

▶ Project Nexus

**Enabling instant
cross-border payments**

Conclusions from a collaboration
with Indonesia, Malaysia, the
Philippines, Singapore and Thailand

▶ Project Nexus

Enabling instant cross-border payments



BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA



BANK OF THAILAND

This publication is available at bis.org

Publication date: July 2024

© Bank for International Settlements 2024. All rights reserved. Use of this publication is subject to the terms and conditions of use published on bis.org. Brief excerpts may be reproduced or translated provided the source is stated.

Contents

Executive summary	4	How Nexus works	19	Oversight approach for Nexus	45	Technology for Nexus	59
Benefits of linking instant payment systems	7	Key takeaways	20	Key takeaways	46	Key takeaways	60
Key takeaways	8	Who would use Nexus?	21	Joint Oversight Forum	47	Technology design principles	61
Interlinking instant payment systems (IPS)	11	The user experience when making a payment through Nexus	22	Oversight arrangements and decision-making	48	Communicating with Nexus	63
How Nexus can accelerate the growth of instant cross-border payments	13	Actors in Nexus	27	Oversight of the Nexus Technical Operator	48	Nexus infrastructure models	64
Benefits for the Sender and Recipient	15	Technology components of Nexus	30	The commercial model for Nexus	49	Connecting to Nexus	66
Progress to date	17	How payments are processed through Nexus	31	Key takeaways	50	Annex: The Nexus technical proof-of-concept between the Eurosystem, Malaysia and Singapore	67
		FX provision in Nexus	33	Costs and transparency for the Sender	51	Acknowledgements	70
		Nexus governance and scheme arrangements	35	The proposed fee structure for IPS, PSPs, FXPs and SAPs	53		
		Key takeaways	36	Deciding whether to join Nexus	55		
		The Nexus Scheme Organisation	37	The role of competition in keeping fees low	57		
		The Nexus Scheme rulebook	40	The Nexus Scheme Organisation	58		

Acronyms

Nexus-specific acronyms are bolded.

AML	Anti-money laundering
API	Application programming interface
ASEAN-5	The five partner countries from the Association of Southeast Asian Nations: Indonesia, Malaysia, the Philippines, Singapore and Thailand
B2B	Business-to-business
BIC	Business identifier code
BIS	Bank for International Settlements
BISIH	Bank for International Settlements Innovation Hub
CFM	Capital flow measures
CFT	Countering the financing of terrorism
CLG	Company limited by guarantee

CPMI	Committee on Payments and Market Infrastructures
DNS	Deferred net settlement
EUR	Euro
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FX	Foreign exchange
FXP	Foreign exchange provider
IBAN	International Bank Account Number
IFSC	Indian Financial System Code
IP+	Instant Payments Plus
IPS	Instant payment system
ISO	International Organization for Standardization
ISO 20022	A technical standard for financial messages
JOF	Joint Oversight Forum
JSON	JavaScript Object Notation

NITMX	Thailand's National Interbank Transaction Management and Exchange
NSO	Nexus Scheme Organisation
NTO	Nexus Technical Operator
PDO	Proxy Directory Operator
PFMI	Principles for Financial Market Infrastructures
P2P	Person-to-person
PSP	Payment service provider (used inclusively to refer to banks and non-bank PSPs)
RTGS	Real-time gross settlement
SAP	Settlement Access Provider
SGD	Singapore dollar
TIPS	TARGET Instant Payment Settlement
UN	United Nations
USD	United States dollar

Executive summary

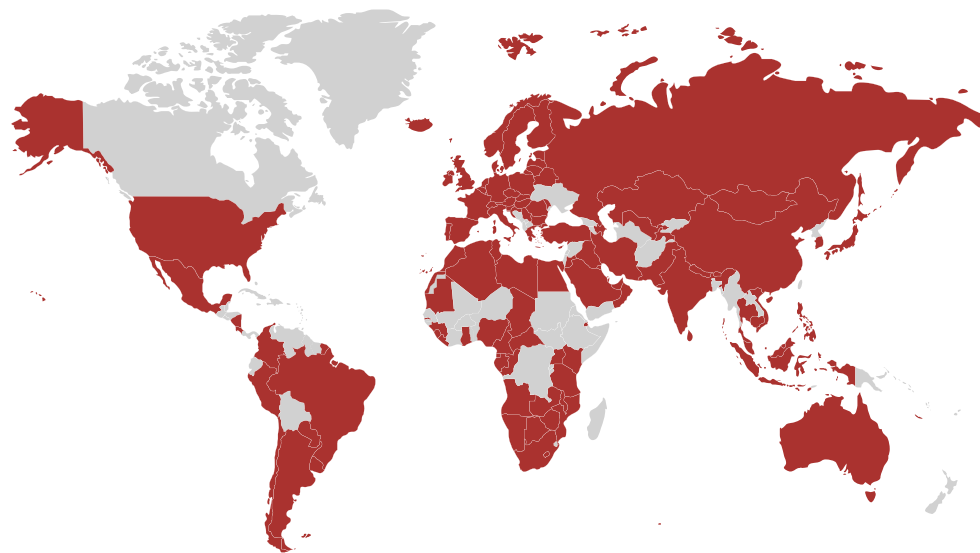
Nexus is a Bank for International Settlements Innovation Hub (BISIH) project that explores how to build on the success of domestic instant payments to improve the speed, cost, transparency and accessibility of cross-border payments.



In over 70 countries today domestic payments reach their destination in seconds at near-zero cost to the Sender or Recipient. This is thanks to the growing availability of **instant payment systems (IPS)**.¹ Connecting these IPS to each other has the potential to enable cross-border payments from Sender to Recipient within 60 seconds (in most cases).



Figure 1: world map with countries with IPS highlighted in red – based on the World Bank's faster payments toolkit



This 'interlinking' of IPS is a priority of the G20 Roadmap for Enhancing Cross-border Payments,² which highlights Project Nexus as a priority action (Action 2(c)) towards achieving the Roadmap's targets for speed, cost, transparency and accessibility.

Interlinking of IPS is already underway. In April 2021, Singapore and Thailand connected their IPS, allowing customers of participating financial institutions to send payments across the border with just the Recipient's phone number.

Since then, several countries in the Southeast Asian region and globally have linked (or are linking) their IPS together. However, connecting countries one-to-one soon becomes complex, since every IPS has different technical standards, business processes and regulatory requirements. Each new bilateral initiative requires a complex technical integration and multi-party legal negotiation.

Project Nexus

Nexus addresses these challenges by making it easier to interlink multiple IPS through a **standardised and multilateral approach**. Each IPS would need to invest time and resources to be able to connect to and communicate with Nexus, but this would be a one-time effort rather than being repeated every time it connects to a new country.

Nexus has been designed with a focus on the needs and user experience of both payers and payees, and evaluated against design principles to ensure that Nexus serves as a public good that should improve the speed, cost, transparency of and access to cross-border payments. (See [Box 4](#)) It has been tested through a successful technical proof of concept that linked test versions of the IPS in the Eurosystem, Malaysia and Singapore.

Building on this work, the BIS Innovation Hub Singapore Centre has spent the last year working with the central banks and IPS operators of Indonesia, Malaysia, the Philippines, Singapore and Thailand ('ASEAN-5')³ to evaluate the model against the reality of their IPS. Most of these countries are pioneers in building bilateral instant

cross-border payment links and now wish to connect all five countries multilaterally. The project team also consulted with central banks, standard-setting bodies, IPS operators and commercial banks from around the world to validate that Nexus is scalable and interoperable with IPS beyond those five countries.

“Nexus has been designed with a focus on the needs and user experience of both payers and payees, and evaluated against design principles to ensure that Nexus serves as a public good that should improve the speed, cost, transparency of and access to cross-border payments.”

This phase of the project set out to:

- develop **governance, scheme and oversight arrangements** that accommodate the regulatory differences between countries while ensuring appropriate risk management, safety, efficiency and resilience for all Nexus payments;
- develop a viable **business and revenue model** for Nexus to ensure financial self-sufficiency and ensure that key industry participants have strong incentives to join Nexus; and
- finalise the Nexus **technology architecture and operational model**, building on the insights from the software developed in the proof of concept.
- This report provides more detail on each of these outputs. Further documentation, including implementation guides for each type of participant in Nexus, is available to central banks and IPS operators on request. As always, the Nexus model is subject to continual improvement over time and feedback is welcome.

Next steps

In the next phase of Nexus, the **BISIH Singapore Centre will support a coalition of countries who are interested to implement Nexus** in the real world and use it to connect their domestic IPS.

The BIS and ASEAN-5 central banks share a desire for any real-world implementation of Nexus to be global rather than regional and will continue to engage more widely with central banks and IPS operators across the world.

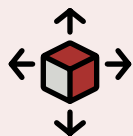
Contact the Nexus team

Central banks and IPS operators interested in connecting to Nexus or using the Nexus blueprint in their other projects can contact the project team at: singapore.centre@bisih.org.

1 Benefits of linking instant payment systems



Key takeaways



Improving cross-border payments

Nexus aims to improve the speed, cost, transparency of and access to cross-border payments. By linking *domestic* instant payment systems (IPS) together, Nexus aims to enable cross-border payments that reach their destination in 60 seconds or less (in most cases).

“Nexus aims to enable cross-border payments that reach their destination in 60 seconds or less.”



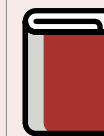
Linking IPS multilaterally

Some countries are already linking their IPS, but the slow and complex process makes scaling a challenge. Linking IPS bilaterally is only commercially viable when connecting close trading partners or strong remittance corridors.



Standardising the scheme

Nexus eases IPS-interlinking by standardising the way that IPS connect to each other. Nexus consists of a payment scheme, supported by software (Nexus Gateways), which allows IPS to communicate using application programming interfaces (APIs) and ISO 20022 messages.



Evaluating the model

Following a successful technical proof of concept that linked test versions of the IPS of the Eurosystem, Malaysia and Singapore, the BIS Innovation Hub Singapore Centre has spent the last year working with the central banks and IPS operators of Indonesia, Malaysia, the Philippines, Singapore and Thailand to evaluate the model against the reality of their IPS.

This work led to the development of a comprehensive scheme and governance framework, commercial model and technology blueprint, which are described in this report.

For many payment Senders, cross-border payments are often slow and expensive, offering a frustrating user experience and imposing significant costs on individuals and businesses.

In some cases, it is not clear to the Sender how long the payment will take, what exchange rate will be applied, or how much money will reach the Recipient after various fees have been deducted.

For banks and non-bank payment service providers (collectively, PSPs), it can be expensive and labour-intensive to provide cross-border payments through traditional channels. They may need to integrate and open accounts with banks in multiple countries (and split their liquidity across multiple currencies) or rely on a larger international bank to route their cross-border payments (meaning that the larger bank sets the cost base for the smaller bank).

In contrast, in over 70 countries today, domestic payments reach their destinations in seconds at minimal cost to the Sender or Recipient (see [Figure 1](#)). This is thanks to the growing availability of IPS. Connecting these IPS to each other has the potential to enable cross-border payments from Sender to Recipient within 60 seconds (in most cases).

Cross-border payments are inherently more complex than domestic payments. Cross-border payments require coordination between PSPs and payment systems in different countries and must go through additional steps such as currency conversion and compliance with anti-money laundering/countering the financing of terrorism (AML/CFT) requirements. However, by using modern payments technology, adopting international payment messaging standards, and building on the existing domestic IPS, it is possible to make the experience of cross-border payments almost as smooth and efficient as domestic payments.



Box 1: Alternative approaches to improving cross-border payments

Innovation across the payments industry has led to noticeable improvements in cross-border payments for some users. However, the landscape is still very fragmented, and the speed, cost, transparency and access to cross-border payments vary depending on the type of payment and the currencies or countries involved.

For cross-border payments through the correspondent banking network, initiatives such as Swift Global Payments Innovation (gpi) have improved speed by allowing banks to see how quickly other banks process payments on average and choose the fastest route through one or more intermediary banks.

“the landscape is still very fragmented, and the speed, cost, transparency and access to cross-border payments vary depending on the type of payment and the currencies or countries involved.”

Swift gpi also improves transparency with regards to the status of a payment, by asking all banks that receive a payment to report back to a central status tracking system.

However, such payments are still heavily reliant on the performance of banks' own systems and processes. (In contrast, the speed of Nexus payments is bound by the strict timeouts imposed by each IPS.)

Some fintech companies and some larger financial institutions have recognised the benefits of sending cross-border payments through IPS and have worked to integrate with multiple IPS. They may do this either directly or through a partnership with existing IPS members. While this approach can deliver near-instant cross-border payments, it is expensive and difficult to scale, as each IPS has a different scheme, technical standard and commercial model.

If every PSP tried to replicate the same approach it would lead to significant duplication of effort across the industry, which in turn would negate the cost savings of using IPS. (In contrast, Nexus standardises the way that IPS connect, and only requires IPS and PSPs to integrate once to get connected to all existing and new participants on the Nexus network. This indirectly spreads the costs of integrating with multiple IPS across every PSP that uses Nexus, meaning that more PSPs can get the benefits of cross-border payments through their domestic IPS at much lower cost.)

Another approach to improving cross-border payments is to rely on 'closed-loop' providers, where everyone is a customer of the same entity, such as very large e-wallet providers that may have hundreds of millions of customers. This is also the argument made by many stablecoin issuers. In general, processing a transaction between two customers of

the same institution (or same ledger, in the case of stablecoins) is fast and at low cost. However, this approach overlooks the end-to-end cost of a payment when the Sender and Recipient are not customers of the same e-wallet provider or stablecoin issuer.

Switching between wallet providers, stablecoins and bank deposits quickly adds friction and starts to undermine any cost savings. Consequently, the efficacy of the closed-loop approach hinges on the extent of customer concentration within a few providers but diminishes in the presence of numerous providers and genuine competition among them. (Nexus prioritises open-loop payments so that customers of different financial institutions can easily make payments to each other, so long as their financial institution is connected to an IPS.)

1.1 Interlinking instant payment systems (IPS)

Linking two IPS together ('interlinking') makes it possible to process a cross-border payment within 60 seconds (in most cases), and often much faster.

Interlinking of IPS has already been implemented in some countries and is in progress in others:

- In April 2021, the interlinking of Singapore's PayNow and Thailand's PromptPay was the first of its kind globally, allowing the customers of participating banks in Singapore and Thailand to send money across the two countries using just the Recipient's mobile phone number.⁴
- Southeast Asia has since become a hotspot for bilateral linkages, with 13 person-to-merchant (P2M) QR payment linkages and four person-to-person (P2P) payment linkages as of May 2024. Examples of P2M QR payment linkages include Malaysia and Thailand in June 2021⁵, Thailand and Indonesia in August 2021, and Malaysia and Indonesia in 2022. Examples of P2P payment linkages include Singapore and India⁶ in February 2023 and Singapore and Malaysia⁷ in November 2023.

- In November 2022, the central banks of Indonesia, Malaysia, the Philippines, Singapore and Thailand signed a memorandum of understanding to cooperate on payment connectivity to enhance cross-border payments.⁸
- In Europe and the United States, EBA Clearing and The Clearing House are collaborating to develop an EUR-USD link.⁹
- Buna is working to connect with IPS in the Arab countries.¹⁰
- The European Central Bank, Sveriges Riksbank and Danmarks Nationalbank are exploring the possibility of providing cross-currency payments between the euro, Swedish krona and Danish krone on the TIPS platform.

Each of these IPS linkages can deliver significant benefits for payment service users (eg individuals and micro, small or medium-sized businesses). However, the

experience has revealed that each bilateral link is a challenging and complex project.

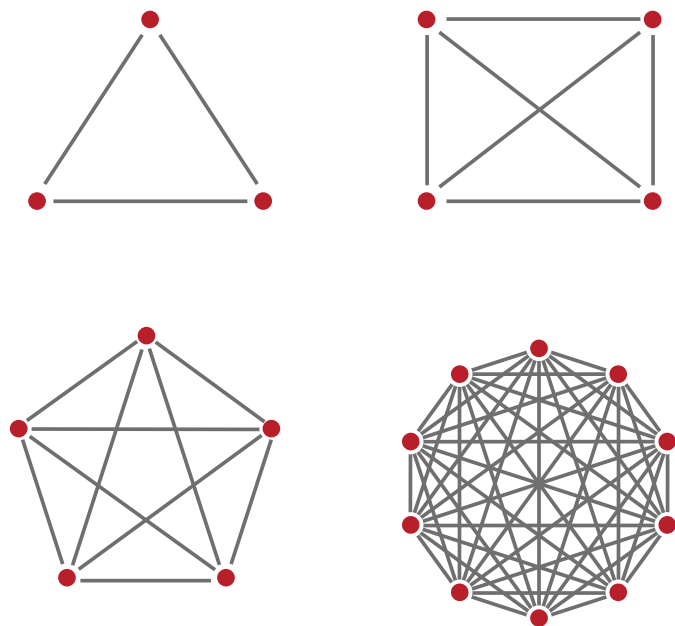
Each IPS has different technical processes and functionality, and different scheme rules, so the IPS operator and banks and PSPs in the country must make significant changes to their systems before they can start sending cross-border payments through the bilateral link. Each bilateral link also requires complex legal negotiations between IPS operators, central banks, banking associations and individual banks. The work then must be repeated for each new bilateral link.

Another challenge is that the number of bilateral links required grows faster than the number of countries joining the network,¹¹ with each link needing its own technical integration and legal negotiation (See [Figure 2](#)).

As a result of these challenges, the **investment in bilateral links is only commercially viable when connecting close trading partners or strong remittance corridors**, meaning that many lesser-used corridors would never be connected bilaterally.

Unlike multilateral arrangements, a bilateral link does not benefit from increasing network effects as new countries join over time. Ultimately, the bilateral approach does not scale beyond a few countries and is not a viable way of connecting all instant payment systems.

Figure 2: number of bilateral links grows faster than the number of countries



Box 2: differences between IPS that must be overcome

Domestic IPS are typically designed without considering cross-border payments or interoperability more generally. Consequently, there are often significant differences between different IPS, including:

Messaging standards: IPS may speak different 'languages' in the way they structure the data in payment instructions and related messages between the different participants.¹² ISO 20022 is being adopted as the new international standard for payment messages, but some IPS use the older ISO 8583 standard or a proprietary standard that is only used in one country. Banks and PSPs themselves may use different data structures internally. These messages need to be translated when moving from one payment system to another, with a risk of data loss or corruption.

