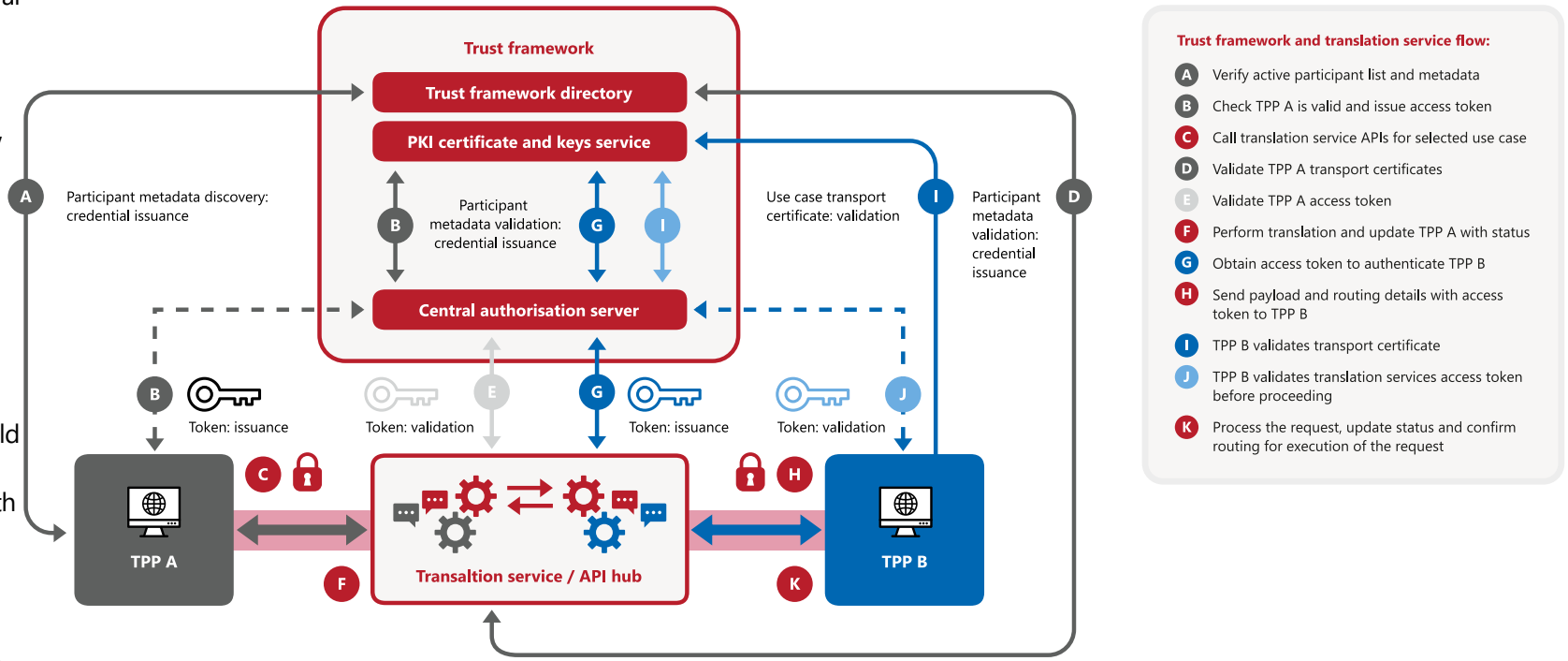
Central authorisation server:
Issues access tokens and authenticates all participants; enables discovery of TPPs connected by aggregators.

Translation services/API hub:
Translates and routes messages from one standard to another via Aperta APIs for execution; case management.

Architecture approach

The prototype operates a single central trust framework directory and PKI, which technically federate with domestic networks using open standards rather than replacing them, as well as a central translation service (see Figure 16). This approach allows Aperta to provide one authoritative layer for discovery, certificate management and access tokens, simplifying cross-border interoperability while preserving local trust architectures. As a result, the design indicates that jurisdictions could connect their existing open finance networks to the Aperta prototype with limited technical changes, subject to regulatory requirements.

Figure 16: Conceptual overview of trust architecture



Trust framework

The trust framework is grounded in the OIDC Federation principles and facilitates secure data-sharing between TPPs registered with Aperta.[40] No consumer data pass through the trust framework, which consists of the following:

- **A trust framework directory** acts as the authoritative registry to enable discovery of all connected participants (and in the case of an aggregator, the banks and third parties it supports), including the services offered by each and how to reach them securely (see Box 6). It enables integration with domestic trust frameworks using identifiers such as local company numbers or LEIs, with API-based automated onboarding, offboarding and synchronisation with the underlying jurisdictional organisation list.
- **A PKI certificate and key service** issues and manages the digital certificates and cryptographic keys used to encrypt data and verify identities, allowing participants to authenticate each other securely. Participants can continue using their existing domestic certificates. Aperta's PKI complements these by providing an additional shared trust layer, issuing and managing the certificates required for secure communication (transport, signing and encryption) in all Aperta interactions.
- **A central authorisation server**, which is a central login and access control, checks who is calling an API, issues tokens (digital passes) and makes sure only authorised parties can access data. Centralisation eliminates the need for each participant to use its own authorisation server, reducing redundancy and complexity.

Cross-border interaction flow

When a TPP in one jurisdiction needs to call an API exposed by a participant in another jurisdiction, the interaction proceeds as follows:

1. The initiating provider discovers the counterparty through the trust framework directory APIs.
2. It requests a sender-constrained access token from the central authorisation server.
3. The provider sends a signed and encrypted request through Aperta's translation and routing services.
4. Aperta validates the request and forwards it to the destination participant for execution.

