



Nexus

A blueprint for instant cross-border payments

with support from



Monetary Authority
of Singapore



This publication is available on the website nexus.bisih.org.

Publication date: July 2021

© Bank for International Settlements 2021. All rights reserved. Use of this publication is subject to the terms and conditions of use published on nexus.bisih.org. Brief excerpts may be reproduced or translated provided the source is stated.

ISBN 978-92-9259-499-2 (online)

Nexus: a blueprint for instant cross-border payments

In many countries today, domestic payments between bank accounts happen in seconds, at near-zero cost, thanks to the growing availability of instant payment systems (IPSs). In contrast, cross-border payments between accounts in two countries can be slow, complicated and expensive,¹ depending on the service used.

IPSs enable domestic account-to-account payments, with the recipient being credited in real time (or near-real time) on a 24/7 basis. They are operational in around 60 countries, and under development in more. This BIS Innovation Hub project explores how we can build on the success of instant payments to improve the cross-border payments experience. It provides a blueprint for a scalable cross-border payments network, *Nexus*, that would connect IPSs in multiple countries, enabling them to offer cross-border payments that reach their destination within 60 seconds.

This short report explains the benefits of linking IPSs to provide cross-border payments. It addresses the challenges that would need to be overcome and explains how a bridging platform like Nexus could streamline this process. It makes recommendations for IPSs that are upgrading or rebuilding their technology to allow for cross-border interoperability.

This blueprint was developed and refined through 25 workshops with IPS operators, central banks and large banks with a significant presence in FX markets and cross-border payments.² We welcome further feedback and suggestions to enhance the blueprint.³



The full blueprint is available from nexus.bisih.org. It provides much more detail on the functionality required by IPS operators and their member banks and Payment Service Providers (PSPs), including message flows and application programming interface (API) specifications for communication between IPSs.

- 1 See Committee on Payments and Market Infrastructure, *Cross-border Retail Payments*, February 2018 www.bis.org/cpmi/publ/d173.htm
- 2 We would like to thank the many public and private sector workshop participants for their time, insights and feedback. Of course, the final design and any errors are the responsibility of the authors, and no endorsement is implied. The blueprint was produced with significant support from Paul van der Valk, Mark Munne, Fred Baer and Harry Kodden of IN4PAY. The National Payments Corporation of India (NPCI) provided technical support to help assess different designs. The team at the Monetary Authority of Singapore provided insights into the lessons learnt from the PromptPay-PayNow link between Thailand and Singapore. Input from other central banks, payment system operators, commercial banks and AML experts was essential to refining and improving the blueprint.
- 3 The Nexus team can be contacted at singapore.centre@bisih.org

The potential for linking instant payment systems

Instant (“fast” or “real-time”) payment systems are now operational in around 60 countries, with others in development. Linking these IPSs together could enable cross-border payments from sender to recipient within 60 seconds in most cases.

A number of fintech providers have used their direct or indirect access to IPSs to provide near-instant cross-border payments. However, in these implementations it is the fintech firm that coordinates two independent payments in two countries; the two IPSs are not directly linked. Linking IPSs would go further by creating interoperability and connecting payment infrastructures – rather than banks – across borders. The Committee on Payments and Market Infrastructures (CPMI) has identified linking IPSs as one of the “building blocks” for enhancing cross-border payments.⁴

In April 2021, Singapore’s PayNow service and Thailand’s PromptPay were linked in a world first, allowing customers of participating banks in Singapore and Thailand to send money to each other using just the telephone number of the recipient.⁵ This demonstrates the significant potential benefits for consumers and businesses. Country-to-country linkages are now being explored by other countries.

Benefits of linking IPSs

Sending cross-border payments through domestic IPSs overcomes some of the challenges of traditional cross-border payments, with potentially significant impacts on speed, cost, transparency and access.



Speed

IPSs already process payments in seconds. Most IPSs can process a domestic payment within 30 seconds, so a cross-border payment – which would first be processed by the IPS in the sender’s country and then by the IPS in the receiver’s country – could plausibly take 60 seconds or less. In contrast, the speed of traditional cross-border payments depends on how quickly each bank in a payment chain picks up and processes the payment.

IPSs can process payments on a 24/7/365 basis in most cases. In contrast, traditional cross-border payments often rely on central banks’ real-time gross settlement (RTGS) systems, which usually operate only during business hours, so payments can be delayed while waiting for an RTGS to “open for business”.

4 See building block 13 in Committee on Payments and Market Infrastructure, *Enhancing cross-border payments: building blocks of a global roadmap*, July 2020 www.bis.org/cpmi/publ/d193.htm

5 <https://www.mas.gov.sg/news/media-releases/2021/singapore-and-thailand-launch-worlds-first-linkage-of-real-time-payment-systems>



Cost

IPSs tend to be very cost-efficient for domestic payments. Domestic payments are often free to customers, while banks may pay a very small fee per transaction. This sets a low-cost basis for cross-border payments through IPSs – although there are always more costs involved in a cross-border payment than in a domestic payment.

Linking IPSs makes it easier for banks to offer cross-border payments to countries where they have no presence or partnerships. In contrast, traditional cross-border payments often require the bank to hold accounts with a bank in each country that it wants to send payments to. These “correspondent” accounts are expensive and time-consuming to set up, and many correspondent banks are withdrawing their services.