Addressing payments: Each IPS may use a different way of addressing the recipient of a payment. In around 80 countries, International Bank Account Numbers (IBAN) can be used, and they are mandatory in the Euro area, but they are not supported in major

markets like the USA, Canada, Hong Kong or Singapore. Local account numbers have different lengths, and financial institution identifiers may be different and have different names (eg BIC, sort code, routing number, IFSC). An increasing number of countries allow payments to be sent to proxies such as mobile numbers or corporate identity numbers, but the proxies that are supported vary from country to country.¹³

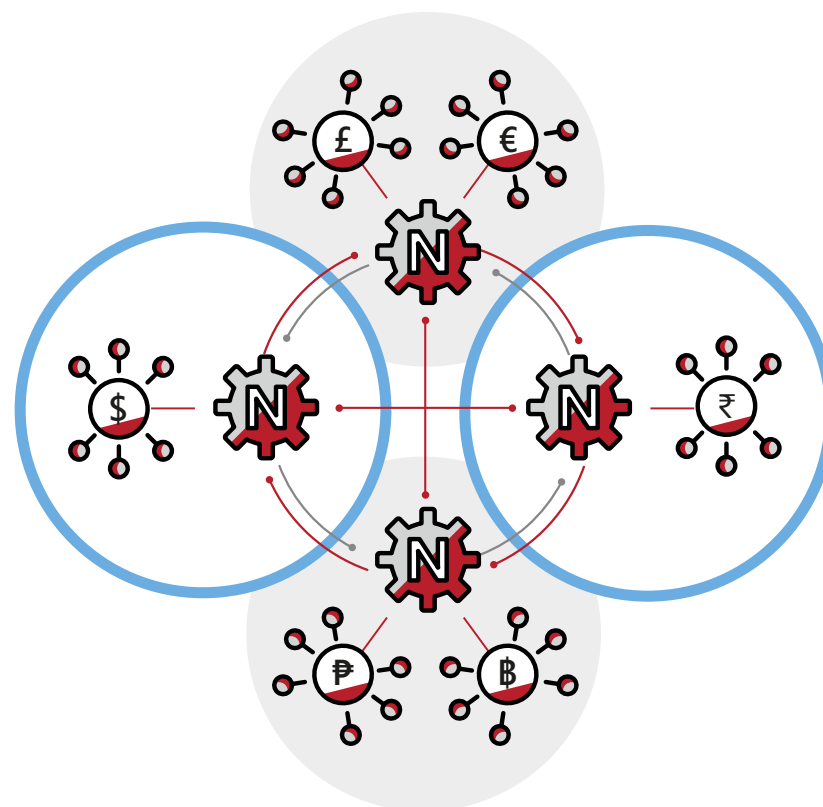
Dispute resolution process: Each domestic IPS has different mechanisms, procedures and timeframes for dispute resolution which can be challenging to manage in a multilateral cross-border context. To compound the problem, dispute resolution processes could differ between existing bilateral interlinking arrangements. This increases the complexity and compliance cost for the IPS and their participants.

1.2 How Nexus can accelerate the growth of instant cross-border payments

Nexus overcomes the limitations of bilateral interlinking by standardising the way that IPS connect to each other.

Nexus is a 'behind-the-scenes' service that would be used by IPS operators and their member PSPs to route instant cross-border payments. An IPS operator connects to Nexus, and then uses a common set of APIs¹⁴ and ISO 20022 messages¹⁵ to exchange payment instructions and other related information with another IPS operator, via the Nexus technology (see [Chapter 6.2](#)). This is a benefit for IPS operators, who can now start to process cross-border payments without needing to build multiple bilateral links.

Figure 3: Nexus Gateways connect IPS to each other, across borders





A common Nexus scheme rulebook helps to manage the differences between the domestic payment scheme rulebooks, particularly differences in rules, standards and operational procedures (see [Chapter 3.2](#)). This helps to minimise operational complexity (and the resulting costs) when dealing with multiple countries.

An IPS operator and its member PSPs must initially invest resources in terms of time and technology to connect to Nexus but can then connect to every other country already on the Nexus network. There is also minimal (if any) additional work for an IPS and its members to do when new countries join the network. This means the network can expand at near-zero marginal cost and effort for existing members and is more inclusive for smaller countries (whose smaller volumes may mean that other countries are not interested in linking bilaterally). In time, Nexus could also connect to other regional networks of IPS, allowing the network of interlinked IPS to grow even faster.

Nexus could significantly accelerate the growth of instant cross-border payments. To connect 70 IPS via Nexus would require 70 technical integration projects (one between each IPS and Nexus) compared with 2,415 *bilateral* initiatives (see [Figure 2](#)). In short, Nexus makes it possible to connect all IPS in a way that would be impracticable through bilateral links.

“A common Nexus scheme rulebook helps to manage the differences between the domestic payment scheme rulebooks, particularly differences in rules, standards and operational procedures.”

1.3 Benefits for the Sender and Recipient



Box 3: G20 Roadmap and targets for enhancing cross-border payments

Improving cross-border payments is a priority for the G20, which has published a Roadmap for Enhancing Cross-border Payments, developed by the Financial Stability Board (FSB) and the Committee on Payments and Market Infrastructures (CPMI). Interlinking of IPS is the second priority area of the Roadmap,¹⁶ which highlights Project Nexus as a priority action (Action 2(c)).

The Roadmap sets several targets for the speed, cost, access and transparency of cross-border payments, with a deadline of end-2027.¹⁷ On cost, the Roadmap sets the target for the global average cost of cross-border payments to be no more than 1%, and no corridor to be above 3% by end-2027. It also adopts the United Nations Sustainable Development Goals (UN SDG) target¹⁸ for the average cost of sending a cross-border migrant

remittance payment of US\$200 to be less than 3% of the value of the payment. On speed, the Roadmap also sets the target that 75% of cross-border payments (more generally) should be completed within one hour, and the rest within one business day. In terms of transparency, the Roadmap defines a list of required information that should be available to the Sender, including sending and receiving fees (including those of any intermediaries), the FX rate and any currency conversion charges, the expected time to deliver funds, tracking of payment status and the terms of service. For access, the target is that all end-users (including individuals and businesses) should have at least one option (such as a payments infrastructure or provider available) for sending and receiving electronic payments.

For the individuals and businesses that send cross-border payments, Nexus could have a significant impact on the speed, cost, transparency of and access to cross-border payments.



Speed

Nexus will enable cross-border payments in seconds, on a 24/7/365¹⁹ basis. As most IPS process domestic payments within 30 seconds, a cross-border payment via Nexus – which would first be processed by the IPS in the Sender’s country and then by the IPS in the Recipient’s country – could plausibly take 60 seconds or less. In contrast, the speed of traditional cross-border payments via correspondent banking depends on how quickly each bank in a payment chain picks up and processes the payment and may take anything from minutes to days.



Cost

Nexus payments should fall within the G20 and UN SDG target of costing the Sender less than 3% of the value of the payment. Nexus builds on and reuses existing IPS, which typically charge a small transaction fee to participants. This sets a low-cost base for cross-border payments through IPS – although there are inherently more costs involved in a cross-border payment than in a domestic one (such as sanctions screening, message translation and currency conversion).



Access

Nexus provides access to cross-border payments to any bank or non-bank PSPs that are eligible to join their domestic IPS. Its design also makes it easier for smaller banks, which may be present in only one country, to offer cross-border payments. However, the specific level of access in a country would still depend on the level of financial inclusion and percentage of people who have accounts with banks or PSPs that are connected to IPS in that country.



Transparency

Nexus gives the Sender transparency about how much it will cost them to pay a specific amount to the Recipient. The Nexus Scheme Rulebook and technology ensure that the Source PSP will show the Sender exactly how much will be debited from their account and exactly how much will be credited to the Recipient’s account, as well as the exchange rate that will be applied.

Nexus also gives the Sender transparency about the status of a payment. By design, a time-critical payment through an IPS either completes or fails within seconds. It is clear to the Sender whether a payment has been accepted by the Destination PSP, whether it is still being reviewed (in the case of non-time-critical payments) or has been rejected.²⁰

1.4 Progress to date

In 2021, the BISIH Singapore Centre developed a **blueprint for Nexus** through multiple design workshops with central banks, banks/PSPs, IPS operators and FX providers.²¹

In 2022, working with the Bank of Italy, Central Bank of Malaysia, Monetary Authority of Singapore, Banking Computer Services (BCS) in Singapore and PayNet in Malaysia, the Nexus team **built a working prototype** to connect the test versions²² of three established instant payment systems of the Eurosystem, Malaysia and Singapore. **This proof of concept confirmed the technical viability of the Nexus model**, and the project report detailing the proposed architecture and key learnings to date was published in March 2023.²³ (See [Annex](#) for a summary of the proof of concept.)

In 2023–24, the Nexus team worked closely with the central banks of Indonesia, Malaysia, the Philippines, Singapore and Thailand (ASEAN-5), which are interested in using the Nexus blueprint as a framework to achieve their public commitment to interlink their domestic IPS. The team tested the Nexus model against the reality of these payment systems, and consulted

with central banks, standard-setting bodies, IPS operators and commercial banks in some of the largest instant payment markets around the world to validate that Nexus is scalable and interoperable with IPS beyond those five countries.

The work has been structured around **three workstreams**, which aimed to:

- design appropriate **governance, scheme and oversight structures** that caters to regulatory variations across countries while ensuring safe, efficient and resilient Nexus payments;
- develop a sustainable **business and revenue model** for Nexus that incentivises key industry players to participate; and
- finalise the Nexus **technology architecture and operational model**, leveraging insights from the developed proof of concept software.

This report summarises the output from this latest phase of work. [Chapter 2](#) gives a high-level understanding of how Nexus works to process a cross-border payment from the Sender to the Recipient. Chapters [3](#), [4](#), [5](#) and [6](#), respectively, go in-depth into the Nexus governance and scheme arrangements, possible oversight approach, business model, and technology and operations.

Detailed technical documentation, including guides for each type of participant in Nexus, is available to central banks and payment system operators on request.

Box 4: Nexus design principles

The Nexus governance and scheme arrangements, possible oversight approach, commercial model and technology blueprint have all been designed around a set of guiding principles:

- **Alignment with public policy goals:** Nexus should enable safe, efficient (fast and low-cost), accessible and transparent cross-border payments. For example, the total cost of a Nexus payment to the Sender should be within the 3% target set by the G20 and the UN Sustainable Development Goals (See [Box 3](#)).
- **Inclusivity:** Nexus should ensure that large and small participants and relevant stakeholders are represented in the decision-making process, and that the design of Nexus does not unfairly exclude countries or types of participant.
- **Neutrality:** Nexus should ensure fairness and impartiality between jurisdictions and financial institutions, and provide a level playing field (for example, by ensuring that aspects of Nexus provision are subject to competition).
- **Financial sustainability:** Nexus as an operation must be able to secure investment for the setup phase, and have a financially sustainable commercial model, so that (in time) revenues are sufficient to cover costs.
- **Agility:** The governance arrangements for Nexus must allow for timely decision-making, decisiveness, and the ability to respond promptly to changes in the payments landscape. The technology architecture must allow for regular enhancements. This is necessary both to manage risk and to ensure ongoing innovation.
- **Scalability:** The design should support the ambition to grow Nexus beyond the initial members, by expanding coverage to other countries or regions over time (either through those countries joining Nexus, or through interoperability with other cross-border instant payment networks). It should also support the extension of Nexus to support new use cases, such as payments to merchants.

2 How Nexus works

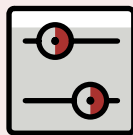


Key takeaways



Supporting account-to-account payments

At launch, Nexus will support low- and medium-value account-to-account payments, from person to person, business to business and person to business (or vice versa). Payments to merchants (P2M) at the point of sale or online and additional use cases will be added to the Nexus roadmap.



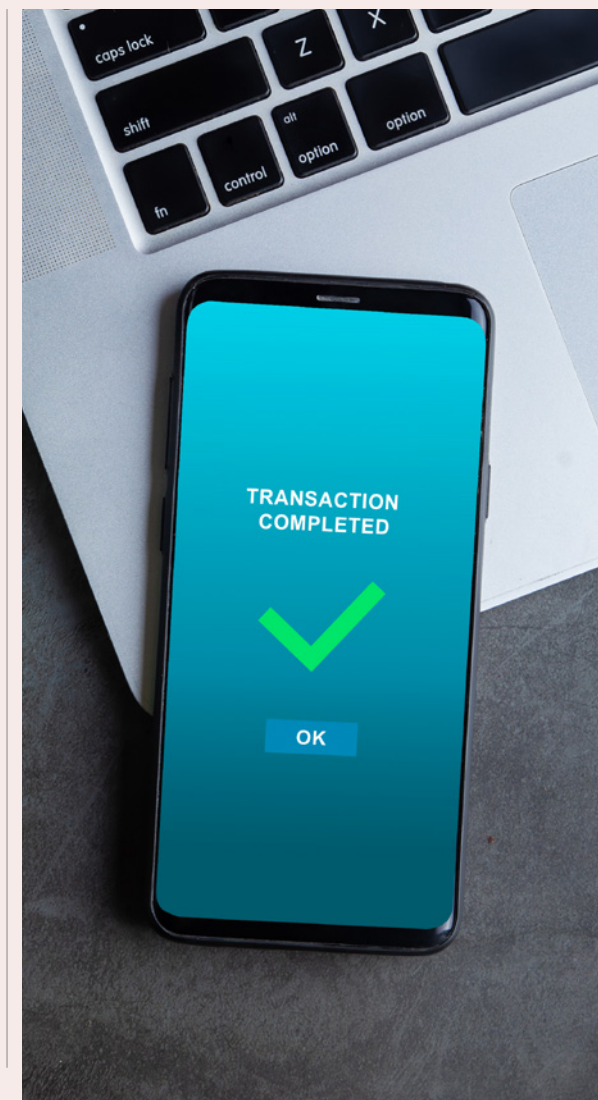
Sequential payments

A Nexus payment is processed sequentially through the Instant Payment Systems (IPS) in the Sender and Recipient's country. If the payment is rejected for any reason, Nexus will ensure that the payment is reversed, and the funds are returned to the Sender.



A flexible model

Nexus provides financial institutions with a flexible participation model that allows them to play the roles that make commercial sense to them, including as a Payment Service Provider (PSP), an FX Provider (FXP), or as a Settlement Access Provider (SAP). Financial institutions can play multiple roles depending on the payment and the corridor.



2.1 Who would use Nexus?



Users

Cross-border payments through Nexus can be sent by individuals or businesses that currently use IPS to send domestic payments (so-called 'retail' payments). This means Nexus supports the **person-to-person (P2P)**, **business-to-business (B2B)**, business-to-person and person-to-business payment use cases.²⁴ Individuals could use Nexus to send payments to family or friends in other countries, while businesses (particularly micro, small and medium-sized businesses) could use Nexus to send payments to suppliers or employees in other countries.



Types of payment

Nexus currently supports account-to-account push payments, ie payments that are initiated by the Sender. Functionality to support pull payments (such as requests to pay), or payments to merchants (P2M) at the point of sale (whether in a shop or online) are not currently supported but could be added at a later date.

All Nexus payments involve a currency conversion from the Sender's currency to the Recipient's currency. Nexus does not currently support cross-border payments in the same currency (for example, euro payments between member countries of the euro zone). It also does not currently support payments that are denominated in currencies other than the currency of both the Source IPS and Destination IPS (for example, it does not support a USD-denominated payment from Singapore to Malaysia). While Nexus does not currently support these features, they are technically feasible and could be added at a later date.



Payment size

There is no overall cap on the value of a payment that can be sent through Nexus. However, most IPS impose a cap on the value of a domestic payment, which can vary from just a few hundred dollars in some countries to over a million dollars (equivalent) in others. Countries may also choose to implement a different cap on the value of a cross-border payment based on domestic regulations, while PSPs could individually set their own (lower) limits on the amount their customers can send. For each payment, Nexus would automatically apply the lowest of the two caps of the domestic IPS.²⁵

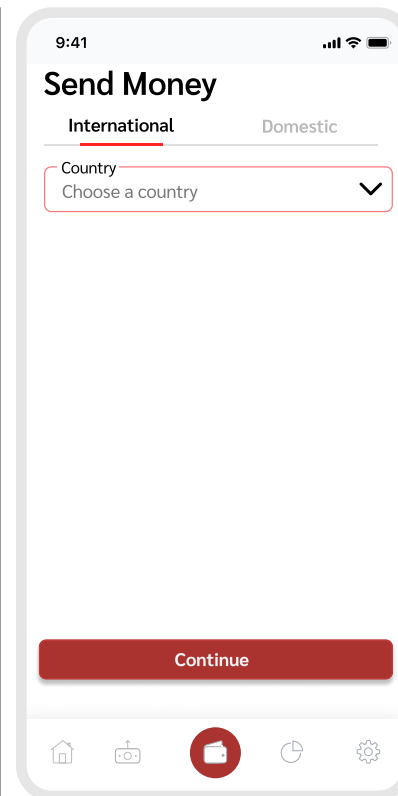
The caps on payment values mean that Nexus could not practicably be used to send high-value, 'wholesale' payments between financial institutions.



2.2 The user experience when making a payment through Nexus

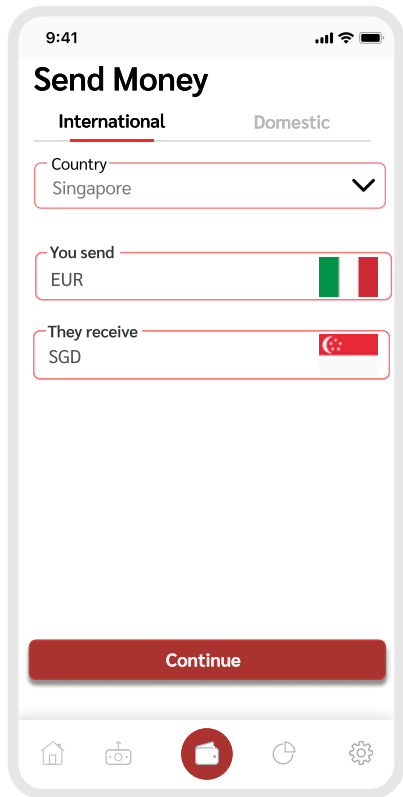
Nexus was designed with a **focus on the needs and user experience** of both payers and payees. This required thinking carefully about how users would want to send and receive payments, and designing the functionality and data exchange in Nexus to support this process.

The example user journey below demonstrates how an individual Sender would use their existing PSP channel (eg an app) to make a payment through Nexus, and describes the steps taken by Nexus behind the scenes. (Note that there is no 'Nexus app' and payment Senders do not register with or interact directly with Nexus.)