This model demonstrates a potential approach for heterogeneous domestic trust frameworks to interoperate through a single set of discovery, registration, token and certificate services built on Open Authorisation 2 (OAuth 2.0), OIDF FAPI 2.0 and X.509 standards.[41]

Interoperability and data services

The central Aperta translation service (API hub) provides routing and standards translation between the five jurisdictional APIs – and a set of Aperta-specific internal APIs for the two use cases – so participants can speak their native standards while still interoperating cross-border. The API hub uses the Aperta data translation protocol to translate from the source jurisdiction data standard into the Aperta-specific internal API specification (see Figure 17). These data are moved across borders between the Aperta APIs before being translated into the destination jurisdiction data standard.

- **The API hub** is an API gateway specialised for open banking and open finance use cases. It routes based on jurisdiction and provider identifiers, forwarding calls to the target TPP. It keeps audit trails of translation operations without storing underlying business data longer than necessary.
- **The translation service** exposes Aperta-specific internal APIs (one per use case) and receives requests from TPPs in their local format, authenticated and authorised via the central trust framework. Using the Aperta data translation protocol logic, it transforms the message payloads between source and destination jurisdictions' API formats for execution, including field renaming and data transformation.

The API hub and translation service largely operate in a stateless mode, with most features operating as passthrough services in reflection of the function of REST APIs and in order to avoid repeated token verification. The main exception is case management for long-running processes, which tracks progress, manages tasks and resolves issues as the use case flows happen.

Box 6: The role of metadata in Aperta's network of networks

Aperta is designed to complement and enable a cross-border extension for local jurisdictions, not replace underlying domestic TPPs. A TPP could be a bank (directly registered with Aperta as a TPP), an aggregator (a special type of TPP which offers one-to-many connectivity to multiple domestic banks) or a fintech such as a trade finance solution provider.

Metadata makes it possible for additional information to be stored against each TPP's registration within the central trust framework directory. This metadata enables third parties that operate as aggregators to register the list of banks and third parties they support.

When an end user selects a particular bank that they wish to use as the source of their existing account information, the metadata is queried and a list of all aggregators who support that bank is returned, along with the bank itself, if also directly registered as a TPP with Aperta. The user can then select which TPP they wish to use to access the bank. For example, if a bank is supported by aggregator A and aggregator B, as well as directly registered as a TPP itself with Aperta, the end user can select from a list of aggregator A, aggregator B and the bank itself to choose the party through which they prefer to connect.

Translation architecture and approach

The API hub remains data-agnostic, using API descriptions as the source of truth to enable run time translation between different API standards.[42] The team created the Aperta data translation protocol through collaborative data workshops to harmonise the jurisdictional open finance API formats, as well as commonly used standards such as SWIFT-ICC trade finance API definitions, following project steering committee guidance (see Figure 17). This created JSON "mapping documents", which specify translation source and target data fields, and a converter function for data type or semantic transformations (see Figure 18). Only data provided in one jurisdiction's standard can be mapped to another via the Aperta translation protocol. The Aperta service does not generate or add any data that are not already present.

The mapping documents are validated against JSON Schema, a rule set that defines the structure of the data; they are then compiled into TypeScript libraries, a typed version of JavaScript that helps to make the code safer and easier to maintain; and these libraries run as Express middleware, meaning they sit in the middle of the API request flow and process requests before they reach the final service. This design choice makes the translation layer transparent, testable and maintainable. The open standard JSONPath was chosen as the core expression language to embed the translation mapping logic, and it fits naturally with the JSON-based APIs and the TypeScript/Node network used by the API hub.

Figure 17: Developing the Aperta data translation protocol

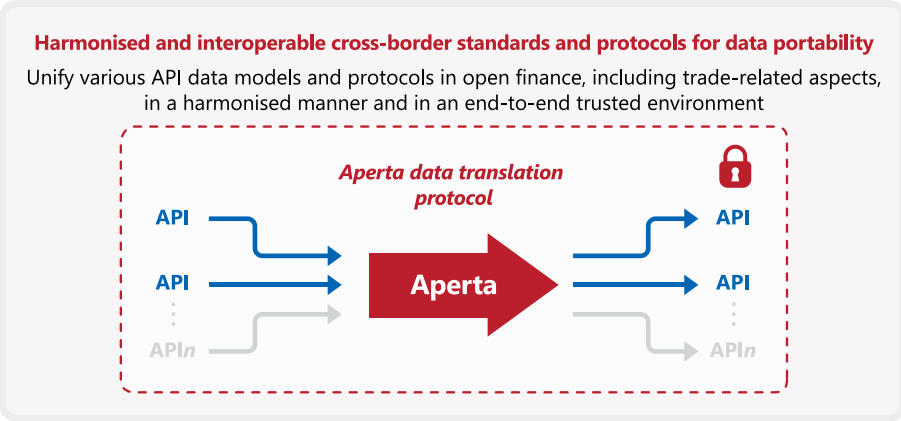
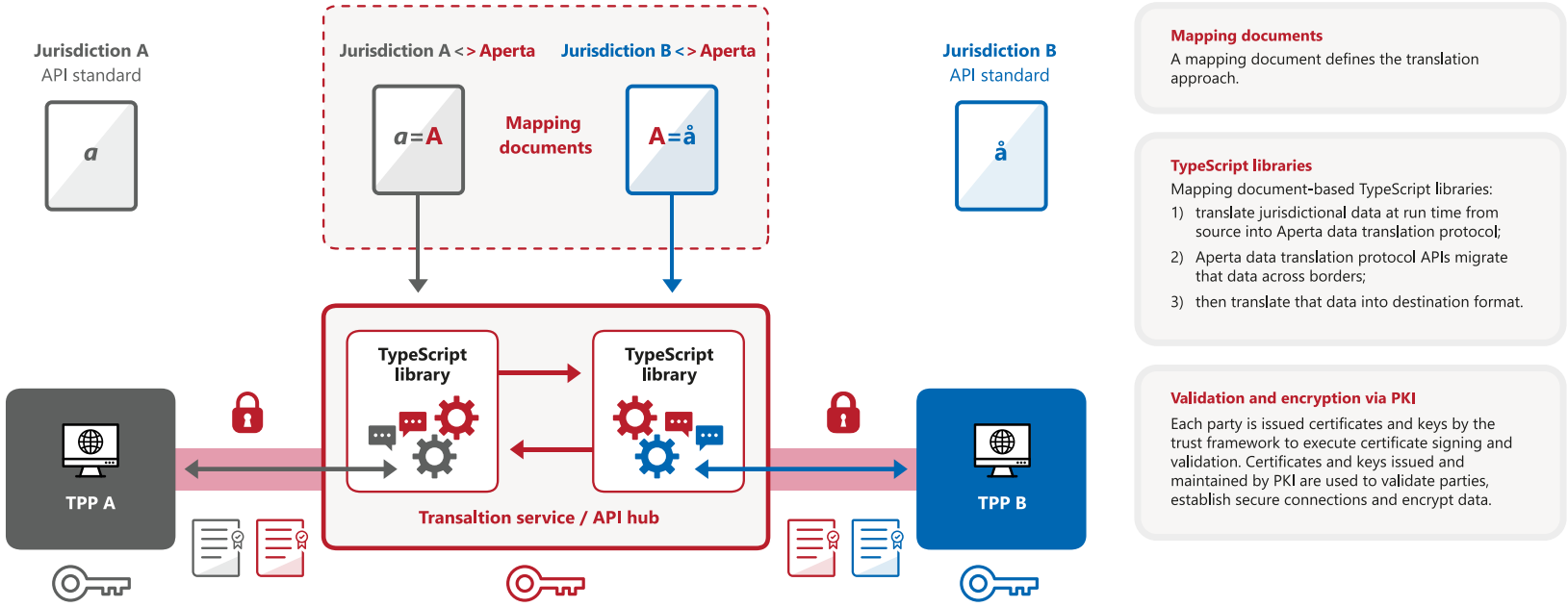


Figure 18: Translation architecture



Security architecture

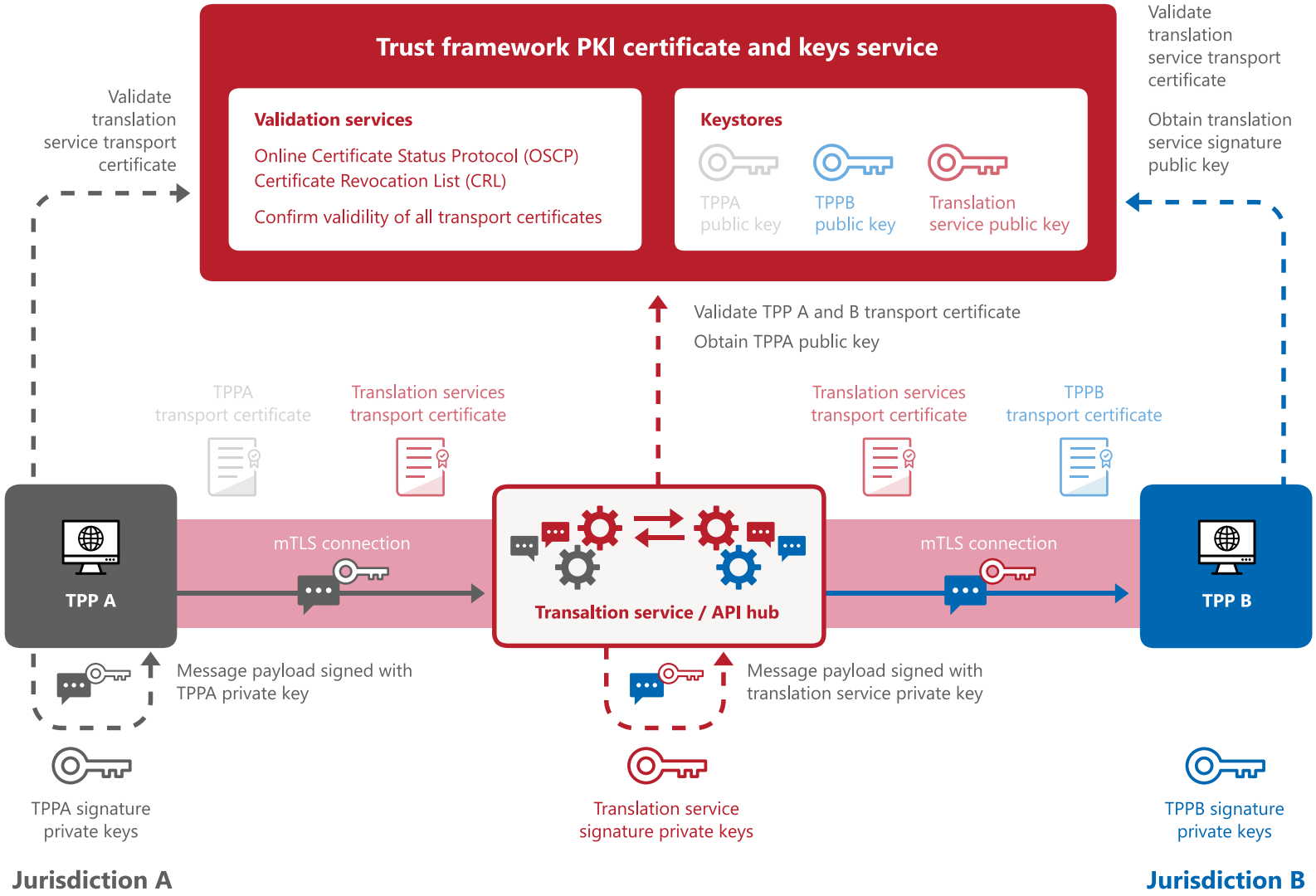
The Aperta prototype is designed to incorporate identity assurance, strong authentication, least-privilege authorisation, encryption, integrity and traceability by design, combining transport-level protection, message level assurance and strict identity governance (see Figure 19). A layered security model is common to both the centralised Option 3 prototype and the federated Option 4, with differences mainly in the locations of trust and enforcement.