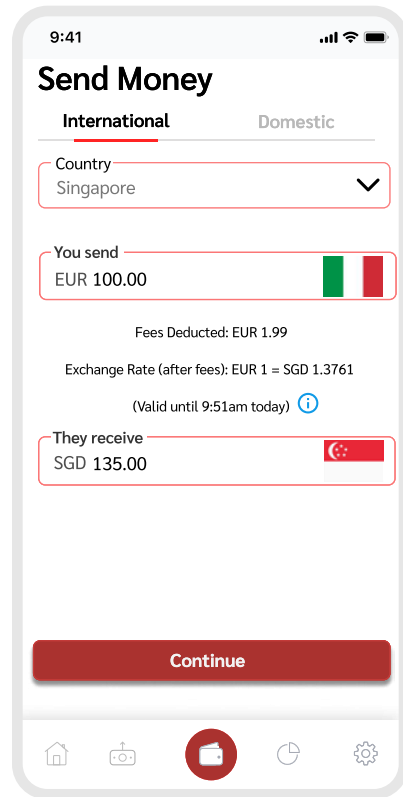


The sender logs in to their bank or PSP's existing app. (There is no separate Nexus app.)

The Sender selects the Destination Country (ie the country of the Recipient).



The Sender enters EITHER the amount they wish to send, in their own currency, OR the exact amount they wish for the Recipient to receive, in the Recipient's currency.



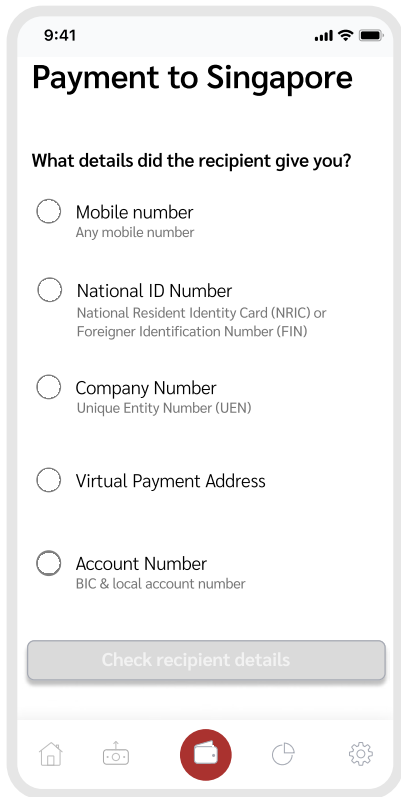
The Source PSP (ie the Sender's PSP) will ask Nexus for available **FX quotes** for payments to the Destination Country. Nexus returns a list of quotes from the FXPs with which the Source PSP already has a business relationship. The Source PSP selects the quote and FXP that it wishes to use.

Then the Source PSP must show the Sender:

- the fees that are charged to the Sender (which may be deducted from the value of the payment or appear as a separate charge on their account);
- the effective exchange rate that will be applied; and
- the exact amount that will be credited to the Recipient's account, in the Recipient's currency.

(See [Chapter 5.1.1](#) for a full description of the transparency requirements and fees in Nexus.)

If the Sender accepts the rate and fees, they click 'Continue'. If they change either the amount to be sent or the amount to receive, the rate and fees will be refreshed (as larger payments may be eligible for better rates).



Next, the Source PSP uses the Nexus APIs to request the full list of address types that can be used to address payments to the Destination Country. This could include proxies (such as mobile numbers or company registration numbers), International Bank Account Numbers (IBAN), or local account numbers.

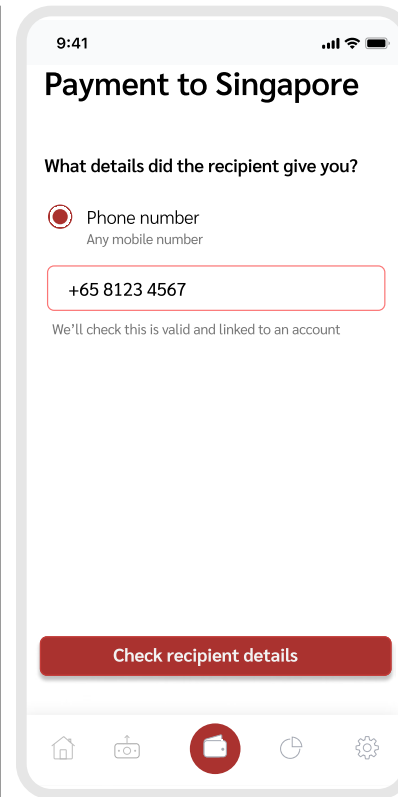
It uses this information to dynamically create a list of address options in the app.

The Sender then selects the type of proxy or account details that the Recipient has provided to them.

The Sender can select a proxy (such as a mobile phone number). Any proxy that is valid in the Destination Country will also be valid through Nexus.

The Sender can alternatively enter a domestic account number and financial institution identifier (such as a BIC) or an IBAN, where these are accepted in the Destination Country.

“The Sender can select a proxy (such as a mobile phone number). Any proxy that is valid in the Destination Country will also be valid through Nexus.”



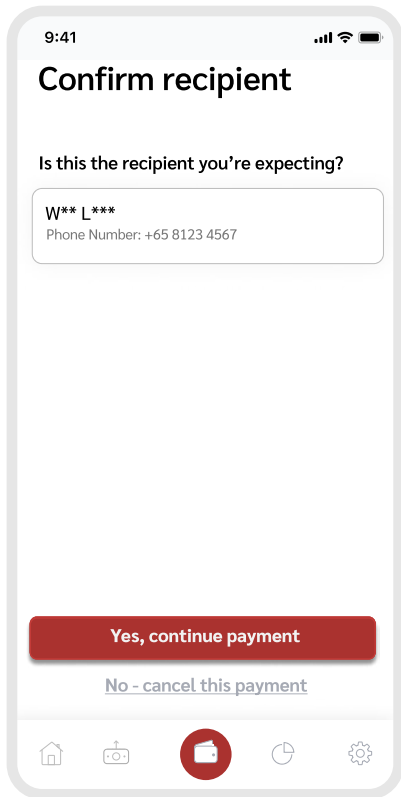
The Source PSP shows the input field for the chosen address type – in this case a mobile number – using details from the Nexus APIs.

The Sender then inputs the details that the Recipient has provided to them.

If a Sender enters a proxy, the Source PSP will send a **proxy resolution request** to Nexus (as an ISO 20022 acmt.023 message). Nexus will then contact the proxy directory in the Destination Country. If the proxy is linked to an account, the proxy directory will respond to Nexus with the associated account details and the full name of the Recipient (which is only visible to the Source PSP), and a display name that can be shown to the Sender.

Nexus will use the account details to confirm that the Recipient's PSP is onboarded with Nexus and able to receive cross-border payments.

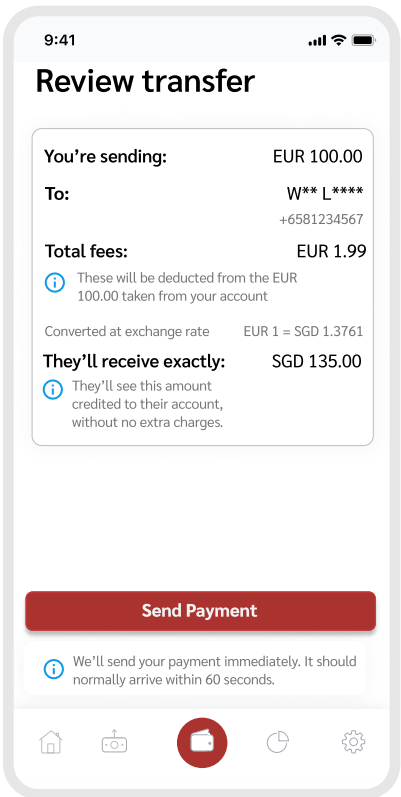
In some cases, Nexus will also reach out to the Destination PSP (ie the Recipient's PSP) to ask for further information about the Recipient and the Recipient's account – a process known as **account resolution**. If the Destination PSP provides this information, it will be returned to the Source PSP to use in the payment instruction, helping to ensure that all compliance and sanctions screening checks can be done efficiently.



Now the Sender is shown the name of the Recipient, as provided by the proxy resolution service or the Destination PSP, where available.

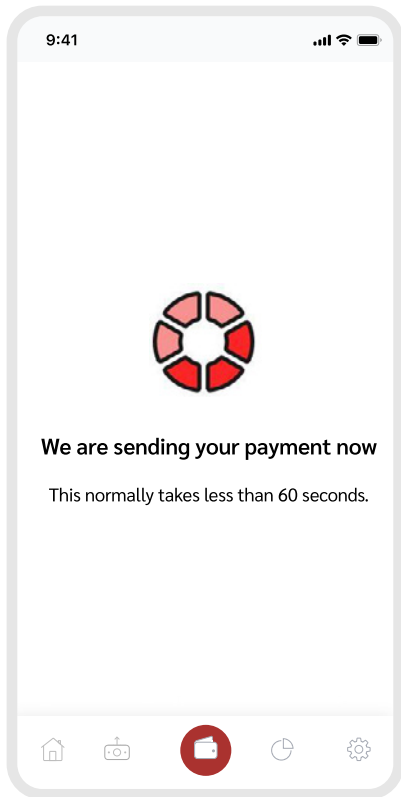
Depending on the data protection requirements in the Recipient's country (and the Recipient's own agreement with their PSP), the Sender may be shown the Recipient's name in full or partially masked. This gives the Sender the confidence that they are sending payments to the correct account and helps to prevent fraud or scams.

The Sender confirms the name (if they do not recognise the name, they can cancel the payment).



The Sender must be given a chance to confirm all details. They are shown exactly what will be deducted from their account, exactly what will be credited to the Recipient, the final exchange rate that applies and any fees that will be deducted.

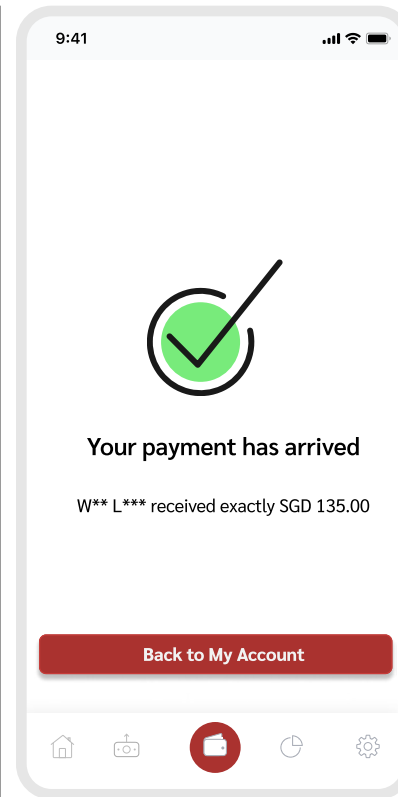
The Sender clicks 'Send Payment'.



The Source PSP can now submit the final payment instruction to the Source IPS (as an ISO 20022 pacs.008 message).

Once the Source IPS has processed the first leg of the payment, the Nexus Gateway will communicate with the Nexus Gateway in the Destination Country, which will trigger the second stage of the process in the Destination IPS.

In most cases, the payment should be processed within 60 seconds.



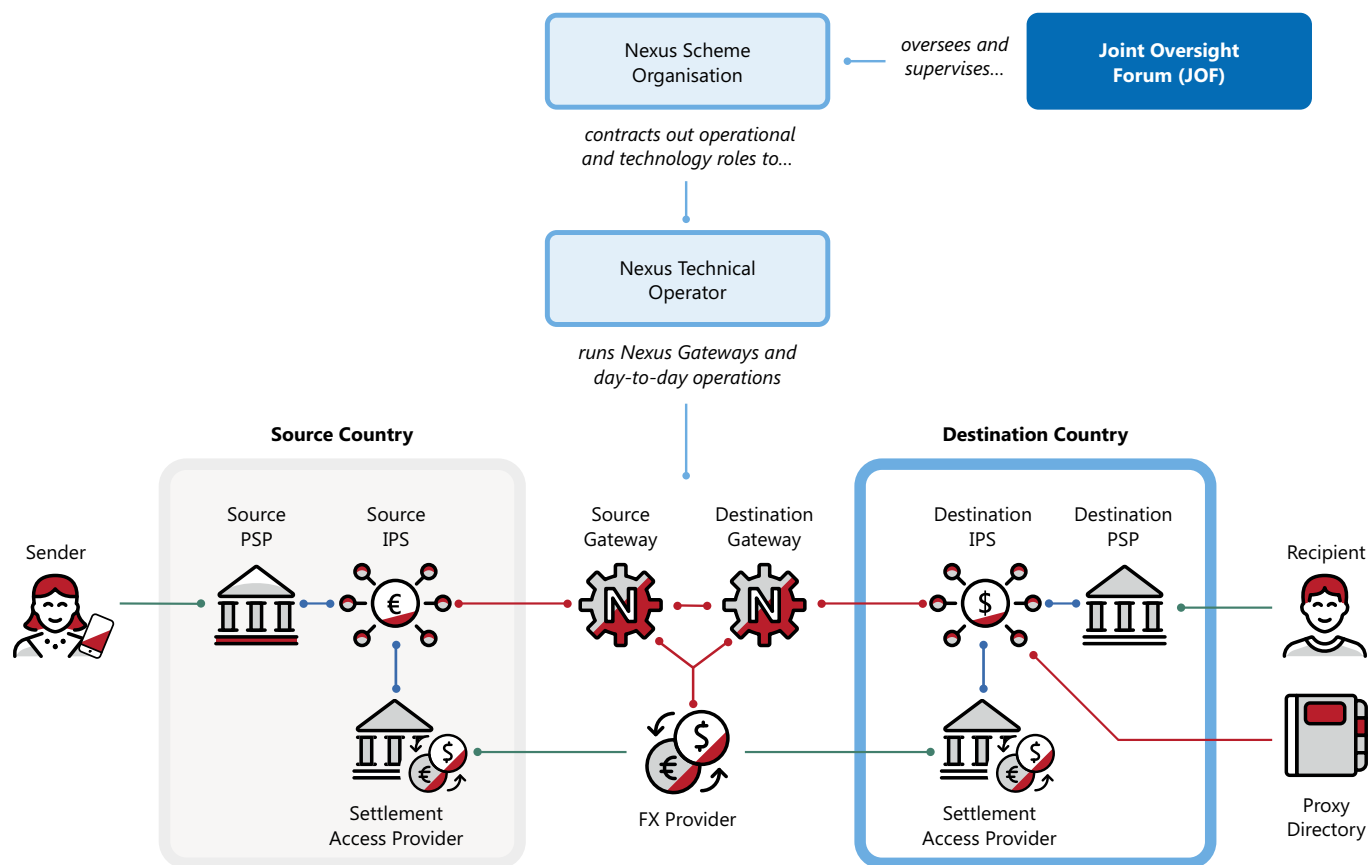
Once the final payment stage is complete, the Recipient's account will be credited, the Recipient will be notified that their account has been credited, and the Sender will be notified that their payment was successful.

In some cases, the payment will trigger an alert against any sanctions lists and will be subject to further review by the Destination PSP. The process and timescale for managing these payments is discussed in [Chapter 3.2.2](#).

2.3 Actors in Nexus

Nexus involves several actors, including the organisations responsible for managing the Nexus scheme and operating Nexus on a day-to-day basis, the financial institutions that participate in Nexus payments, and the end-users who send and receive payments through Nexus.

Figure 4: diagram of all actors and the relationship between them



2.3.1 The Nexus Scheme Organisation

The Nexus scheme would need to be owned and managed by an entity, known provisionally as the **Nexus Scheme Organisation (NSO)**. The NSO is responsible for producing and managing the **Nexus Scheme Rulebook**, which is a binding agreement that defines the types of participants in Nexus (ie IPS operators, FXPs, PSPs and SAPs) and their rights and obligations. It also describes the eligibility requirements and process for joining Nexus, while providing a mechanism for dispute resolution. The NSO's governance arrangements are set out in the **Nexus Scheme Management Rules**, which outlines the relationship between the owners, Board of Directors, Executive Management Team and key stakeholder groups. These rules serve as the NSO's constitution.

The NSO is also responsible for developing the product roadmap and fee model and managing disputes escalated by participants. Finally, the NSO is responsible for managing the Nexus Technical Operator.

2.3.2 The Nexus Technical Operator

Running a payment system requires a significant amount of technical and operational expertise. The NSO may choose to outsource the day-to-day running of the technology and operations required by Nexus to an experienced payment system operator via a competitive bidding process. The operator that is awarded the contract would play the role of '**Nexus Technical Operator**' (NTO). The NTO would be responsible for providing and maintaining the technology and network that supports Nexus, and for providing an operations team that onboards new participants and provides technical support.

2.3.3 Instant Payment System (IPS) operators

IPS operators run the IPS that enable Senders and Recipients to make instant *domestic* payments, ie between two accounts in the same country.

2.3.4 Proxy Directory Operators

Proxy Directory Operators (PDO) run the directories that link a proxy (such as a mobile number) to a specific account. In most cases, it is the IPS operator that runs the proxy directory for a specific country. However, in some countries the PDO is a separate entity, and so Nexus treats this as a separate role with its own specific requirements and obligations.

2.3.5 End users: Sender and Recipient

End users of Nexus can be individuals or businesses that use IPS to send payments. The **Sender** is the user who initiates the payment and sends money to the **Recipient**.

2.3.6 Three roles for financial institutions: PSP, FXP and SAP

There are three roles that **financial institutions** can play in Nexus: as a **Payment Service Provider (PSP)**, an **FX Provider (FXP)** or a **Settlement Access Provider (SAP)**; these are described below. The participation model in Nexus is flexible, allowing financial institutions to fulfil the roles that make commercial sense to them and rely on specialists (such as third-party FXPs, discussed below) for services that they do not want to provide themselves. A single financial institution may play one or more roles in a specific payment and may play different roles for different corridors. Each role comes with its own set of obligations and responsibilities, which are defined in the Nexus Scheme Rulebook (see [Chapter 3.2](#)).

“The participation model in Nexus is flexible, allowing financial institutions to fulfil the roles that make commercial sense to them and rely on specialists (such as third-party FXPs, discussed below) for services that they do not want to provide themselves.”

Role 1: Payment Service Provider

Payment Service Providers (PSPs) are the financial institutions that provide accounts to the end-users. These institutions may be licensed banks or (in some countries) non-bank PSPs. In Nexus, **the term ‘PSPs’ is used inclusively to cover all banks and non-bank payment service providers that are eligible to connect to an IPS.**

In a Nexus payment, the **Source PSP** is the Sender’s PSP, and the **Destination PSP** is the Recipient’s PSP.