Data encryption and security
Mutual transport layer encryption and message-level signatures work together to ensure confidentiality, authenticity, integrity, and non-repudiation of data exchanges.

Transport encryption with TLS
Communication occurs over mutual transport layer security (mTLS) sessions. Both parties validate each other's identity using certificates issued by the Aperta's PKI before exchanging data.

Message signatures
Signatures guarantee that messages are authentic, unaltered and originate from the source. Each participant signs messages with their private key; the recipient uses the corresponding public key from Aperta's keystore to validate the message.

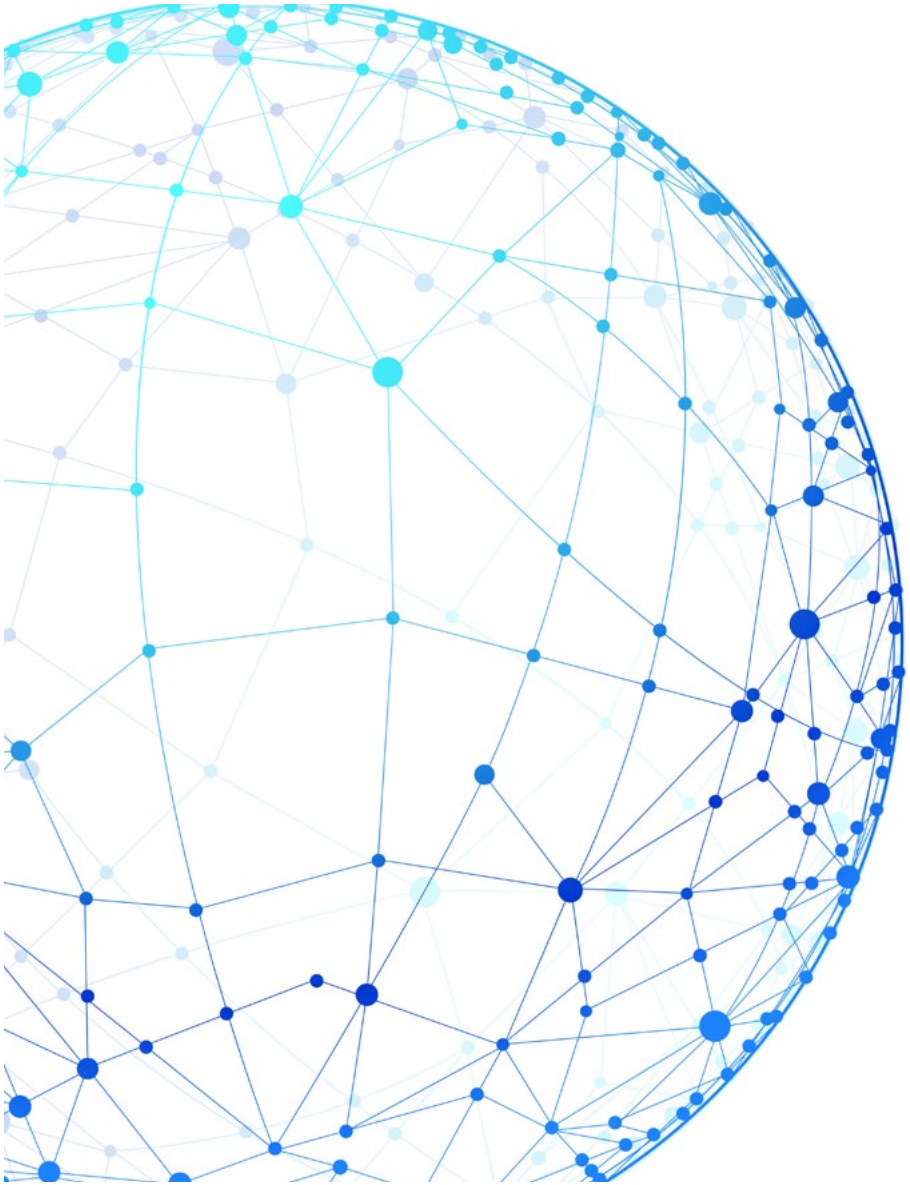
Figure 19: Aperta's security architecture



Box 7: Security considerations for a cross-border infrastructure like Aperta

Aperta's security considerations include the following:

- establish a **single, authoritative cross-border trust framework** to register participants, applications and APIs, with clear roles and permissions that are recognised consistently across all jurisdictions;
- implement a **coherent, governance rich PKI model for transport certificates,** favouring a centrally operated root (or tightly governed federated roots) to avoid fragmented certificate authority (CA) landscapes and ensure predictable certificate issuance, validation and revocation;
- mandate **strong, standardised machine-to-machine authentication and authorisation** (mTLS, asymmetric client credentials, sender constrained tokens under a FAPI aligned profile) so that access decisions are enforced uniformly irrespective of local implementations;
- require **end-to-end confidentiality, integrity and non-repudiation** for sensitive messages, combining TLS with signed (JWS) and, where appropriate, encrypted (JWE) payloads so that intermediaries can route without accessing SME data;
- ensure **comprehensive, tamper-resistant audit trails and operational monitoring** across trust, PKI, authorisation and translation components, enabling supervisors to reconstruct cross-border flows and investigate incidents without centralising underlying business data; and
- **govern security policy at network level** (cryptography baselines, onboarding criteria, incident handling, minimum domestic controls) to prevent weaker national practices from undermining overall cross-border resilience, with arrangements that are compatible with both centralised and federated architectures.



The Aperta security profile secures machine-to-machine communication between network participants using a resource server-focused OAuth 2.0 with a resource server-focused design, "resource server" meaning the API server that handles authenticated requests after an access token has been obtained (see Box 7). It aligns with the FAPI 2.0 Security Profile, a widely accepted security standard for open finance.[43] Aperta adopts FAPI 2.0 as the underlying profile in order to leverage an industry-accepted pattern already used in multiple open finance deployments and to avoid custom security designs in each jurisdiction.[44] Encryption relies on mutual transport layer encryption (mTLS), which authenticates both parties, and message-level signatures to protect data both in transit and at message level, while remaining adaptable to different regulatory environments.

Identity, PKI and certificates

TPP, application and API identities are maintained in the Aperta trust framework's registry of organisations, their roles and their client/software identifiers. A dedicated Aperta PKI issues and manages X.509 certificates for mTLS, while participants supply their own signing and encryption keys. This provides a single cryptographic trust anchor in the centralised model (Option 3); in a federated architecture (Option 4) equivalent trust chains are established through OIDC Federation entity statements and signed metadata instead of a single certificate authority (see Box 7).

Authentication, authorisation and access control

All machine-to-machine calls are authenticated using mTLS plus OAuth 2.0 private key web tokens, with a central authorisation server issuing short-lived, sender-constrained access tokens to prove ownership, aligned to FAPI 2.0. Resource servers rely on token verification, scopes and certificate thumbprints for fine grained authorisation decisions, ensuring that access rights are centrally governed yet locally enforced. In the federated model (Option 4), the same pattern applies but client registration and trust are distributed via federation trust chains, not a single central server, increasing autonomy while retaining strong assurance.

Encryption, integrity and non-repudiation

Data in transit are protected with transport layer security (TLS) using Aperta-issued transport certificates. Where end-to-end confidentiality is required as messages traverse the central translation service, JSON web encryption (JWE) is applied. JSON web signatures (JWS) secure payloads and support non-repudiation with verification keys obtained from Aperta's PKI, enabling central components to route and audit flows without inspecting sensitive business data within the API.

Auditability, monitoring and operational security

Alongside standard cloud infrastructure controls for high availability, redundancy and threat protection, the trust framework components generate comprehensive audit trails for registration, certificate life cycle operations, token events and translation activity, supporting supervisory review, incident investigation and operational monitoring. In a federated model (Option 4), equivalent logs are distributed but linked via common identifiers and federation policies, enabling reconstruction of cross-border transaction chains without centralised data storage and ensuring end-to-end auditability across jurisdictions.

Capturing consent

Obtaining SME/user consent for a service is a mandatory requirement for open finance. Aperta's role is to connect TPPs across jurisdictions while minimising impact on existing open finance; therefore, Aperta acts as a data processor, not a data controller, when providing this technical infrastructure to TPPs.

Because of this, and to enable a seamless customer experience that users are familiar with, the user only needs to grant consent via the TPP (or bank acting as a TPP) in their own jurisdiction, not to Aperta. The consent itself does not flow through Aperta at all, only the data which are shared between TPPs across jurisdictions.

At a high level, consent builds on existing open finance consent flows in each jurisdiction, but the way consent is "projected" across borders differs materially between the prototype's centralised trust and translation model (Option 3) and a federated trust model (Option 4).

How consent works in Option 3 (Centralised aggregator of TPPs and trust frameworks)

In Option 3, users grant consent within their domestic network. The local TPP (or aggregator, if operating as one) obtains and manages consent with the user's FI exactly as is done today, with familiar domestic user experience patterns (redirect, delegated, decoupled or embedded) as outlined in the local open banking or open finance standards.[45] They create a domestic consent object and receive an access token bound to that consent.

Aperta then acts purely as a cross-border data processor and translator: it never becomes a consent authority, and no new "Aperta consent" is created. In the cross-border account opening use case, for example, user A in jurisdiction A gives consent to TPP A to share data from bank A with TPP B abroad; TPP A retrieves the data under that domestic consent and passes only the data through Aperta to TPP B, with Aperta translating formats on the way. The consent record, lifecycle (extension, revocation, expiry) and liability remain within the domestic context (between user, TPP and bank) in order to avoid changing any jurisdiction's consent model and maximise feasibility for the prototype.

For the trade finance use case, where no domestic open finance API exists yet for the required artefacts, Aperta defines a new, generic consent model in the API specification, but still applies the same principle: consent is captured by the TPPs in each jurisdiction and includes permission to share specific documents cross-border via Aperta. Here, the key choice is to design a minimal, cross-jurisdiction consent schema tailored to trade artefacts while keeping Aperta in a processor role, not as an identity or consent authority.

How consent works in Option 4 (Federated trust with OIDC Federation)

In Option 4, consent is still granted by users to TPPs and banks, but it is anchored in a fully federated trust and discovery layer rather than in a central translation hub. OIDC Federation provides common mechanisms for dynamic registration, metadata discovery and policy so that a TPP in jurisdiction A can directly present its identity and authorisation request to a bank or data holder in jurisdiction B under a shared federation policy.[46]

In this model, consent objects and authorisation requests are explicitly portable across borders: a TPP's client and their policies are recognised across the network through federation metadata, and domestic network components implement common security and consent profiles (see Figure 20). This places a heavier responsibility on jurisdictions' domestic networks, as it requires upgrading to common federation and consent semantics, agreement of cross-jurisdiction consent models and treatment of the federated network (rather than Aperta alone) as the trust anchor shaping who is permitted to request – and act on – consent. This elevates the ambition of Project Aperta from "bridge domestic consents via a processor" to "align domestic consent and security so that cross-border consent is natively understood at each endpoint" and would come with far greater impact on and required harmonisation between participating jurisdictions.

Figure 20: Comparison of consent models for Options 3 and 4

Element	Option 3 - Centralised aggregator of TPPs and trust frameworks	Option 4 - Federated trust with OIDC Federation
User consent journey	User follows a familiar, purely domestic consent flow with their local TPP/bank; no new "Aperta consent" screens.	User provides consent via local TPP/bank, but flows need to incorporate common federation/consent semantics; may differ from today in some markets.
Number of consents user must manage	One domestic consent per data-sharing relationship; cross-border use is implicit in that consent.	One; however users may see more standardised consent language as consent is expected to carry harmonised, network-wide claims.
Cross-border visibility for user	TPP discloses which foreign party will receive data to the user; Aperta remains invisible as a back-end processor/translator.	Federation could enable clearer, standardised naming and certification of foreign parties in the consent user experience, improving cross-border transparency.
Change required to domestic consent stacks	Existing jurisdictional consent models are reused, with minimal Aperta-specific extension needed for trade finance should not cause existing models to fail or behave unexpectedly.	Material upgrades required to adopt common federation, security and consent profiles; higher short-term impact on domestic network.
Legal role of Aperta/network	Aperta acts as a data processor only, routing and translating data under domestic consents; controller obligations remain with local TPPs/banks.	The federated network becomes a shared trust and policy fabric; Aperta (as trust anchor) shapes who may request and act on consent but avoids end user data controller status.
Supervisory and regulatory implications	Easier to fit within current frameworks: regulators can treat cross-border flows as extensions of existing open finance consents plus an additional processor.	Better long-term alignment, but higher regulatory design effort; Raises more structural questions (governance of federation, cross-border recognition of consent semantics, liability allocation).

B. Project Aperta: beyond the technical proof of concept prototype

"Reusable artefacts" in Project Aperta are the artefacts that remain useful after prototype decommissioning and can be reused or extended by future networks, regulators and markets. Project Aperta's requirements, architectures, designs, protocols, source code and blueprints are reusable, non-proprietary assets that any jurisdiction or provider can adopt to create or join interoperable open finance frameworks beyond this prototype.

Documentation and designs

- Requirements analysis document covering use cases, functional/non-functional requirements and jurisdictional analysis
- Solution design description and comparison, including the evaluation of all four architectural options and the selected approach
- Detailed technical architectures for both Option 3 (Centralised aggregator of TPPs and trust frameworks) and Option 4 (Federated trust with OIDC Federation)

Reusable technical frameworks

- Transnational trust framework architecture, protocols, data formats and registry specifications for identifying and managing all participants
- Transnational PKI architecture, certificate profiles and example artefacts to secure transport, signing and encryption across jurisdictions
- API translation specifications and reference source code for the two SME use cases, including mapping approach and common data model guidance
- Consent management architecture and specifications for cross-border, consent-driven data-sharing
- Conceptual encryption and security framework, plus reference source code for the Aperta encryption mechanism

Prototype assets for future reuse

- Configured instances of the trust framework and API hub (with manuals and training material) that can be replicated or adapted by other initiatives
- Five model banks with synthetic data and open finance APIs, plus five demo TPP web apps and their source code
- Developer portal content, ie API documentation, usage manuals, sample payloads, downloads and test collections
- Testing artefacts and research outputs, ie test concepts, scripts, training material and feedback/report contributions, including customer experience insights

The reusable assets are subject to the following caveats:

- **Future evolution of standards and approach upon which Aperta is based:** Both the approach and code have been developed at a particular point in time (2025/26), and developments in standards may either facilitate or negate some of the strategic option choices, eg should broad adoption of OpenID federation occur over the next few years, this would act as an accelerant.
- **Code and prototype artefacts are templates:** Artefacts are delivered to a proof of concept standard; further work would be required to make them production-ready. For example, the user experience design and user interface are designed for testing/simulation, not consumer-facing readiness.
- **Static nature of code:** Code libraries are static and not updated as part of the project.
- **Developing on open source brings benefits and risks:** Developing on open source confers significant advantages, including cost savings; high flexibility; rapid innovation; ready adoption and community-driven, transparent collaboration. Key challenges include a lack of dedicated, formal support; a steep learning curve; potential security vulnerabilities and risks related to maintenance or abandonment of projects.

References

[1] An API is a "set of routines, protocols and tools for building software applications" that provides a standardised interface for secure data exchange between banks and third parties; see Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, November 2019.