Role 2: FX Provider

Every cross-border, cross-currency payment requires an actor that is willing and able to exchange one currency for another. In Nexus, the entity providing this service plays the role of **FX Provider (FXP)**. FXP’s would be regulated financial institutions that hold accounts in at least two jurisdictions and that are willing to accept the Source Currency from the Sender and pay out the Destination Currency to the Recipient.²⁶

In some cases, the Source PSP will act as FXP for its own payments; this can happen where the Source PSP is present in two countries or already holds funds in the Destination Country. In other cases, the Source PSP will make use of a **third-party FXP**; this is more common when the Source PSP operates in only one country or does not wish to hold funds in the Destination Country.

Third-party FXP’s inform Nexus of the current rates at which they are willing to exchange one currency for another. These rates are shared with PSPs that are sending payments on behalf of their customers. FXP’s compete to offer the best rates for a specific corridor, helping to ensure a competitive market.

FXP’s are discussed in more detail in [Chapter 2.6](#).

Role 3: Settlement Access Provider

To act as an FXP in Nexus, a financial institution must hold an account in the Source IPS and Destination IPS of the corridor or currency pair in which it intends to participate. However, if the institution is not a member of a particular IPS, it can hold an account at an existing member (ie an existing PSP).

PSPs that provide accounts to FXP’s act as **Settlement Access Providers (SAPs)**.²⁷ When an FXP uses an SAP, Nexus payments will flow into and out of the FXP’s account at that SAP.

SAPs are likely to be used by:

- FXP’s that are not eligible to be a member of a particular IPS (eg a non-bank FX dealer);
- FXP’s that will find it too expensive to become a member of a particular IPS (eg an FXP that does not also operate as a PSP in one of the countries in the corridor); and
- PSPs in other countries that want to act as an FXP for their own payments.

2.3.7 Joint Oversight Forum

Finally, the NSO and the entire Nexus scheme and arrangement may be overseen by a Joint Oversight Forum (JOF) comprising the central banks/regulators of the participating countries.²⁸ The JOF would set oversight expectations and oversee the NSO to ensure Nexus is operated safely and efficiently, consistent with international best practices such as the Principles for Financial Market Infrastructures (PFMI) and in line with public policy objectives. A lead overseer would be appointed among the central banks/regulators to coordinate the oversight activity and facilitate information sharing (See [Chapter 4](#)).

2.4 Technology components of Nexus



There are three key technological components of Nexus:

The **Nexus Gateway** is a piece of software and infrastructure that manages cross-border communication between IPS operators and coordinates the processing of Nexus payments between two countries. Nexus Gateways would also manage other functions such as cross-border proxy resolution, interaction with FXPs, and calculation and provision of FX quotes to PSPs. Each IPS will connect to a Nexus Gateway (See [Chapter 6.3](#)).



IPS communicate with the Nexus Gateways via a **standardised set of APIs and ISO 20022 messages**. This common technical interface enables multiple IPS operators to connect without having to adapt to the unique approach of each other's country. Nexus enables IPS to connect even if they do not use the ISO 20022 standard. This is achieved via an intermediary step of translating their domestic formats into the ISO 20022 format (See [Chapter 6.2](#)).



Finally, a **secure network** connects each IPS to a Nexus Gateway, and connects the Nexus Gateways together (See [Chapter 6.4](#)).

2.5 How payments are processed through Nexus

Unlike a typical IPS, Nexus does not maintain a ledger of balances or obligations between financial institutions and does not hold funds or accounts for PSPs.

Instead, Nexus acts as the coordinator of two separate but related instant payments across two separate IPS. These two separate payments are processed by the IPS in almost the same way as any other domestic payment.²⁹

Importantly, Nexus does not require changes to the domestic clearing and settlement process of each IPS. The domestic IPS does not need to be aware of any non-domestic currency involved in the payment and does not need to coordinate the timing of its settlement cycles with other countries. Nexus is compatible with IPS that use real-time immediate settlement models,³⁰ or deferred net settlement (DNS) models.³¹ That said, the IPS will need to make some technical changes to enable the processing of Nexus payments.

2.5.1 An example payment

Once the Sender has completed the setup process shown in [Chapter 2.2](#) and clicked 'Send Payment', the Source PSP can initiate the final payment instruction.

Note that the following description is significantly simplified, with some steps, such as sanctions screening, left out. The exact process may also vary slightly from IPS to IPS. The figures and exchange rate shown are broadly realistic but have been adjusted slightly to give round numbers. A more detailed and technical description of each step is given in the Payment Processing section of the technical documents, available to central banks and IPS operators on request.

“Nexus does not maintain a ledger of balances or obligations between financial institutions and does not hold funds or accounts for PSPs. Instead, Nexus acts as the coordinator of two separate but related instant payments across two separate IPS. These two separate payments are processed by the IPS in almost the same way as any other domestic payment.”

In this scenario, the Sender wishes to send S\$135 to the Recipient. Once the Sender approves the payment:

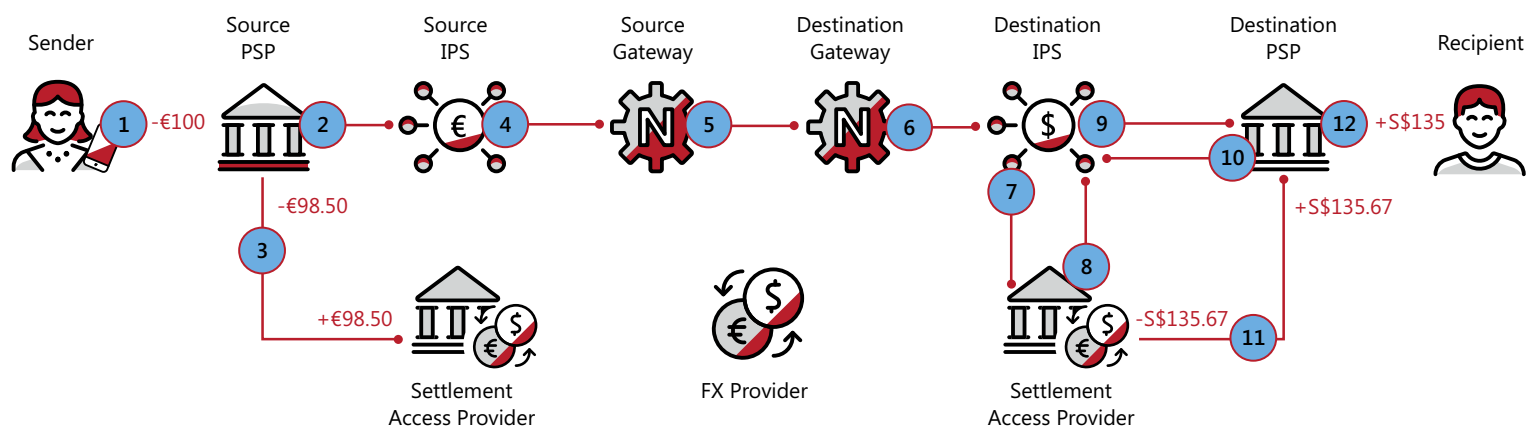
- 1 The Source PSP debits³² €100 from the Sender's account.
 - The Source PSP deducts its own fee, €1.50, from the payment. (This fee is set at the Source PSP's discretion.)
- 2 The Source PSP sends the payment instruction to the Source IPS.
- 3 The Source IPS processes a transfer of €98.50 from the Source PSP to the FXP's account (at its Source SAP).
- 4 The Source IPS forwards the payment instruction to the Source Nexus Gateway.

- 5 The Source Nexus Gateway looks up the quote referenced in the payment instruction, validates the exchange rate in the payment instruction is the same as in the original quote, applies the exchange rate of 1.3774 (so that the value is now S\$135.67) and then sends the payment instruction to the Destination Nexus Gateway.
- 6 The Destination Nexus Gateway forwards the payment instruction to the Destination IPS.
- 7 The Destination IPS sends the payment instruction to the FXP's Destination SAP for review.

- 8 The Destination SAP checks that the FXP has sufficient funds and then sends the payment instruction back to the Destination IPS as an instruction to make the payment to the Destination PSP.
- 9 The Destination IPS forwards the payment instruction to the Destination PSP for its review and acceptance.
- 10 The Destination PSP reviews the instruction and applies any relevant compliance checks. If it is willing to accept the payment, it will send a confirmation of acceptance back to the Destination IPS.

- 11 The IPS processes a transfer of S\$135.67 from the FXP's account at the Destination SAP to the Destination PSP.
 - The Destination PSP deducts its fee of S\$0.67 (See Chapter 5.2).
- 12 The Destination PSP credits the Recipient the remaining S\$135.00. (This is exactly the amount that the Sender was originally shown.)
- 13 Finally, the Destination PSP sends a confirmation message (not shown in the diagram above), which flows back through Nexus to the Source PSP, which informs the Sender that the payment is complete.

Figure 5 – how a payment is processed in Nexus



2.5.2 When payments fail

Nexus is designed so that if a payment is rejected by any participant, the whole payment process will be reversed and funds will be returned to the Source PSP and Sender. A payment may be rejected for several reasons, such as the Recipient's account being closed or frozen.

2.6 FX provision in Nexus

The FX provision model in Nexus is designed to be flexible so that each PSP can take the approach that works for them.

Larger PSPs, which may be present in multiple countries and participate in multiple IPS or hold accounts in multiple countries, are likely to provide FX conversion for their own payments. Smaller PSPs are more likely to want to use third-party FXPs (which could indeed be larger multi-national PSPs, as well as non-bank FX dealers).

The advantage of this approach is that it allows PSPs to send cross-border payments without having to hold multiple currencies in multiple countries (because this role can be performed by the FXP). This also means the PSP does not have to hold accounts with PSPs in multiple other countries (which can be expensive to set up and maintain).

2.6.1 Rates and quotes

As Nexus payments are high volume and relatively low value (compared to wholesale FX market trades), it is impractical to ask FXPs to bid on individual payments. Instead, Nexus requests FXPs to provide a rate that they are happy to offer for all Nexus payments. This rate will apply until the FXP sends a new rate.

Nexus uses these rates to generate quotes that are provided to Source PSPs at the point that a Sender sets up a payment.

FXPs can configure Nexus so that better rates can be offered for larger transactions and for certain PSPs. Nexus will automatically apply any improvements when generating the quotes.

2.6.2 FXP access to instant payment systems

If the FXP is already a member of the Source and Destination IPS (and therefore also a PSP), it can directly receive a payment in the Source Currency from the Source PSP and pay out the Destination Currency to the Destination PSP. However, if it does not have membership in either or both IPS, the FXP will instead need to make use of an SAP. The use of SAPs allows an FXP to provide currency conversion to PSPs in a country even if the FXP is not a member or not eligible to be a member (ie non-bank FX dealers) of a country's domestic IPS.

2.6.3 FXPs and PSPs

As FXPs are providing a service to the Source PSP, the FXP will normally want to complete know your customer/ business checks on PSPs before it starts providing FX conversion services to those PSPs. The FXP can inform Nexus once it is ready to start providing FX conversion services to a particular PSP. Nexus will share an FXP's rates and quotes only with a PSP that it has already approved.

2.6.4 Managing FX risk

For FXPs, FX risk in Nexus is relatively limited because the time between a quote being sent to the PSP and the payment being completed is no more than a few minutes.

However, FXPs that hold funds in accounts at SAPs will have cross-border credit exposures to those SAPs. Alternatively, if the SAP provides a line of credit to the FXP, the SAP may have a credit exposure to the FXP. These risks must be managed bilaterally between these parties, but do not in any case pose a risk to the immediate processing of Nexus payments.

2.6.5 Future support for intermediary currencies

For each currency pair, Nexus currently requires that there shall be at least one FXP that can *directly* connect the two currencies. However, as Nexus scales, there will be an increasing number of corridors that are used less often and may not have FXPs that operate in both currencies. For example, while there are several PSPs that operate in both Malaysia and Singapore, there are likely to be few PSPs that are present in both Malaysia and Mexico. For these less commonly used currency pairs, it may be necessary for a payment to flow through a third currency, such as euros. This feature will be added to Nexus as it scales.



3 Nexus governance and scheme arrangements



Key takeaways



A hybrid public-private ownership model

Nexus would be owned and managed by an entity, known provisionally as the Nexus Scheme Organisation (NSO). The NSO would be jointly owned by the participating countries under a hybrid public-private ownership model. The NSO would operate on a not-for-profit basis and be incorporated as a company limited by guarantee in an appropriate home jurisdiction.



Nexus Scheme Rulebook

The NSO would also be responsible for producing and managing the **Nexus Scheme Rulebook**, which defines the eligibility requirements, rights and obligations of participants in the scheme, and describes the processes, rules and technical standards that govern how payments are made through Nexus. The Rulebook complements domestic scheme rulebooks (which typically do not address cross-border payments).



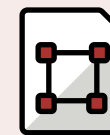
Outsourcing operations

The NSO would be ultimately responsible for the running of Nexus but may choose to outsource its day-to-day technology and operations roles to an experienced firm, known provisionally as the Nexus Technical Operator (NTO).



Public policy objectives

The Nexus governance and scheme arrangements have been designed to support Nexus's public policy objectives and adhere to the design principles of inclusivity, agility, financial sustainability, neutrality and scalability (See [Box 4](#)).



Designed to be compliant

Nexus is designed to be compliant with domestic regulatory requirements and to respect each country's domestic monetary and financial stability policies. The NSO and its participants must comply with the applicable laws in the participating countries including AML/CFT and sanctions screening rules, FX and capital flow management (CFM) measures, and regulatory reporting requirements.

3.1 The Nexus Scheme Organisation

Nexus would be owned and governed³³ by a dedicated and separate legal entity known provisionally as the **Nexus Scheme Organisation (NSO)**.

The NSO is responsible for the overall governance and management of Nexus, and for issuing the Nexus Scheme Rulebook (see [Chapter 3.2](#)).

The NSO's governance arrangements are set out in the **Nexus Scheme Management Rules** which serves as the NSO's constitution that each of the participating countries would subscribe to when they sign up to become a joint owner of Nexus.

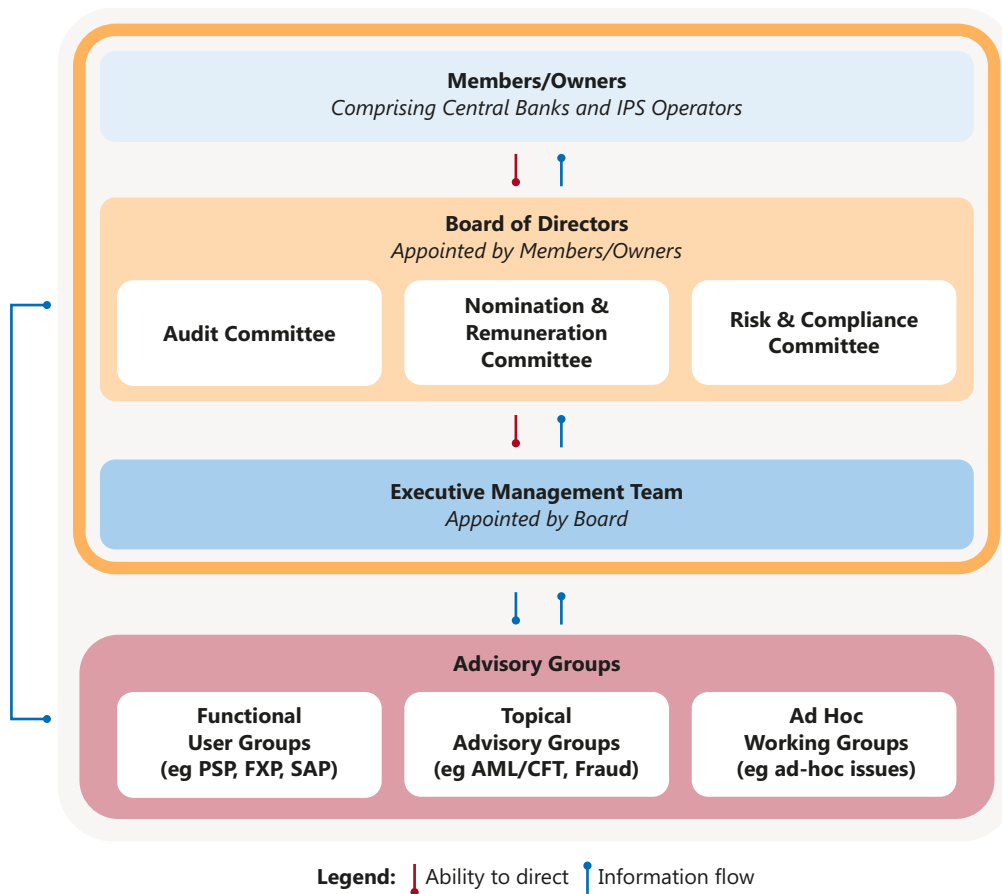
A common Nexus payment scheme and rulebook avoids the need for hundreds of bilateral negotiations between IPS operators and their member PSPs in each country, as well as ensuring a more consistent user experience and service level for payers and payees. This arrangement will give the Nexus payment scheme a well-founded, clear, transparent and enforceable legal basis and governance arrangements to ensure its overall soundness, in line with the PFMI.³⁴

3.1.1 Ownership model

The composition of owners is a key design choice for the NSO as it would determine who may exercise control and shape the direction of Nexus. In this regard, the NSO would be jointly owned by the participating countries under a hybrid public-private ownership model. Each participating country may nominate an entity that best represents its interest (ie central bank or IPS operators³⁵) to be a joint owner of the NSO.³⁶ Central banks that are joint owners of the NSO would need to put in place the necessary controls to manage any potential conflict of interests with their overseer role.³⁷

Such an ownership model would ensure that each participating country has a say in the running of Nexus. It would also foster the right balance between public and private sector interests to achieve the public policy goals, whilst ensuring the long-term financial sustainability of Nexus.





3.1.2 Corporate structure

Given Nexus’s overriding public policy objective of enabling safe, efficient, accessible and transparent cross-border payments, the NSO would be incorporated as a **company limited by guarantee (CLG)** which operates on a **not-for-profit basis**. CLG is a corporate structure commonly used for not-for-profit organisations. Unlike a company limited by shares, the owners (members) of a CLG do not have any shares in the company and vote on a one-member-one-vote basis.

While a CLG *may* generate a surplus (when revenues are greater than costs), the surplus cannot be distributed to the members of the CLG as dividends.³⁸ Instead, any surplus must be retained within the CLG and used to further the purposes of the company. For instance, any surplus generated by Nexus (after the initial investment has been repaid) may be used to further improve the service, add new functionality, or – in the case that no enhancement is needed – lower the fees that Nexus charges to participants. Consequently, the CLG corporate structure is most aligned with the public policy goals of Nexus.

The CLG corporate structure adopts an equal voting model (one-member-one vote), where each member is entitled to one vote for any decision requiring the members’ approval. This would ensure parity among the member countries and foster consensus-building in Nexus, aligned with the Nexus key design principles of neutrality and inclusivity.