[2] Open finance frameworks are the rules, standards, governance arrangements, technical specifications and operating models that define how open finance works in a jurisdiction or market. They are broader than just technology; they can include APIs, consent rules, liability arrangements, accreditation and supervisory requirements. See Financial Stability Institute, Key considerations for open finance – Executive summary, June 2025.

[3] See Cambridge Centre for Alternative Finance (CCAF), The global state of open banking and open finance, November 2024, www.jbs.cam.ac.uk/wp-content/uploads/2024/11/2024-ccaf-the-global-state-of-open-banking-and-open-finance.pdf.

[4] This BIS paper examines international experiences with open finance, shedding light on its impact on competition, market entry and financial access, while discussing the challenges that remain. See H Eroglu, G Cornelli, J Frost, F Rühmann and V Shreeti, "Opening doors to open finance: evidence from the international experience", BIS Papers, no 168, March 2026.

[5] For commentary on reglobalisation and the new imperatives for cross-border trade, see World Economic Forum (WEF), "Reglobalization: Rewiring the world economy for a new era of growth", 12 January 2026, www.weforum.org/stories/2026/01/reglobalization-world-economy-growth/.

[6] The BISIH's Project Nexus aims to connect domestic instant payment systems to improve the speed, cost and transparency of and access to cross-border payments. Similar to Aperta, instead of building custom connections for every new country that it connects to, a payment system operator can make one connection to the Nexus platform. See BIS, Project Nexus: enabling instant cross-border payments, August 2025, www.bis.org/about/bisih/topics/fmis/nexus.htm.

[7] The prototype incorporated India as a test case to highlight Aperta's readiness for high-volume markets. It models interoperability with India's advanced fintech infrastructure, including the Account Aggregator framework. This demonstrates the platform's potential to connect diverse ecosystems, especially given strong remittance and workforce links (such as the 4.3 million (2024) Indian expats in the UAE who drive USD ~26 billion in annual remittances (19.2% of total USD 135.4 billion in FY25) and need seamless access to open bank accounts across borders). See Embassy of India in Abu Dhabi, UAE, "Indian community in UAE", and A Sengupta, "Economic survey 2026: Remittances rise to $73 bln in H1 FY26, account for 3.5% of GDP in FY25", ETBFSI, 29 January 2026.

[8] See World Bank Group, The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of Covid-19, July 2022, which notes that digital financial services and datasharing frameworks expand access to finance for underserved SMEs by lowering costs, enabling innovation at scale and improving credit inclusion.

[9] See N Jentzsch and A Lange, Cross-border credit reporting: aiming for international practices and standards – Exploratory report, World Bank Group, June 2022: "Technology can leapfrog slow regulatory changes (for example, harmonisation) and create legally compliant processes and products. Moreover, open standards for international credit reporting, as well as smart deployment of artificial intelligence, are a route to faster internationalisation of credit reporting."

[10] According to the United Nations Conference on Trade and Development (UNCTAD), two thirds of global trade is carried out via defined corridors, much of which are undergoing reconfiguration as companies broaden their supplier base and shorten supply chains following geopolitical shocks such as Covid, the Ukraine conflict and recent trade policy. UNCTAD has "value chains continue to reconfigure – geopolitics redraws trade and investment maps" as its fourth global trend for 2026. See UNCTAD, "Top trends redefining global trade in 2026", Global Trade Update, January 2026.

[11] Ibid.

[12] Supporting SMEs is vital for a more inclusive global economy. See WEF, "Why supporting SMEs is critical for global trade stability and a more inclusive economy", 16 January 2023, www.weforum.org/agenda/2023/01/why-supporting-smes-is-critical-for-a-global-trade-stability-and-and-a-more-inclusive-economy.

[13] See Organisation for Economic Co-operation and Development, "Trade finance for SMEs in the digital era", OECD SME and Entrepreneurship Papers, no 24, May 2021, which highlights how information asymmetries, fragmented cross-border data and manual processes increase perceived risk, slow onboarding and constrain SME access to finance.

[14] The introduction of Eroglu et al (2026) defines open banking and open finance and discusses the role of APIs.

[15] See Open Banking Limited, OBL Impact Report 7: open banking delivers real-world impact as adoption accelerates year-on-year, May 2025, www.openbanking.org.uk/insights/obl-impact-report-7-open-banking-delivers-real-world-impact-as-adoption-accelerates-year-on-year/.

[16] Ibid.

[17] See Section 2 of Eroglu et al (2026).

[18] See Consumer Financial Protection Bureau, "Required rulemaking on personal financial data rights", www.consumerfinance.gov/personal-financial-data-rights/; of particular interest is the section titled "SBREFA outline of proposals under consideration and panel report", which considers open finance and data access from the perspective of small businesses in the United States.

[19] See CCAF (2024).

[20] See "Comparative snapshot: India's UPI and Brazil's Pix" in CCAF, Digital public infrastructure and digital financial services: convergence, landscape and regulatory considerations, July 2025, pp 32–4, www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/digital-public-infrastructure-and-digital-financial-services/.

[21] BCB maintains statistics on Pix at www.bcb.gov.br/en/financialstability/pixstatistics.

[22] See Australian Competition and Consumer Commission (ACCC), "The Consumer Data Right", www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right.

[23] For documents and information on the UK Data (Use and Access) Act 2025, see UK Government, "Data (Use and Access) Act 2025", July 2025, www.gov.uk/government/collections/data-use-and-access-act-2025.

[24] See Hong Kong Monetary Authority (HKMA), "Strengthening fintech co-operation between the Hong Kong Monetary Authority and the Financial Services Regulatory Authority of Abu Dhabi Global Market", 22 November 2023, www.hkma.gov.hk/eng/news-and-media/press-releases/2023/11/20231122-3/.

[25] A Murray and J Buckenham, "Research note: Open banking and open finance in the UK", Financial Conduct Authority, October 2025.

[31] The BISIH's Project Nexus aims to connect domestic instant payment systems to improve the speed, cost and transparency of and access to cross-border payments. Similar to Aperta, instead of building custom connections for every new country that it connects to, a payment system operator can make one connection to the Nexus platform.

[32] The International Chamber of Commerce Digital Standards Initiative (ICC DSI) aims to accelerate the development of a globally digitalised, interoperable trade environment. It engages the public sector to progress regulatory and institutional reform and mobilises the private sector on standards interoperability, digital trust and accelerated adoption of digital trade globally. See ICC DSI, "The ICC Digital Standards Initiative: Establishing a globally harmonised digital trade environment", www.dsi.iccwbo.org/.

[33] The ICC and SWIFT launched the first API standards for guarantees and standby LCs. See ICC, "ICC and SWIFT unveil first API standards for guarantees and standby letters of credit", 13 August 2023, www.iccwbo.org/news-publications/news/icc-and-swift-unveil-first-api-standards-for-guarantees-and-standby-letters-of-credit/ and SWIFT, "Bank guarantees API".

[34] A joint initiative from the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) and the ICC has created the Cross-Border Paperless Trade Database to track cross-border trade digitalisation. Examples of trust frameworks include private networks such as the Trade Worldwide Information Network (TWIN), in use in Kenya, which uses distributed ledger technology to make global trade efficient. The Global Shipping Business Network (GSBN) is also using PKI in conjunction with blockchain capability to enable interoperability between documentation standards for trade documentation digitisation. See UNESCAP, "Cross-Border Paperless Trade Database", www.digitalizetrade.org/.

[35] TWIN is a private next-generation digital infrastructure powered by IOTA, designed to make global trade more efficient, and it is already used for projects like the Trade Logistics Information Pipeline (TLIP) in Kenya to speed up customs clearance and reduce border delays. See more at www.twin.org/home.

[36] ICC DSI, Digitalising global trade: A roadmap to interoperability and trust at scale, July 2025, Chapter 4.

[37] See OBL, "Customer experience guidelines – Get started", standards.openbanking.org.uk/customer-experience-guidelines/introduction/ and BCB, "Open Finance Brasil – User experience guidelines", www.bcb.gov.br/en/financialstability/openfinanceoverview, which together define an open finance user experience journey as the end-to-end customer flow of authentication, consent capture and authorisation for secure data-sharing between providers using standardised, transparent and user-controlled digital interfaces.

[38] See World Trade Organization (WTO), "Members adopt a pathway to bring E-Commerce Agreement into force via interim arrangements", 28 March 2026, www.wto.org/english/news_e/news26_e/mc14_28mar26_341_e.htm, which notes that 66 WTO members (covering ~70% of global trade) have agreed to implement the E-Commerce Agreement through a structured pathway, reinforcing a shared commitment to a baseline set of global digital trade rules built on internationally recognised standards and frameworks.

[39] Agentic AI with Model Context Protocol (MCP) in open finance enables AI assistants to securely use financial APIs to do multi-step tasks like checking balances, comparing products or initiating payments. The main benefit is that MCP gives the AI a standard way to keep context, chain actions and work across systems more reliably than custom one-off integrations.

[40] A federation is an agreement between parties that trust each other. A federation mechanism is a trust-based framework that allows users to access multiple, distinct third parties, applications or systems with a single set of trusted credentials and extend trust across organisational boundaries. In a multilateral federation, trust can be mediated by a third party (the trust anchor) within a trust framework. This avoids the need for bilateral agreements. See the OpenID Foundation federation specification at www.openid.net/specs/openid-federation-1_0.html.

[41] OpenID Foundation (OIDC Core, FAPI 2.0), IETF (OAuth 2.0/JWT RFCs) and ITU/ISO X.509 standards (openid.net, www.rfc-editor.org, www.itu.int) together define federated trust patterns enabling secure API discovery, sender-constrained access tokens, certificate-based validation and cross-domain authorisation between heterogeneous identity and trust frameworks.

[42] See OpenAPI specifications at www.openapis.org/.

[43] "Resource server" is the OAuth 2.0 term for an API server. The resource server handles authenticated requests after the application has obtained an access token.

[44] The FAPI Working Group is open source and part of OpenID, and the specification and all history of the project can be accessed at www.openid.net/wg/fapi/specifications/.

[45] There are several approaches to this authentication and authorisation flow:

1. redirect, whereby the user is redirected from the TPP's web or mobile application to the bank's existing web or mobile application with which the user is familiar, so the user does not have to access a new website or download a new mobile app;
2. decoupled, whereby the user is redirected from the TPP's web application to the bank's mobile application via (for example) a QR code, allowing the user to authenticate using biometrics in their mobile banking application;
3. delegated, whereby the user remains in the TPP's web or mobile application and uses credentials provided by the TPP to authenticate (this method allows the TPP to control the entire experience and provides the least friction for the user); and
4. embedded, whereby the user remains in the TPP's web or mobile application and uses credentials provided by the bank to authenticate.

[46] OIDC Federation is a framework for establishing trust and enabling secure, short-lived authentication between identity providers and relying parties (apps) without requiring manual, longterm credentials. The documentation is available at www.openid.net/specs/openid-federation-1_0.html.

Project Aperta
Enabling cross-border interconnectivity through open finance interoperability

ISBN 978-92-9259-955-3
bis.org