3.1.3 Choice of home jurisdiction

The initial members of Nexus would need to select the home jurisdiction in which the NSO should be incorporated.

The choice of home jurisdiction is a critical design choice as it would determine the applicable legal, regulatory and oversight framework to which the NSO would be subject. Selecting an appropriate home jurisdiction would also help to engender trust and enhance the overall credibility and attractiveness of Nexus to potential participants.

To help select the most appropriate home jurisdiction, the project team developed a set of selection criteria which include the following factors:

- **legal system**, considering the suitability of corporate structures and whether there is a robust corporate governance and accountability environment and a strong civil justice system;
- **regulatory environment**, considering whether there is mature and stable regulation of payment systems, payment arrangements and services;
- **reputation and image**, considering the jurisdiction's economic and business reputation, level of diplomatic ties, precedence of hosting multilateral entities and level of political stability;
- **ease of doing business** in the jurisdiction; and
- **quality of infrastructure**, including utilities, payments and communications, and transportation infrastructure.

3.1.4 Decision-making bodies and processes

Similarly to any corporate entity, the NSO will have several decision-making bodies. Day-to-day decisions are taken by the Executive Management Team, led by the Chief Executive Officer (CEO).

Certain high-impact decisions, however, are made with the approval of the **Board of Directors** ('the Board'). For instance, these may include decisions on a company's overall strategy and major changes to the scheme rulebook, fee model and risk management policies. The Board is responsible for appointing the Executive Management Team, holding them accountable for the overall objectives and strategy for Nexus. The Board will consist of a representative of each of the joint owners of the NSO,³⁹ and independent directors⁴⁰ who must make up at least 40% of the Board. The role of the independent directors is to ensure that the Board's decisions are in the interests of Nexus as a whole (countering the risk that directors who represent a member country may give undue weight to needs of their own country).

The Board would be chaired by an independent member (ie not representing any member country). The Board of Directors can set up several **sub-committees** – consisting of smaller groups of directors – to focus on issues such as audit, risk and compliance, nomination and remuneration, and amendments of scheme rules.

The Board is, in turn, accountable to the **Members**, who are the joint owners of the NSO.⁴¹ Decisions that have a fundamental impact on the purpose, strategic direction or structure of Nexus would be 'reserved matters' that must be approved by the Members.

Finally, the Board may establish **Advisory Groups** comprising subject matter experts in the participant (IPS operators, FXPs, SAPs and PSPs) and other stakeholder communities, to ensure that any decisions of the NSO consider broader stakeholder views.

3.2 The Nexus Scheme rulebook

The NSO is responsible for defining and updating the **Nexus Scheme Rulebook** ('the Rulebook'), which sets the eligibility criteria and defines the rights and obligations of the different participants in Nexus (IPS operators, FXPs, SAPs and PSPs), and provides a mechanism for dispute resolution.

The Rulebook is supported by several technical implementation guides for participants.

Changes to the Rulebook are managed through a consultative process, outlined in the Nexus Scheme Management Rules, and must be approved by the NSO's Board of Directors.

In designing the Rulebook, the project team benchmarked it against other key payment schemes in use around the world and assessed its compatibility with the regulatory regimes of the ASEAN-5 countries. Where possible, the project team suggested ways to standardise or harmonise approaches between countries to promote greater efficiency and foster alignment to higher standards. Where this was not possible, the project team explored the use of technology and standards to accommodate the necessary differences between countries in the most efficient manner.

The following sections describe a few highlights of the Rulebook.

3.2.1 Scheme adherence and participation

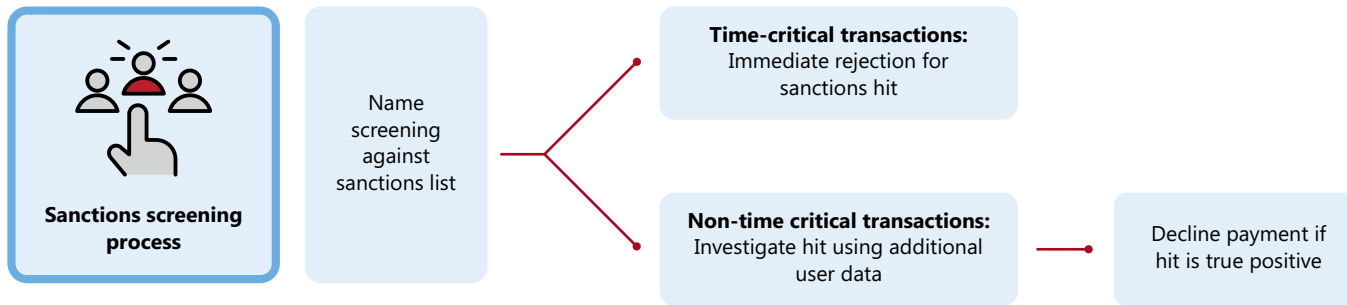
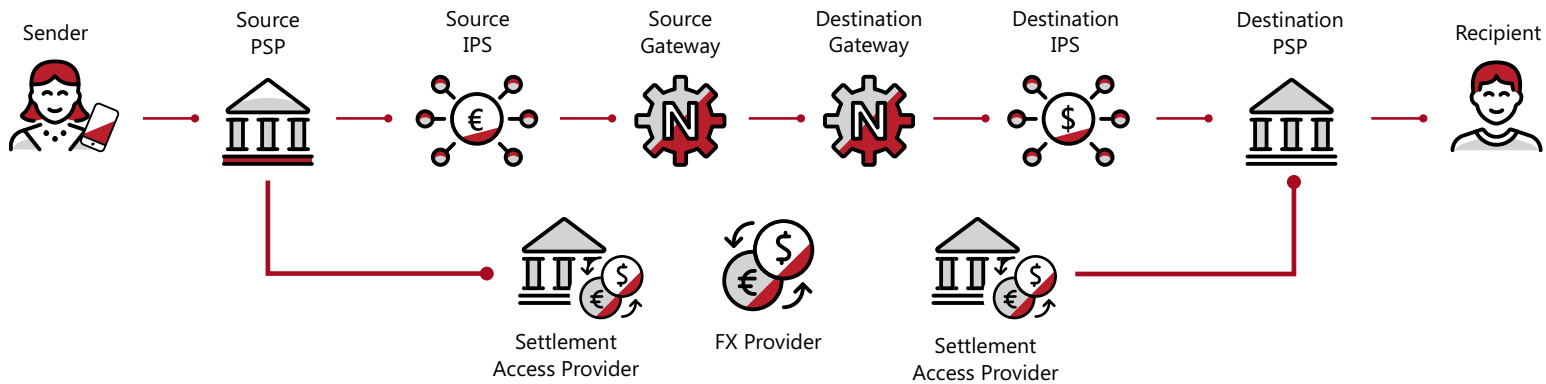
Each participant in Nexus must agree to adhere to the Nexus scheme (ie agree to comply with the rules and obligations in the Rulebook) before they can start processing Nexus payments or provide FX services. IPS operators and third-party FXPs (which provide FX to other PSPs) must adhere directly to the Nexus scheme and interact with the NSO. In turn, IPS operators will manage the adherence of their member PSPs and SAPs to the Nexus scheme. This can be done, for example, by incorporating the Nexus scheme as an addendum to the domestic IPS scheme.

3.2.2 Sanctions screening

Each participant in Nexus is responsible for complying with the laws and regulations that apply in their respective jurisdiction, such as AML/CFT rules. Importantly, the Source and Destination PSPs are responsible for applying **sanctions screening** to Nexus payments. (Nexus does not perform sanctions screening itself.) Typically, the SAPs will also perform sanctions screening, while the FXPs will not, although this depends on the regulatory requirements of the Source and Destination Countries.

The Source PSP can mark a payment as **time-critical** when the use case requires near-instant confirmation of rejection, for example when paying in-store or paying for a taxi, or **non-time-critical**, for example when using Nexus for bill payments. The status of the payment should be set by the Source PSP based on what it knows about the context in which the payment is initiated.

Figure 6: sanctions screening process flow



For all Nexus payments, PSPs must carry out their sanctions screening in real time (ie immediately upon receiving the payment instruction). If the Source PSP has marked the payment as **time-critical** and this payment generates an alert against the sanctions list, the Destination PSP will need to reject the payment, giving immediate certainty of the payment status to the Sender. However, if the payment is marked as **non-time-critical**, the Destination PSP may accept the payment without immediately crediting it to the Recipient and take a defined amount of extra time (no more than a few hours, as defined in the Rulebook) to resolve any sanctions alerts.

The non-time-critical flow addresses a significant challenge with instant cross-border payments. Since each cross-border payment must be screened against sanctions lists, and screening software generates a high rate of false positives, it is possible that some legitimate payments would trigger an alert. It is not possible for someone to review these payments within a few seconds, and so without the non-time-critical flow, these legitimate payments would unfortunately be rejected.

To reduce the percentage of false positive alerts generated by the screening software, the Rulebook facilitates both the Source PSP and Destination PSP to **exchange verified information** of the Sender and Recipient, respectively, for the purpose of sanctions screening – a process known as **account resolution** or **request for information (RFI)**. Using verified information on the Sender and Recipient would reduce the likelihood that payment may be rejected due to inaccurate information keyed-in by the Sender.

3.2.3 Purpose of payments

The AML/CFT and any foreign exchange rules of the participating countries may require the Sender to declare the purpose of cross-border payments. Typically, each country has a different list of **purpose codes**, and PSPs must therefore manage multiple lists. Nexus simplifies this process by asking each country to map their domestic purpose codes to the ISO 20022 External (Category) Purpose Code when sending payment instructions to Nexus, and vice versa when receiving payment instructions from Nexus.

3.2.4 Fraud mitigation

Instant payments may be exploited by fraudsters, so it is important to ensure robust fraud prevention. Each PSP may implement different fraud controls based on their respective risk assessment and domestic regulations. To elevate the minimum standard and instil confidence in the security of Nexus transactions, the Rulebook requires the PSPs to implement several mandatory fraud controls:

- The Source PSP must require multi-factor authentication of the Sender.
- The Source PSP must display the name of the Recipient to the Sender (whenever possible) before it confirms the payment. (The display name will be provided by either the Proxy Directory Operator or the Destination PSP.)
- The display name of the Recipient should be masked by the Proxy Directory Operator or Destination PSP, in accordance with both the data protection regime in the Destination PSP's country and the Destination PSP's terms and conditions as agreed to by the Recipient.

- The Source PSP should also 'rate limit' how many proxy resolution requests a Sender can make without sending a payment, to prevent scammers collecting customers' information and misusing it for the purpose of fraud.
- Source PSPs should implement real-time fraud checks on each transaction before it is submitted to the IPS.

In time, additional fraud mitigation and prevention checks can be implemented by Nexus at a central level to complement the efforts by the individual PSPs in combating fraud. This may include fraud intelligence tools that harness the power of data and network analysis to facilitate PSPs to better predict, detect and stop fraud.

“To elevate the minimum standard and instil confidence in the security of Nexus transactions, the Rulebook requires the PSPs to implement several mandatory fraud controls.”

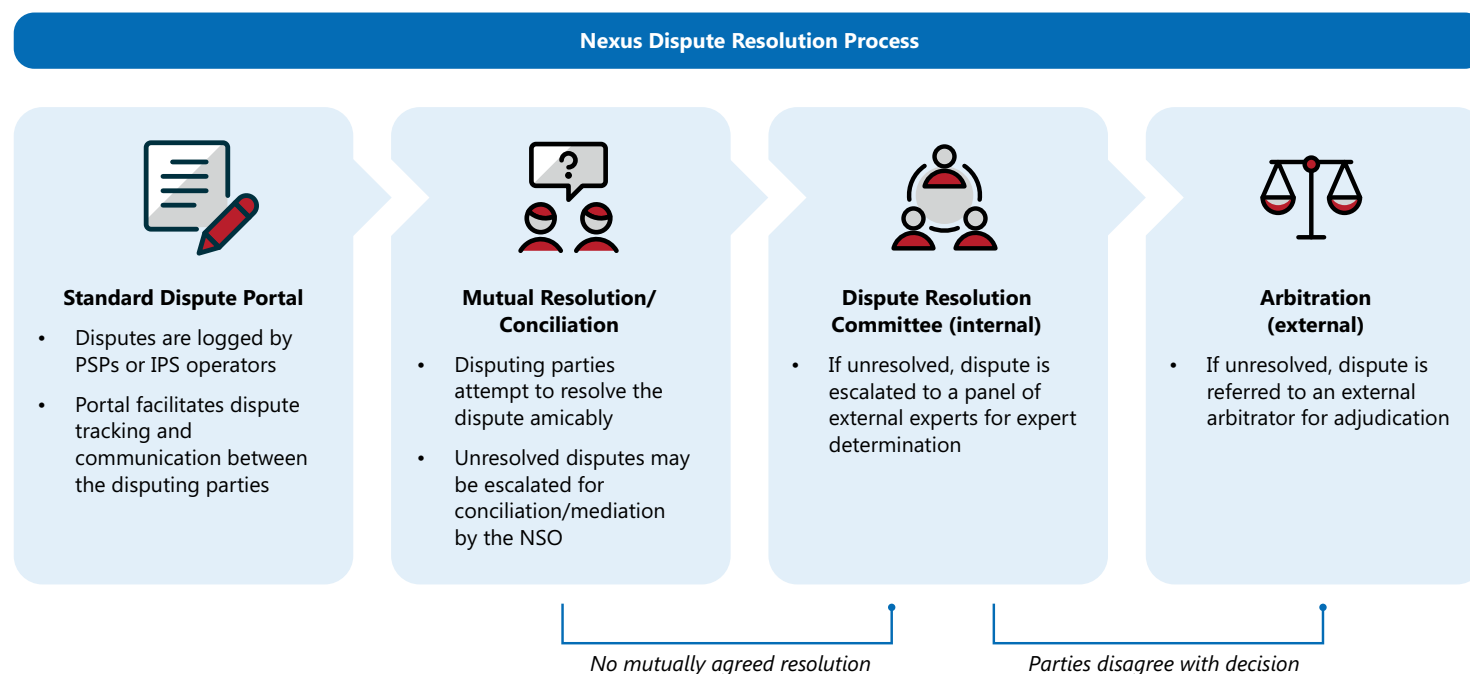


3.2.5 Dispute resolution

Dispute resolution timeframes and processes vary from country to country, meaning that Nexus must define a standardised process that applies to Nexus payments. There are three key aspects to the Nexus dispute resolution framework:

- Nexus will provide a standard Nexus Dispute Portal in which disputes can be raised, tracked and resolved between the Source PSP and Destination PSP. This will facilitate tracked communication between the relevant parties in the dispute and avoid the need for disputes to be handled via email or phone. The portal will also make it easier for disputes to be escalated to the NSO if they cannot be resolved by the Source PSP and Destination PSP. On the longer-term roadmap, Nexus will add support for dispute management via ISO 20022 messages to help automate the process.

Figure 7: dispute resolution process



- The Rulebook will define a standard timeframe within which a PSP must raise a dispute after a payment is processed, and standard timeframes for other parties to respond to disputes.

- There will be a Nexus Dispute Resolution Committee that will be established to deal with disputes that need to be escalated. In the final case, if the parties are not satisfied with the decision of the Nexus Dispute Resolution Committee, they could escalate the dispute to an external arbitrator in accordance with the procedures set out in the Rulebook.

“Nexus will provide a standard Nexus Dispute Portal in which disputes can be raised, tracked and resolved between the Source PSP and Destination PSP.”

3.2.6 Managing credit and settlement risks

Nexus accommodates different IPS settlement models, such as deferred net settlement or immediate settlement in central bank money. (See [Chapter 2.5](#) for details.) Nexus is therefore agnostic to the exact risk management regime within each IPS but places some minimum requirements on the Source and Destination IPS to ensure that credit and settlement risk does not flow from one IPS to another through Nexus. Specifically, for each payment:

- The Source IPS must **ensure funds from the Source PSPs are secured** and made available to the Source SAP (including in case of the insolvency of the Source PSP during the settlement cycle) by implementing appropriate controls (eg immediate settlement in central bank money, prefunding or collateral regime).

- The Destination IPS must also **ensure funds from the Destination SAP are secured** and made available to the Destination PSP (including in case of insolvency of the Destination SAP during the settlement cycle) by implementing appropriate controls (eg immediate settlement in central bank money, prefunding or collateral regime).
- FXPs must **manage their own credit risk exposure with SAPs** bilaterally and vice versa by implementing appropriate controls (eg trust accounts or prefunding requirement).

This approach ensures that a range of domestic settlement models can be accommodated. It also opens the door to other alternative payments infrastructure, such as central bank digital currencies (CBDCs), to connect to Nexus if they can meet the same requirements of providing secured funds and instant payments.⁴²

3.2.7 Data protection

Nexus adopts a two-pronged approach to safeguard the security and privacy of data:

- **Technology and infrastructure-level protection:** As discussed in [Chapter 6.3](#), the design of the Nexus technology supports data protection by ensuring that each IPS can see only transactions that relate to its own PSPs. Visibility into the personally identifiable data in each transaction is restricted to only those who need to know (eg when a dispute is escalated to the NSO). In addition, there are strict requirements on end-to-end physical and cybersecurity protections (eg data encryption, endpoint defence, data storage security).

- **Data protection obligations:** Participants in Nexus are responsible for complying with the data protection and privacy regulations that are applicable to them. Accordingly, the Rulebook requires each participant to have adequate consent (or other legal basis) to collect and process personal data. As to the transfer of personal data to another country, each participant agrees to enter into a data-sharing agreement in which it undertakes to comply with the data protection, data sovereignty and data residency obligations (if any) that shall apply to it as data importer or exporter, respectively.

4 Oversight approach for Nexus



Key takeaways



Interest in operations

Nexus is a cross-border payments scheme that connects multiple domestic IPS. Domestic IPS are normally classified as critical national infrastructure and may be systemically important to the financial system. For this reason, central banks and regulators in countries that connect to Nexus will have a strong interest in how Nexus is managed and regulated, and each may wish to oversee the arrangement to ensure safe, efficient and resilient operations.



Joint Oversight Forum

In discussions with the payment oversight teams in the ASEAN-5 central banks, the project team developed the concept of a **Joint Oversight Forum (JOF)** comprising the central banks/regulators of the participating countries. The JOF would enable effective coordination between the NSO's home regulator and the participating countries' regulators.



Lead overseer

The central bank/regulator in the home jurisdiction of the NSO would be appointed as the lead overseer to coordinate the oversight activity and facilitate information sharing with other central banks/regulators in the JOF.

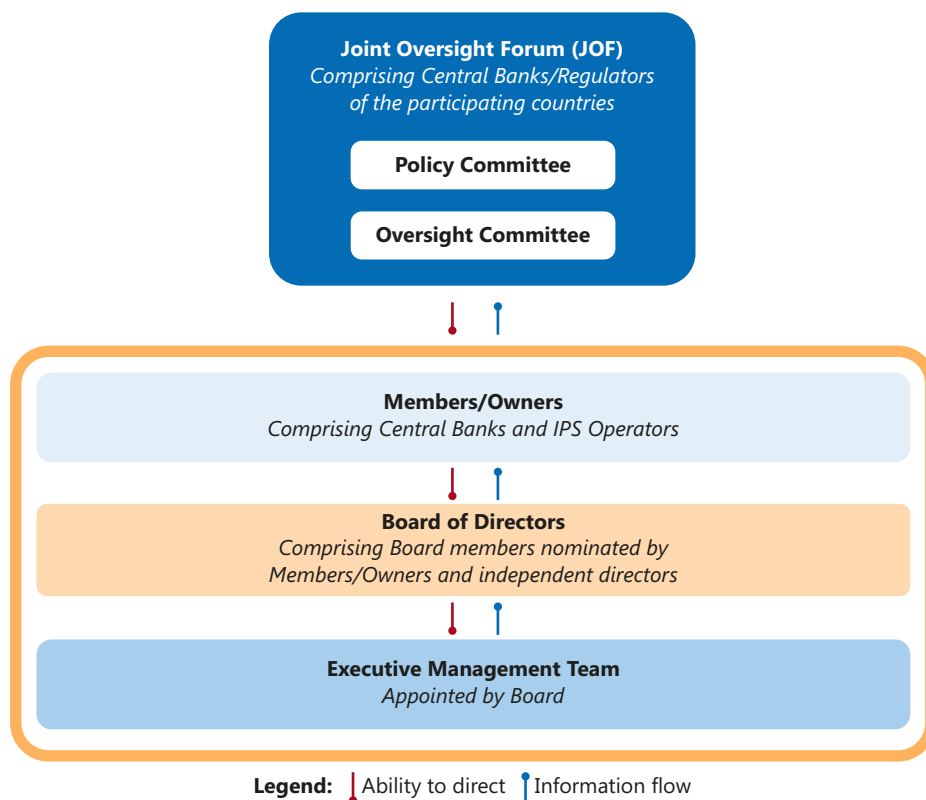


Oversight expectations

The JOF would set oversight expectations and oversee the NSO to ensure Nexus is operated safely and efficiently, consistent with international best practices such as the PFMI. The degree of oversight would be calibrated appropriately to be proportionate to the risks posed by Nexus.

4.1 Joint Oversight Forum

Figure 8 – Joint Oversight Forum



Nexus itself and the NSO would be regulated and overseen by the central bank or relevant regulator in the NSO's home jurisdiction (ie the country in which it is incorporated). This central bank or regulator would act as the **lead overseer** and would have ultimate authority over the oversight of Nexus.⁴³ However, Nexus must also comply with the regulatory and oversight requirements of each of its participating countries. The Joint Oversight Forum would therefore play an important role in ensuring that the requirements placed on Nexus by different countries are not in conflict or mutually incompatible.

The Joint Oversight Forum (JOF) would have three objectives:

- to promote Nexus's alignment with public policy goals, as described in [Chapter 1.4](#);
- to ensure Nexus complies with applicable laws and regulations, and to ensure the NSO has controls and processes in place that would prevent it from posing a risk to monetary and financial stability; and
- to provide a forum for the lead overseer and other regulators to coordinate oversight of the NSO, share oversight findings and raise specific issues.

The JOF could be structured into two tiers, as follows:

- **Policy Committee** which serves as a forum for central banks/regulators to discuss strategic public policy issues pertaining to Nexus (eg implications for monetary and financial stability, cross-border flows, financial inclusion); and
- **Oversight Committee** which serves as a forum for central banks/regulators to share information and coordinate joint oversight and/or supervision to ensure the NSO operates in a safe, efficient and resilient manner.

4.2 Oversight arrangements and decision-making

The PFMI may be used as a starting point for developing the oversight framework for Nexus, where the intensity of oversight is calibrated to be proportionate to the risks posed by Nexus.

The lead overseer will act as the primary contact point between the JOF and the NSO and will manage any requirements such as information requests.

The JOF will aim to make decisions by consensus, but if consensus cannot be reached, a vote may be taken. The JOF may decide to make a recommendation or issue a directive to the NSO Board, consistent with the regulatory powers of the lead overseer and regulators in the JOF. Any decisions made by the JOF will be communicated to the NSO by the lead overseer.

The JOF is intended to support each of the central banks or regulators whose countries participate in Nexus, rather than to supersede them. While each country could still take specific actions against the NSO in line with their own regulatory powers, it would be best if issues are raised for discussion at the JOF and any actions against the NSO are coordinated via the JOF.

4.3 Oversight of the Nexus Technical Operator

The day-to-day operations of Nexus may be outsourced to an experienced firm, known as the Nexus Technical Operator (NTO)

(see [Chapter 2.3.2](#)).

If the NTO is in the same jurisdiction as the NSO, then the lead overseer will be able to apply direct oversight over the NTO. However, if the NTO is in a different jurisdiction, the lead overseer may set oversight *expectations* on the NSO, and it would be incumbent on the NSO to ensure that the NTO complies with such expectations via its contractual relationship with the NTO. The lead overseer could also collaborate with the relevant central bank or regulator in the NTO's country, where applicable.

5 The commercial model for Nexus



Key takeaways



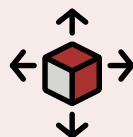
Balancing interests

The proposed commercial model in this chapter describes the revenue opportunity and the costs faced by each Nexus participant (IPS, PSP, FXP or SAP). The model must balance the interests of the Sender and Recipient (who want the lowest overall cost) while providing incentives for all the participants that are involved in processing Nexus payments (ie IPS operators, PSPs, FXPs and SAPs).



Industry consultations

The model has been designed to be commercially viable for participants, when potential revenue, likely costs and any cost savings from taking a multilateral approach are factored in. The model has been developed through workshops with a range of IPS operators, PSPs and FXPs, both in the ASEAN region and globally. The commercial model will continue to be refined through consultation with potential participants and will be finalised in due course by the Nexus Scheme Organisation (NSO).



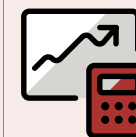
Expanding the scheme

The Nexus project team started with the initial scenario in which Nexus launches with low- or medium-value person-to-person and business-to-business payments within the ASEAN-5 countries. However, the ambition is for Nexus to expand, connecting to IPS in other regions and globally, and the Nexus scheme and technology have been designed to support future connection to a wide range of IPS. The inclusion of additional countries and new use cases will increase the benefits for all existing participants and reduce the payback period for any initial investments.



Benchmarking fees

The Nexus project team has benchmarked the likely fees from each participant and the cost structure they face to confirm that Nexus will be competitive with existing cross-border payment options and can feasibly provide cross-border payments where the total cost to the Sender is within the G20's target of 3% of the value of the transfer.



Financially sustainable

The NSO itself must be financially sustainable. The NSO will earn revenue by collecting a fee per transaction that covers the costs of running Nexus. The initial members will need to cover the initial setup costs and the operating costs immediately after launch (until Nexus's volumes become sufficient to cover day-to-day costs).

5.1 Costs and transparency for the Sender

The G20 Roadmap for Enhancing Cross-border Payments sets the target that the global *average* cost of sending a cross-border *retail* payment should be no more than 1% by end-2027, and that no corridor should be above 3%.

For migrant remittance payments specifically, the G20 adopts the UN Sustainable Development Goal that such payments should cost no more than 3% on average (See [Chapter 1.3](#)). This means that if a Sender sends a payment of \$200, the total fees (including invoiced fees and deductions) should be no more than \$6.

Through workshops with a range of IPS operators, PSPs and FXPs, both in the ASEAN region and globally, the Nexus project team has benchmarked the likely fees from each participant and the cost structure they face. These benchmarks were used to confirm that **Nexus can feasibly provide cross-border payments where the total cost to the Sender is within the G20's 3% target** (and hopefully lower), while still allowing each participant to earn sufficient revenue from the payment to make it commercially viable to join Nexus. Importantly, Nexus can achieve this at an overall cost to the Sender

that is **competitive with alternative methods of making cross-border payments**. The cost to the Sender for these alternatives varies depending on the type of provider and the corridor used but are often between 2% and 5% of the value of the payment, and are sometimes as high as 10%.

5.1.1 Transparency of fees and FX rates

The Nexus Scheme Rulebook sets requirements around the transparency of the fees and FX rate that the Sender will be charged, so that the Sender can make an informed decision before proceeding with the payment. For one example of how fees might be presented, see [Chapter 2.2](#).

Specifically, before the Sender approves a payment, the Source PSP must display:

- the exact amount that will be debited from the Sender's account, in the Sender's currency; and
- the exact amount that will be credited to the Recipient's account, in the Recipient's currency.

Each Source PSP has the discretion to charge either an invoiced fee (which appears as a separate line item on the Sender's account statement), a deducted fee (which is deducted from the value of the payment itself) or a combination of both.

If an invoiced fee is charged, it must also be shown to the Sender before they approve the payment.

The Source PSP must also show the Sender one of the following:

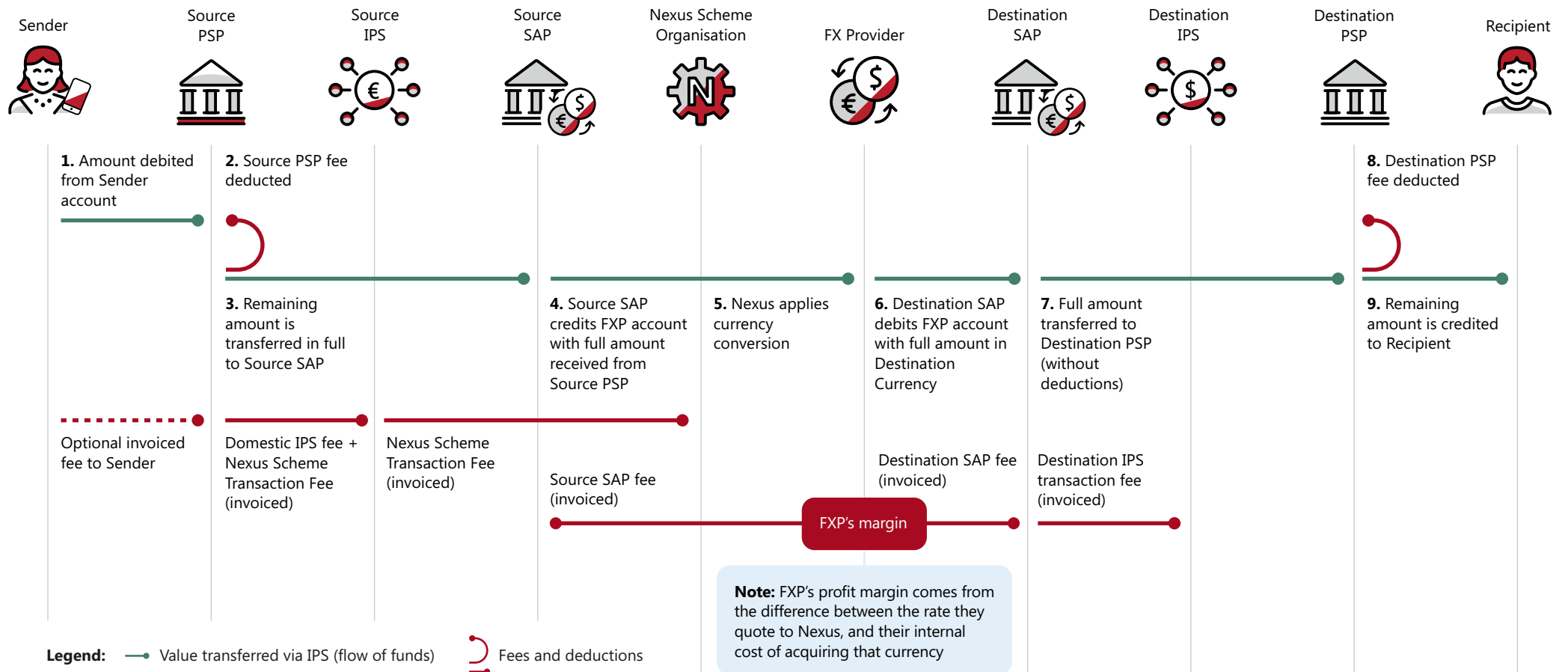
- an effective exchange rate (including any deductions), which is simply the ratio between (a) the amount debited from the Sender's account and (b) the amount credited to the Recipient's account; or
- total deducted fees + exchange rate after fees – in this option the Source PSP shows the total deducted fees charged by both the Source PSP and Destination PSP together (in the Sender's currency). The exchange rate shown is the ratio between the amount after fees and the amount credited to the Recipient's account.

This transparency requirement is designed to ensure that the Sender can see, with certainty, what the Recipient will receive for a given amount of the Source Currency. However, it leaves sufficient discretion to PSPs to present their fee model as they wish, given that some PSPs prefer to show the best exchange rate with fees, and others prefer to show a single effective exchange rate that embodies all fees.



5.2 The proposed fee structure for IPS, PSPs, FXP's and SAPs

Figure 9 – fee structure in Nexus



As with any cross-border payment service, each of the participants in a Nexus payment needs to be reimbursed for the service they provide. The Nexus Scheme specifies the fee arrangements for four participants: the Source PSP, the NSO, the FXP, and the Destination PSP:

- The **Source PSP** has discretion over the fees that it charges to the Sender. However, it may collect the fee as a deduction from the payment amount, or as a separate 'invoiced fee' that appears as a separate line item on the Sender's account statement, or a combination of both. The Nexus transparency requirements (see [Chapter 5.1.1](#)) ensure that the Sender can understand the total cost of sending the payment regardless of how those fees are collected.

- The **NSO** charges a Nexus Scheme Transaction Fee to the Source IPS. This is an invoiced fee, charged to the Source IPS (and not deducted from the value of the payment). This is described in [Chapter 5.5](#).
- The **FX Provider (FXP)** is not permitted to charge a *fee* to any party or make a *deduction* from the value of the payment.⁴⁴ Instead, it must quote an exchange rate that is sufficient to cover all its costs, including any fees it must pay to the Source SAP and Destination SAP, and any necessary profit margin. The exchange rates that the FXP offers are at the sole discretion of the FXP.

- The **Destination PSP** charges a *Destination PSP fee*, which is deducted from the value of the payment before the remaining sum is credited to the Recipient's account. The exact level and structure of the Destination PSP fee would be set by the NSO but would need to be known in advance of the payment being made so that Nexus can calculate the exact amount that would be credited to the Recipient.

The Destination PSP fee is intended to reimburse the Destination PSP for processing inbound Nexus payments. The Destination PSP fee is particularly important for PSPs that receive many more payments than they send, such as PSPs in net remittance receiver countries, and which may not recover their initial investment through Source PSP fees alone. The existence of the Destination PSP fee therefore ensures that the network is not restricted only to PSPs that can be confident of sending a high volume of outbound payments.

For the supporting participants – the Source IPS, Destination IPS, Source SAP and Destination SAP – the Nexus scheme does not define the fee arrangements, as these are negotiated bilaterally (between the IPS and PSPs, and between the SAPs and FXPs). However, none of these participants are permitted to make a deduction from the value of the payment as it is transferred (as this would make it too complex for Nexus to calculate the amount that would be credited to the Recipient's account), and so they must instead charge an invoiced fee after the payment is complete.

5.3 Deciding whether to join Nexus

Given the fee structure described above, each potential participant will make their own **cost-benefit analysis** to assess whether the revenue they could earn is likely to exceed the upfront and ongoing costs they will incur to participate in Nexus.

As described above, participants will earn **revenue** either from the Sender (for the Source PSP and Destination PSP) or by charging other participants (for the IPS, FXP and SAPs). Every participant will also incur **onboarding costs** to integrate with Nexus, such as supporting new payment flows in their payments engine, or training staff to use a new service. Once they start processing Nexus payments, they will face **ongoing operational costs**, including their internal costs of processing Nexus payments, as well as any fees they must pay to other participants (including the NSO).

Taken together, this means that the incentive to join Nexus will depend on:

- the size of the **total addressable market**, including the size of payment flows between existing countries in the network, and countries expected to join in the foreseeable future;
- the number and type of **use cases** that Nexus supports (such as person-to-person, business-to-business, or person-to-merchant);
- the **volume and average transaction value** of payments through Nexus;
- the **average fee as a percentage of the transaction value**;
- the **upfront costs** of joining and integrating with Nexus;
- the **ongoing costs** of processing Nexus payments; and
- any **cost savings** achieved by improving or automating existing processes.

The project team considered each of these levers when designing the commercial model, scheme and technology for Nexus.

5.3.1 Assessing the revenue opportunity

To estimate the size of the **total addressable market**, the project team commissioned a specialist data provider to evaluate the payment flows between each of the ASEAN-5 countries (intra-ASEAN flows), as well as the most significant flows between the ASEAN-5 as a whole and the rest of the world (extra-ASEAN flows). This analysis showed there is a sizeable flow of intra- and extra-ASEAN payments that could in future be processed by Nexus.

Importantly, if countries beyond the ASEAN-5 were to join in the foreseeable future, the additional flows would increase the benefits and reduce the payback period for each participant (including the NSO).⁴⁵ The same applies if Nexus were to support new use cases, such as person-to-merchant (P2M) payments or payments initiated through a QR code.

The **average transaction value** depends on (a) the **use cases** (ie types of payment) that are being sent through Nexus, and (b) any **caps** on the payment size that are imposed by IPS operators or PSPs. Nexus will start by offering person-to-person (P2P) payments, which are generally low or medium average value, and business-to-business (B2B) payments, which tend to be medium average value. However, the average transaction value will be limited should the IPS operators and PSPs (or their regulators) wish to set a limit for cross-border payments which is less than that set for domestic payments; doing so will limit the average transaction value. If those limits are raised over time (for example, as IPS operators and PSPs become more comfortable managing instant cross-border payments), it will allow larger payments, such as medium-value B2B

payments, to flow through Nexus and increase the average transaction value and volumes flowing through existing participants, with no additional effort on their part.

Regarding the **average fee as a percentage of a transaction**, there is a trade-off between the interests of the Sender (who would like a lower average fee) and the participants (who would like a higher average fee). The Nexus Scheme Rulebook does not set a cap on the overall cost to the Sender, so the final cost to the Sender in practice will depend on the level of competition between participants (see [Chapter 5.4](#)).

5.3.2 Assessing the costs of participation in Nexus

Ultimately, all costs of a payment through Nexus are borne by the Sender. Therefore, higher costs at any point in the process mean that the Sender must pay more to deliver the same amount of funds to the Recipient. The Nexus project team spoke to a wide range of PSPs and FXPs to understand the factors that currently impact their cost of providing payments or FX, and the scale of changes they would need to make to integrate with Nexus. The team also spoke to

technology providers and existing IPS operators to establish the likely cost of building and operating Nexus.

Based on these insights, Nexus has been designed with several features to help minimise the cost to participants, by incorporating reusability, scalability and standardisation in its design. Notably, this is achieved by:

- **Reusing existing instant payment system infrastructure** (ie domestic IPS) and the robust liquidity and credit risk management in those systems, rather than creating a new cross-border clearing and settlement mechanism. This means that Nexus requires only a relatively light core infrastructure, which (simplistically) just manages communication between IPS via APIs and ISO 20022 messages.
- **Adopting an ‘integrate once’ model** which minimises future changes to a PSP or IPS operator’s core systems when new countries join the network. This is significantly more cost-effective than making changes every time the country connects to a new country bilaterally, or than using a different type of provider for each different country.
- **Reusing a PSP’s existing secure connection to its IPS**, rather than asking each PSP to create a new connection to Nexus.
- **Using widely adopted standards**, such as RESTful APIs and ISO 20022 payment messages (see [Chapter 6.2](#)).
- **Streamlining processes that are duplicative or highly administrative.** For example, Nexus encourages the use of the standardised Correspondent Banking Due Diligence Questionnaire (CBDDQ) by FXPs when onboarding PSPs, and by SAPs when onboarding FXPs.
- Providing **cost savings** by using standards and standardisation. For example, by using the ISO 20022 message standard, which is already becoming widely adopted for cross-border payments.

5.4 The role of competition in keeping fees low

The Nexus Scheme Rulebook does not set a cap on the overall cost to the Sender in order to meet the G20 targets. Instead, the Nexus commercial model relies on competition between different participants.

The Nexus model separates out the different roles that a financial institution can play in a cross-border payment to increase competition between those roles and level the playing field (for example, by allowing smaller FX dealers to compete with larger international financial institutions):

- PSPs compete to send specific payments, because the Sender may compare the fees and FX rates offered by different PSPs. The Nexus Scheme transparency requirements discussed in [Chapter 5.1.1](#) also support Senders to compare different PSPs.
- FXPs compete to offer the best rates to Source PSPs.
- SAPs compete with each other to offer services to FXPs.
- The Nexus service itself is in competition with alternative cross-border payment services.

In addition to the competition between participants, Nexus also imposes strict transparency requirements (see [Chapter 5.1.1](#)) to help end-users make informed choices about which PSP they want to send payments through.

“The Nexus model separates out the different roles that a financial institution can play in a cross-border payment to increase competition between those roles and level the playing field.”



5.5 The Nexus Scheme Organisation

The **Nexus Scheme Organisation (NSO)** would operate on a not-for-profit basis, meaning that any surplus after costs will be reinvested into the service.

5.5.1 NSO fees

The NSO does not charge a joining fee or annual membership fee to PSPs, FXPs and SAPs to minimise barriers to joining Nexus. Once a participant is onboarded with Nexus, the NSO will charge the Source IPS a **Nexus Scheme Transaction Fee** for each payment through Nexus. This fee will be set on a '*cost recovery plus*' basis, so that the fee covers the costs of providing the service plus a modest margin which can be re-invested to enhance existing services or add new features or functionalities.

The Source IPS, in turn, will charge this fee to the Source PSP (or in some cases, split it between the Source PSP and Source SAP).

The Nexus Scheme Transaction Fee is therefore ultimately covered by the total fees paid by the Sender, so it is important that the service provided by the NSO (and Nexus Technical Operator) is cost-effective.

5.5.2 NSO costs and funding requirement

The NSO will incur costs to set up Nexus, including the organisation, processes and technology, and to cover operating costs for a period after launch as Nexus payment volumes may not yet generate sufficient revenue to the NSO. This setup cost and the early-stage operating deficit will therefore need to be funded by an initial investment from the initial members. Over time the income from fees would allow the NSO to recover the initial costs of building Nexus; this payback period is estimated at eight to ten years if Nexus connects only the ASEAN-5 countries but would be shorter if it expands to other countries.

Once the initial startup costs have been recovered, the NSO may choose to reinvest any surplus in new services, and/or potentially reduce the transaction fee.

The final decision and calibration of the fee model would be undertaken by the NSO.

6 Technology for Nexus



Key takeaways



Optimising the cost of ownership

The Nexus architecture is designed to optimise the total cost of ownership across the network, to respect data protection and privacy requirements, and to ensure resilience and scalability.



Nexus Gateway software

Nexus uses APIs and ISO 20022 messages to provide a standardised way for one IPS to communicate with another, via the Nexus Gateway software. The Nexus Gateways manage addressing, proxy resolution, FX conversion and payment processing.



Cost-effective architecture

The Nexus architecture is designed to be cost-effective, highly scalable and resilient, and flexible enough to accommodate cloud and on-premises installations depending on the requirements of each IPS.



Secure data

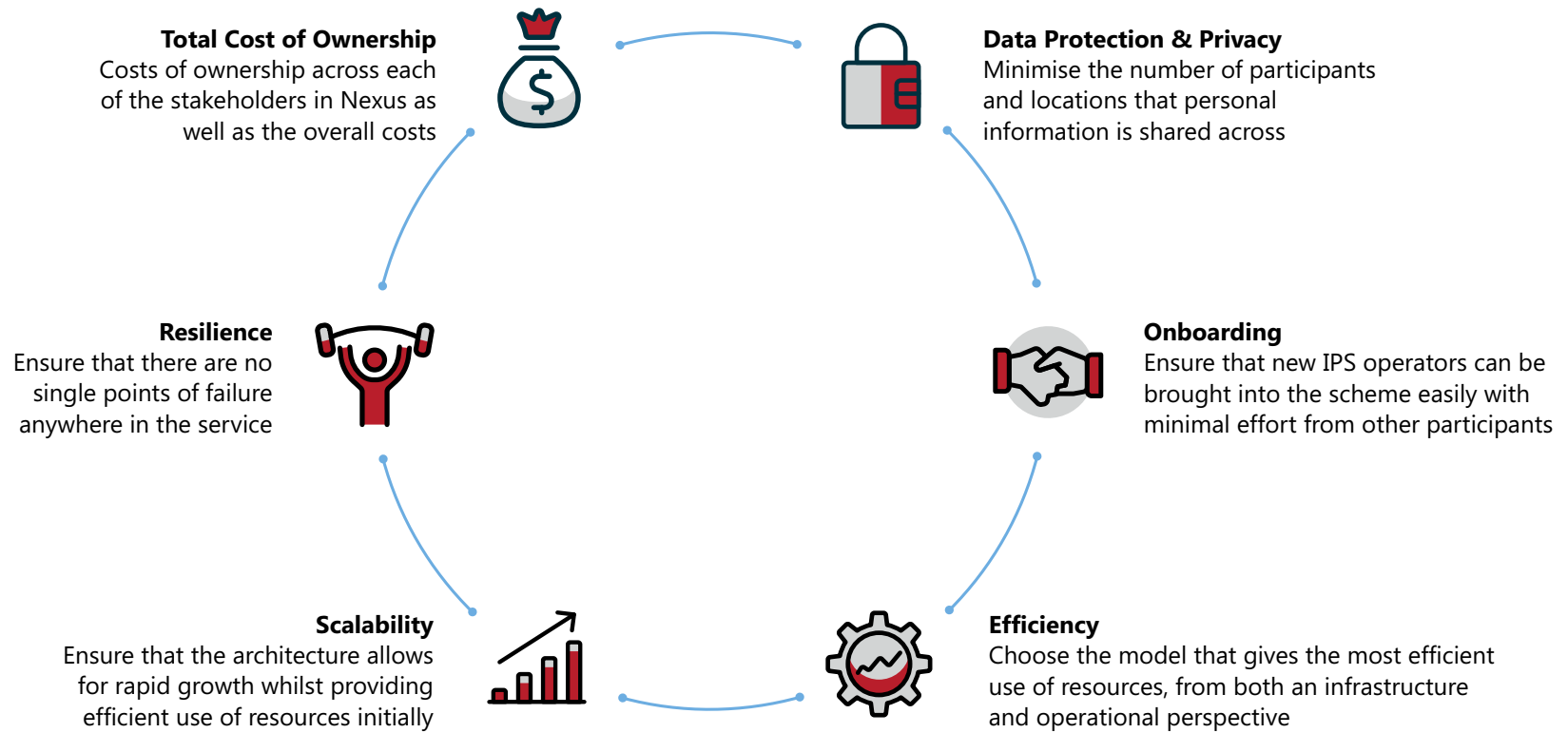
Data relating to transactions are visible only to the IPS and PSPs that were involved in those transactions. Sensitive data are segregated by country and can be stored in the cloud or on-premises if required by local data residency requirements.



Technical documentation

Detailed technical documentation for Nexus is available to central banks and payment system operators on request.

6.1 Technology design principles



The Nexus functionality, technology architecture and infrastructure model were designed around the following principles:

- **Optimising total cost of ownership:** All the costs of processing a Nexus payment, across all participants, are ultimately passed on to the Sender through fees, deductions and the FX rate. Therefore, the infrastructure model should optimise the total cost of ownership holistically across all participants (including IPS operators, FXPs and PSPs) and not only those costs that are directly incurred by the Nexus Scheme Organisation (NSO) or Nexus Technical Operator (NTO).

- Costs must also be fairly shared across all the participants in the scheme. This means that custom requirements from a specific IPS operator may be accommodated if (a) accommodating the requirements does not increase the total cost of ownership across all participants, or (b) the costs of accommodating IPS operator-specific requirements can be separated out and charged back to the IPS operator with those requirements.
- **Data protection & privacy:** Much of the data processed by Nexus will contain personally identifiable information, ie sensitive information such as names, addresses and account details. Nexus must therefore protect this data from unauthorised access and must enable data to be stored in a way that is consistent with data protection, data sovereignty and data residency requirements. These requirements might differ from country to country.

- **Ensuring resilience:** Nexus will connect domestic payment systems which themselves may be designated systemically important or qualify as critical national infrastructure. Typically, these domestic systems must operate on a 24/7/365 basis, with very little downtime, and so Nexus must be resilient enough to operate 24/7/365, with strong disaster recovery measures.
- **Scalability:** The Nexus infrastructure should be scalable so that it is initially cost-effective for the starting volumes, but able to scale to much higher volumes over time.

- **Efficiency:** The Nexus service should be designed to make efficient use of resources, from both an infrastructure and operational perspective. Design choices should be evaluated against the extent to which they either simplify or introduce complexity to the operations of Nexus.
- **Onboarding:** The ambition is for Nexus to expand beyond the initial countries, so the NSO/NTO must ensure that new domestic IPS can be brought into Nexus easily with minimal effort from – and zero disruption to – existing participants. It must be easy to make changes to the Nexus service without requiring highly coordinated participant testing events.

6.2 Communicating with Nexus

6.2.1 APIs

Nexus communicates with participants using a collection of APIs (application programming interfaces). The body of these API requests and response will contain reference data in the JavaScript Object Notation (JSON) format, or ISO 20022 messages in XML format.

JSON APIs are used mainly for reference data, such as the details of the countries available in Nexus and the address types in those countries.

Nexus APIs may be *synchronous* or *asynchronous*. Synchronous APIs give an immediate response and are used for requests that Nexus can answer without communicating with any other systems, such as reference data and FX quotes. For asynchronous APIs, Nexus acknowledges the request but sends the response later, after communicating with other participants (such as the Destination IPS, Destination PSP and proxy directory).

6.2.2 ISO 20022 messages

All payment instructions and payment-related messages to Nexus must be in the ISO 20022 format, following the Nexus usage guidelines. For each message, there are specific usage guidelines that ensure Nexus and participants can correctly process the message. The guidelines are aligned with the *CPMI's Harmonised ISO 20022 data requirements for enhancing cross-border payments*⁴⁶, and the *CBPR+*⁴⁷ guidelines for cross-border payments, followed by the *IP+*⁴⁸ guidelines for instant payments. Where there are conflicts between these guidelines, Nexus follows the CPMI guidance.

The main payment instruction is pacs.008 (FI to FI Customer Credit Transfer), and the response to this instruction is the pacs.002 (FI to FI Payment Status Report). Each pacs.008 payment instruction must contain only one payment.

Nexus also uses acmt.023 (Identification Verification Request) for proxy and account resolution, and acmt.024 (Identification Verification Report) as the response.

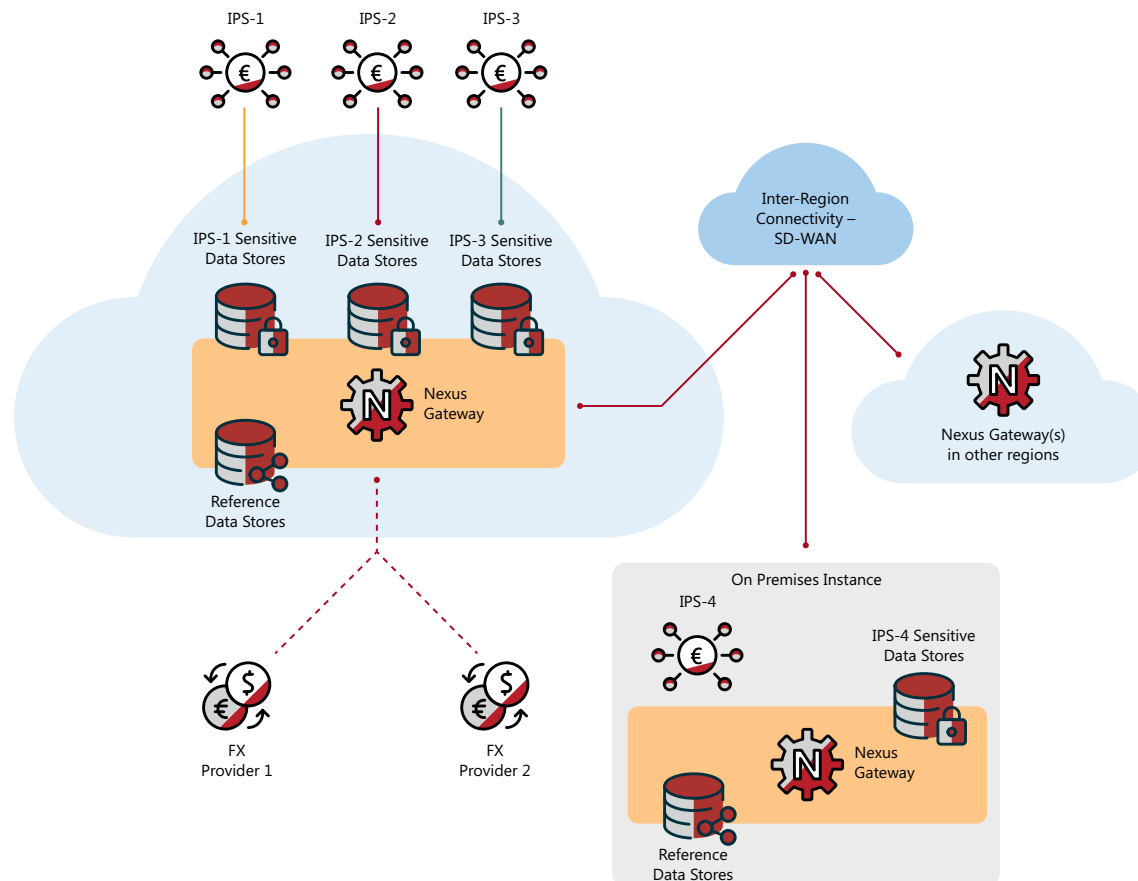
6.2.3 Message translation

Not all IPS use ISO 20022 for domestic payments, for example some use the ISO 8583 standard or a proprietary domestic standard. In this case, the IPS must translate any message to the Nexus standard before sending messages to Nexus (and after receiving messages from Nexus).

Alternatively, an IPS can choose to support the full Nexus-standard ISO 20022 messages domestically. This approach requires more upfront work from the IPS and its member PSPs but maximises interoperability with other payment systems; it would also align the domestic message format with the ISO 20022 messages that PSPs will need to use for cross-border payments through Swift and other cross-border networks, and so could improve harmonisation and simplify messaging overall for PSPs in the long term.

6.3 Nexus infrastructure models

Figure 10: Nexus architecture models



6.3.1 Standard model: Shared Nexus Gateway, hosted in the cloud

By default, Nexus Gateways will be hosted in the cloud, and a single Gateway can process payments for multiple IPS.

Within each Shared Nexus Gateway:

- The reference data set, which does not contain personally identifiable information, is shared between, and accessible to, all IPS. This is known as the **Reference Data Store**.
- Each IPS operator will have their own dedicated and separate **Sensitive Data Store** (database), which contains only transactions that are sent from or to that country, along with related messages such as proxy resolution requests.

Owing to the pricing structure of cloud infrastructure, allowing multiple IPS to share the computing capacity of a Gateway – while separating and insulating sensitive data – is an efficient way of optimising costs while maintaining security. The costs of running the Shared Nexus Gateways would be factored into the Nexus Scheme Fee (see [Chapter 5.2](#)).

If Nexus expands beyond one geographical region, a second cloud region could be used to host a second Gateway, with that Gateway being used by IPS operators in the new region. (Both regions would be connected to each other (see [Chapter 6.4](#)).

6.3.2 Non-standard models

Some IPS operators have their own technical requirements or policies that could mean the default cloud-hosted Shared Nexus Gateway model may not be suitable for them. Concerns such as data residency or government policies on use of the cloud may mean that a non-standard approach is required. There are three main non-standard approaches that an IPS operator could choose:

- **An IPS operator-Dedicated Nexus Gateway, hosted on the Nexus cloud:** This Gateway would be functionally identical to the Shared Nexus Gateway, and hosted on the same cloud. However, this Gateway would only process transactions for a single IPS operator (and so is 'dedicated' to that IPS operator). This model can give the IPS operator more control over the configuration and access to that Gateway infrastructure. However, as the basic costs of running that Gateway are not shared across multiple IPS operators, it is slightly more expensive to run a Dedicated Nexus Gateway.

- **An IPS operator-Dedicated Nexus Gateway run on an IPS operator-selected cloud:**

An IPS operator could choose to run a Dedicated Nexus Gateway on a cloud service provider of their own choosing (where the cloud service provider is different from the one used by the NTO), or on their own cloud service provider account (if using the same cloud service provider as the NTO). The specific cloud service provider must be assessed by the NTO before this can be approved. Again, this will be more expensive than simply using the Shared Nexus Gateway.

- **On-premises Dedicated Nexus Gateway:** Where an IPS operator has local regulatory requirements which require the processing of transactions onshore, or a policy against the usage of the cloud, the Nexus architecture allows the NTO to deploy a Gateway to local servers in the IPS's own data centre. The service would be managed remotely by the NTO, using a Platform as a Service (PaaS) approach.

Each of these non-standard options adds complexity and has higher running costs than the Shared Nexus Gateway. While these incremental costs will initially be paid by the NTO, the IPS operator choosing a non-standard model will be expected to cover the difference between the cost of providing a Shared Nexus Gateway and the cost of providing the custom model they select.

6.4 Connecting to Nexus

IPS operators that use a Shared Nexus Gateway (cloud-hosted) will connect to Nexus using a virtual private network (VPN) over the internet. This allows the IPS operators to use their existing network infrastructure and circuits to establish a connection through a VPN tunnel. VPN connectivity can be set up in a matter of hours with no need to purchase additional hardware or circuits.

IPS operators that host an on-premises Dedicated Nexus Gateway need to create only one connection to a Software Defined Wide Area Network (SD-WAN) which will manage connections between that IPS and the rest of the Nexus network.

FXPs will connect directly to the Nexus Gateway implementation that is closest to them geographically. FXP connectivity to Nexus will use HTTPS direct over the internet. Whilst these data are commercially sensitive, they will not contain any personally identifiable information and forms part of the Nexus Reference data. These data will still be encrypted both in transit and at rest to ensure that they remain secure.

Proxy Directory Operators will not connect directly to Nexus. Instead, they will be connected to Nexus indirectly via the IPS operators for which they provide domestic proxy lookup services.

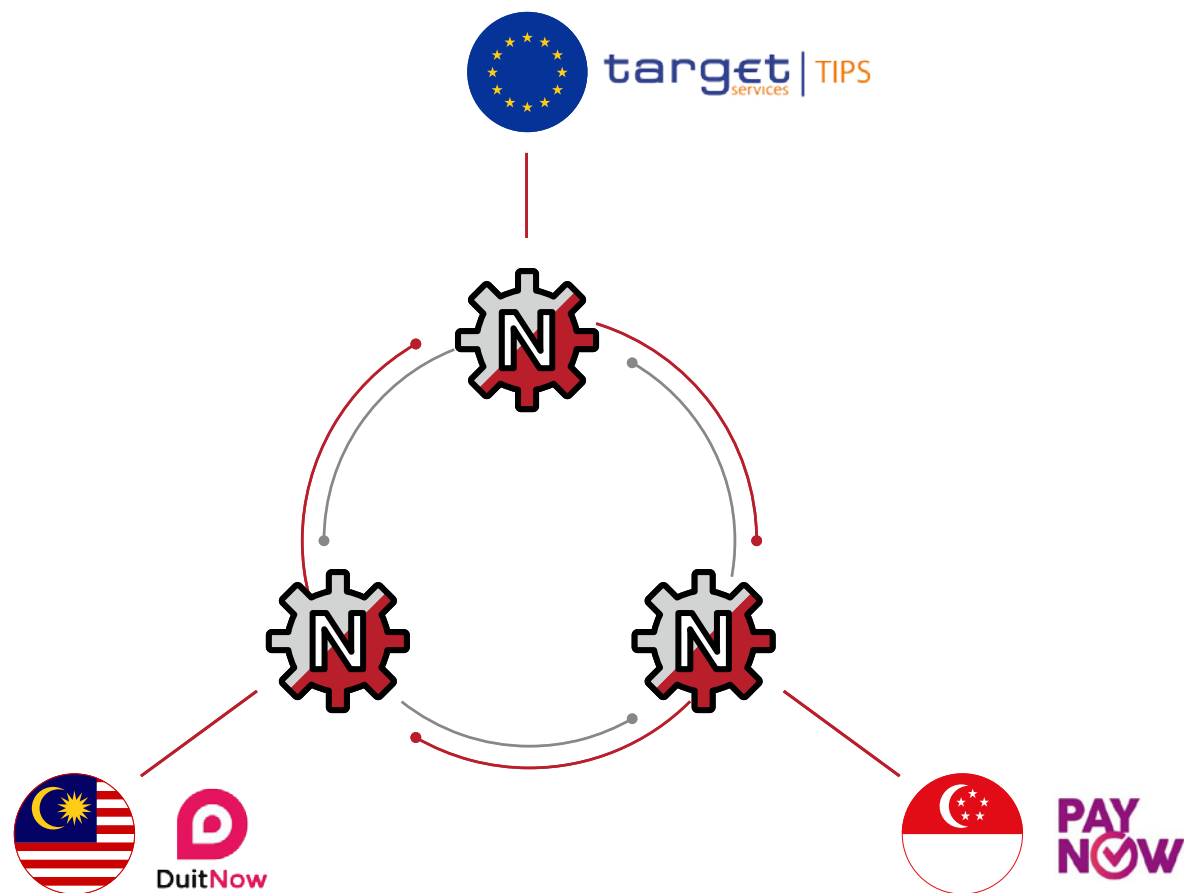
PSPs and SAPs will not connect directly to Nexus. Instead, they will be connected to Nexus indirectly via their existing secure connection to the IPS, with the IPS relaying requests and responses between Nexus and the PSP.



7 Annex: The Nexus technical proof-of-concept between the Eurosystème, Malaysia and Singapore



Figure 11 – the proof of concept connected the Eurosystem, Singapore and Malaysia



Based on the blueprint published in 2021, in 2022 the Nexus project team built a working prototype of the Nexus Gateway and used it **to connect the test systems of three established IPS:**

- the Eurosystem's **TARGET Instant Payment Settlement (TIPS)** system, operated by the Bank of Italy on behalf of the Eurosystem and overseen by the European Central Bank;
- Malaysia's **Real-time Retail Payments Platform (RPP)** operated by PayNet and overseen by the Central Bank of Malaysia; and
- Singapore's **Fast and Secure Transfers (FAST)** payment system, operated by Banking Computer Services (BCS) and overseen by the Monetary Authority of Singapore.

Each of these payment systems is important to the functioning of their respective economies. As a rule, since experimental changes should never be made directly on the live or 'production' version of a system, the Nexus proof of concept did not connect to these live payment systems or process 'real money' payments. Instead, each IPS operator set up an exact replica of its domestic payment system and filled it with manually generated testing data. No real customer information or sensitive data were used at any point in the proof of concept.

To enable the use of proxies (such as mobile phone numbers) in the proof of concept, each IPS operator also created replicas of the following proxy resolution services: TIPS's **Mobile Proxy Lookup (MPL)** service; Malaysia's **DuitNow**; and Singapore's **PayNow**.

The three systems were connected by Nexus Gateways, which managed the communication between each IPS and other IPS on the network. Three instances of the Nexus Gateway were set up in the BISIH's cloud environment – one per IPS operator (hence, a Singapore Gateway, a Malaysia Gateway and a TIPS Gateway).

After ensuring there was a secure network connecting the different IPS, the development team built an API gateway to manage efficient communication between each IPS and a Nexus Gateway. A message queue system was set up to enable communication between each Nexus Gateway and all the other Nexus Gateways. A reference data service was built to allow each IPS to provide the information needed by Nexus and PSPs to process cross-border payments to that IPS, along with an administration portal (graphical user interface) to allow IPS operators to update that information without directly using the APIs.

With this foundation in place, the team built a service to connect the three proxy directories, followed by a service to connect the IPS payment processing engines themselves. Communication between Nexus and the IPS operators relied on ISO 20022 messages and some custom APIs. Although all three IPS used ISO 20022, there were cases where the domestic message formats did not fully align with the Nexus messages, and so IPS operators needed to apply message translation to the domestic messages before sending them to Nexus. Finally, the team built an FX Service that can accept rates from FXPs and provide these to PSPs at the point they initiate a payment.

The software and infrastructure developed was proof of concept grade, meaning that much more work would be required on resilience, performance and security before it could be used for 'real money' payments.

In parallel to the technical work, a separate workstream developed a draft scheme and governance framework for the Nexus scheme, to ensure that the technology supported compliance with the necessary rules, obligations, transparency requirements and business processes. These deliverables were further developed in Phase 3 of the project, as described in [Chapter 3](#).

The lessons from the proof of concept are described in more detail in the 2023 report⁴⁹ and were the basis for a redesign of key parts of Nexus during the most recent phase of work.

Acknowledgements

The BISIH Singapore Centre would like to thank our partner central banks: Bank Indonesia, Central Bank of Malaysia, Central Bank of the Philippines, the Monetary Authority of Singapore, and the Bank of Thailand. We would also like to thank their respective IPS operators: Bank Indonesia (operator of BI-FAST in Indonesia), PayNet (Malaysia), the Philippines Payments Management Inc. and BancNet (the Philippines), Banking Computer Services Ltd (Singapore) and NITMX (Thailand).

We also thank the many workshop participants from banks, fintech companies, FXPs, infrastructure providers and other industry participants for their time, insights and feedback. Feedback from central banks around the world was invaluable in ensuring that Nexus is future-proofed for countries outside the ASEAN-5.

For this phase of the project, Oliver Wyman advised BISIH on the development of the governance, scheme and oversight framework, and supported BISIH in shaping the business case. In addition, Baker McKenzie provided legal support for this work. FXC Intelligence supported the project with cross-border payments data and market intelligence. iPlan supported work on the functional design of Nexus. CGI supported work on the architecture, infrastructure and network model for Nexus. We are grateful to all teams for their dedication and work throughout the project.

Finally, we would like to thank colleagues across the BIS Innovation Hub and our project partners for their comments on this report. Of course, the final design and any errors are the responsibility of the project team, and no endorsement is implied.



Endnotes

- 1 Often known as 'fast' or 'real-time' payment systems.
- 2 See www.fsb.org/wp-content/uploads/P230223.pdf
- 3 These are five nations from the 10-member Association of Southeast Asian Nations (ASEAN).
- 4 See www.mas.gov.sg/news/media-releases/2021/singapore-and-thailand-launch-worlds-first-linkage-of-real-time-payment-systems
- 5 See www.bnm.gov.my/-/cross-border-gr-payment-linkage-between-malaysia-and-thailand
- 6 The PayNow-UPI service allows payments to be addressed using a mobile phone number, UPI identity or Virtual Payment Address (VPA). See www.mas.gov.sg/news/media-releases/2023/launch-of-real-time-payments-between-singapore-and-india
- 7 See www.mas.gov.sg/news/media-releases/2023/launch-of-cross-border-real-time-payment-systems-connectivity-between-singapore-and-malaysia
- 8 In addition, Brunei, Vietnam and Laos have since signed up to the Regional Payments Connectivity MoU. See www.mas.gov.sg/news/media-releases/2022/central-banks-of-indonesia-malaysia-philippines-singapore-and-thailand-seal-cooperation-in-regional-payment-connectivity
- 9 See www.ebacclearing.eu/news-and-events/media/press-releases/6-october-2022-immediate-cross-border-payments-ixb-pilot-set-to-revolutionise-international-payments/
- 10 See buna.co/announcement/buna-launches-its-instant-payment-service-ips
- 11 The number of links required to connect all members of a network bilaterally is calculated as $(n(n-1))/2$, where n is the number of members.
- 12 For an excellent primer on payment messaging standards see the World Bank's guide 'Messaging Standards in Fast Payments', available from Project FASTT at fastpayments.worldbank.org/resources
- 13 For an excellent primer on proxies, see the World Bank's guide 'Proxy Identifiers and Database in Payments', available from Project FASTT at fastpayments.worldbank.org/resources
- 14 Application Programming Interfaces (APIs) allow different systems to speak to each other and exchange data or instructions. For example, the banking app on the Sender's phone will use APIs to ask Nexus which proxy types are available in the Recipient's country.
- 15 ISO 20022 is a standard for payment messages. It provides a set of messages for various payment-related functions, such as sending a payment instruction, confirming the success or failure of a payment, or asking for resolution of a proxy (eg mobile phone number) to the underlying account details. When multiple systems use the same message standard, there is no need to translate a message every time it moves between systems.
- 16 See Committee on Payments and Market Infrastructures, Enhancing cross-border payments: building blocks of a global roadmap, July 2020, www.bis.org/cpmi/publ/d193.htm, and the FSB's next steps for enhancing cross-border payments, October 2022, www.fsb.org/2022/10/g20-roadmap-for-enhancing-cross-border-payments-priorities-for-the-next-phase-of-work/
- 17 See www.fsb.org/2021/10/targets-for-addressing-the-four-challenges-of-cross-border-payments-final-report/
- 18 See Target 10.c: 'By 2030, reduce to less than 3 per cent the transaction costs of migrant remittances and eliminate remittance corridors with costs higher than 5 per cent' at sdgs.un.org/goals/goal10#targets_and_indicators
- 19 Traditional cross-border payments often rely on central banks' high-value payment systems, which process transactions between financial institutions and usually operate only during business hours. This means payments can be delayed while waiting for a central bank payment system to 'open for business'. See the CPMI's consultative report on operating hours of RTGS systems at www.bis.org/cpmi/publ/d199.htm.
- 20 One exception is in the case of a non-time-critical payment that has been accepted by the Destination PSP but not yet credited to the Recipient. In this case, the Sender will be informed that the payment will be slightly delayed while the Destination PSP completes their checks. A Service Level Agreement in the Nexus Scheme Rulebook will set a cap on the maximum time that the payment can be delayed.
- 21 See www.bis.org/publ/othp39.htm

- 22 Each IPS operator created an exact replica of their domestic payment system and proxy resolution service in an insulated testing environment. This allowed them to adapt their systems to integrate with Nexus while avoiding any risk of disrupting the live domestic payment systems. No 'real money' payments or real customer accounts were used.
- 23 See www.bis.org/publ/othp62.htm
- 24 Nexus can also support payments from a government to individuals or businesses and vice versa. For example, a pensions authority could use Nexus to make pension payments to overseas citizens.
- 25 IPS caps range from the equivalent of US\$ 140 in Turkey right up to the equivalent of US\$ 1.2 million in the United Kingdom, although some IPS have no limit.
- 26 In [Figure 4](#), the FXP is shown outside any specific country, as for any specific payment they may not be based in the Source Country or in the Destination Country. However, the FXP will always have a specified home jurisdiction and must be compliant with the rules and regulations of that country. They may also be bound by the regulations of the country to which they are providing FX conversion.
- 27 The Settlement Access Provider acts as a correspondent to the FXP (its 'respondent'). Banks are generally becoming less willing to provide correspondent banking services to other banks. One benefit of the arrangement in Nexus is that only (some) FXPs need to rely on a correspondent relationship with an SAP. FXPs that are members of an IPS, and PSPs that are willing to use third-party FXPs for all their payments, do not need to maintain accounts or relationships with banks in other countries.
- 28 The JOF will have direct oversight over the NSO but not the NTO. However, it can set expectations on the NTO through the NSO, by issuing recommendations/guidelines and information requests. It may also coordinate with the NTO's home regulator, if applicable.
- 29 One key difference is that in a domestic payment, the Source IPS would be waiting for an acceptance from the Recipient's PSP in the same country. In contrast, for a Nexus payment, the Source IPS must forward the payment instruction to Nexus and wait for a response from the Destination PSP in the Destination Country.
- 30 In a real-time immediate settlement model, a \$10 payment between the Sender and the Recipient is settled by an immediate transfer of \$10 of (central bank) money between the Sender's PSP and the Recipient's PSP's respective accounts at the central bank.
- 31 In deferred net settlement models, a \$10 payment between the Sender and the Recipient is recorded as a \$10 obligation from the Sender's PSP to the Recipient's PSP. At the end of the settlement cycle (which might be daily, every few hours or even every few minutes), the net flows between each PSP are calculated and only the net amounts are transferred between the PSPs' accounts at the central bank.
- 32 ie The Source PSP reduces the balance of the Sender's account by EUR 100
- 33 Governance, as defined in the PFMI, is 'the set of relationships between an FMI's owners, board of directors (or equivalent), management and other relevant parties, including participants, authorities, and other stakeholders... Governance provides the processes through which an organisation sets its objectives, determines the means for achieving those objectives, and monitors performance against those objectives'. See bis.org/cpmi/publ/d101a.pdf
- 34 PFMI Principle 1 (Legal Basis): 'An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions'; and PFMI Principle 2 (Governance): 'An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders'.
- 35 There is a range of ownership models for IPS operators, ranging from fully public (eg Bank Indonesia in Indonesia) to hybrid public-private (eg PayNet in Malaysia) and fully private (eg PPMI in the Philippines, BCS in Singapore and NITMX in Thailand).
- 36 Such flexibility is important to ensure the scalability of Nexus. While some central banks may choose to be a joint owner of the NSO to ensure public policy alignment, there are some central banks that may not have the mandate or prefer not to do so.
- 37 For example, by ensuring clear segregation between their owner/operator and overseer roles within their organisational structure and decision-making process.

- 38 In contrast, a company limited by shares can choose to distribute profits to its owners (shareholders) as dividends.
- 39 As the number of member countries grows, it may be impractical to have each joint owner nominate their representative in the Board as it would make the size of the Board unwieldy. At this stage, an appropriate mechanism can be introduced to select Board members based on relevant considerations (eg profile, geographical representation, transaction volume).
- 40 An independent director refers to a non-executive director who does not have any material relationship with the company and its owners and affiliates that would interfere with the exercise of his/her independent judgement.
- 41 The 'members' in a company limited by guarantee play the same role as the shareholders in a company limited by shares.
- 42 The BIS Innovation Hub Project Icebreaker explored connecting three experimental retail CBDC systems together to enable cross-border payments in CBDC. Many of the challenges are similar to the challenges of linking IPS. See www.bis.org/about/bisih/topics/cbdc/icebreaker.htm
- 43 Oversight can be defined as 'a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned payment, clearing, settlement and related arrangements, assessing them against these objectives, and where necessary, inducing change'. (See CPMI Glossary).
- 44 This is necessary to ensure that the Source PSP can easily compare the offer from multiple FXPs. In addition, permitting FXPs to charge both a fee and the FX rate would add significant complexity to Nexus, particularly when calculating quotes.
- 45 The payback period is the time it takes for the profit on revenues earned by a Nexus participant to cover the initial cost of onboarding and integrating with Nexus.
- 46 See www.bis.org/cpmi/publ/d218.htm
- 47 Cross-border Payments and Reporting Plus (CBPR+) is a working group that manages ISO 20022 market practice and implementation guidelines for cross-border payments on the SWIFT network.
- 48 Instant Payments Plus (IP+) market practice and guidance for ISO 20022 messages.
- 49 See www.bis.org/publ/othp62.htm



Project Nexus

Enabling instant cross-border payments

ISBN 978-92-9259-758-0
bis.org