Access

IPSs typically allow all banks in a country to make and receive payments. Some IPSs also provide access to non-bank PSPs. If IPSs were linked, most citizens could initiate a cross-border payment through their bank or PSP. The specific level of access in a country would depend on the level of financial inclusion and percentage of people who have bank accounts in that country.



Transparency and certainty

In many traditional cross-border payments services, variable fees are levied by each bank in the payment chain. This means the sender does not know how much the recipient will receive until the payment reaches them. Linking IPSs would eliminate long correspondent banking chains and allow fees to be calculated upfront and shown to the sender before they commit to make a payment.

By design, a payment through an IPS either completes or fails within seconds, so the sender has certainty about the status of their payment. In contrast, traditional cross-border payments may fail at multiple stages in the payment chain, sometimes hours after the sender has initiated the payment.



Safety and security

IPSs have strong risk management regimes to mitigate credit and settlement risks within the domestic payment system. A cross-border network of linked IPS payments can build on these risk management frameworks. Some cross-border exposures will need to be addressed outside the domestic IPS scheme.

The obstacles to linking IPSs

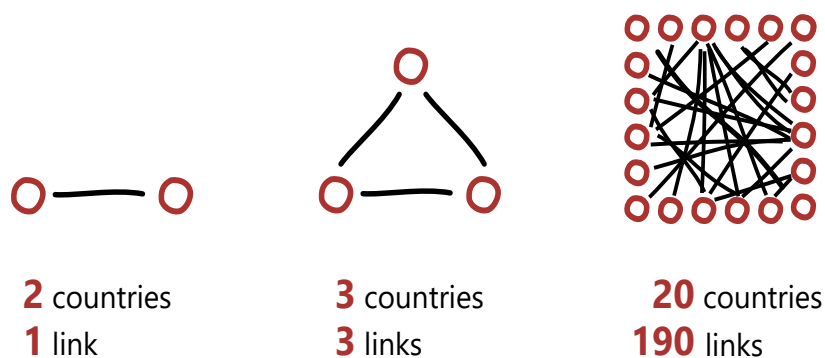
Linking IPSs is not straightforward. Cross-border payments are inherently more complex than domestic payments; they require additional steps, such as currency conversion and compliance checks to prevent the financing of terrorism and other illicit activities. A further challenge comes from the fact that IPSs have different processes and functionality, and often speak different “languages” in the way they share data and payment instructions. Each IPS may use different:

- data formats, standards and mandatory fields;
- processes and the sequence of steps in a payment process;
- scheme rules around liability, disputes, data protection and privacy etc; and
- functionality, including whether aliases are used and whether there is a confirmation of payee service.

This complexity increases exponentially as more participants join the network. Three countries require just three country-to-country links, but a network of 20 countries would require 190 country-to-country links. Each IPS operator would need to maintain custom-built links with 19 other IPSs, each with their own standards and processes. This is difficult from a software development and IT operations perspective. The compromises that IPSs would need to make for each bilateral link could result in sender and recipient user experiences that vary wildly depending on the destination country. Most problematically, the complexity involved could potentially put the resilience of the domestic payment system – which may be systemically important – at risk.

Consequently, linking IPSs bilaterally makes sense when two countries have a close relationship and a significant flow of payments. However, a more scalable approach is needed to create a truly global network of IPSs offering cross-border payments.

Figure 1: Country-to-country links grow faster than the number of countries



How Nexus helps

Nexus overcomes the complexity of linking IPSs on a country-to-country basis by providing a standardised way for domestic payment systems to speak to each other. This enables “interoperability” between payment systems.

Nexus includes two main elements:



The **Nexus Scheme** defines the rules and obligations for IPSs, banks and Payment Services Providers who make cross-border payments through Nexus (“Nexus payments”). This is intended to supplement domestic IPS schemes – which do not normally address cross-border payments – with the minimum number of changes required to enable cross-border payments.



The **Nexus Gateway** is a software component which coordinates processes such as compliance, FX conversion, message translation and the sequencing of payments between two countries.

Each IPS and its members would need to adapt their systems to be compatible with Nexus. These adaptations are expected to be minimal, although they may vary depending on the structure of each IPS. Countries would make this adaptation just once, and then be able to connect to any other country in the Nexus network with no additional work to undertake when new members join. For each IPS, this would involve significantly less work – and less cost – than connecting to multiple IPSs one-by-one. A network of 20 countries linked by Nexus would require just one integration to Nexus per IPS, and 170 fewer integrations than using custom country-to-country links.

This provides a more scalable approach to building a cross-border payment network between IPSs, by reducing the cost of implementation, and therefore reducing the cost of the cross-border payments service itself.

Nexus essentially defines a set of capabilities that IPSs should provide – or work towards providing – to ensure the best cross-border user experience for senders and recipients of payments. Not all IPSs will have these capabilities at the start, so Nexus is designed to operate with a minimum set of functionalities to ensure that payments can still go through. This minimum set of functionalities must always be sufficient to ensure full compliance with relevant regulations.

Nexus is designed around user needs

Nexus has been designed with the user experience of senders in mind, and aims to meet the following requirements:



Speed

Nexus aims to provide cross-border payments within 60 seconds in most cases.



Cost

Fees should be lowered by increasing efficiency and reducing manual intervention.



Transparency

Fees and FX rates should always be shown to the sender before they commit to the payment.



Access

Anyone who can send a domestic instant payment through the local IPS should be able to send cross-border payments through Nexus.



Confidence and security

Senders should be given certainty that they are sending funds to the correct account through some form of confirmation of payee, wherever possible.



Usability

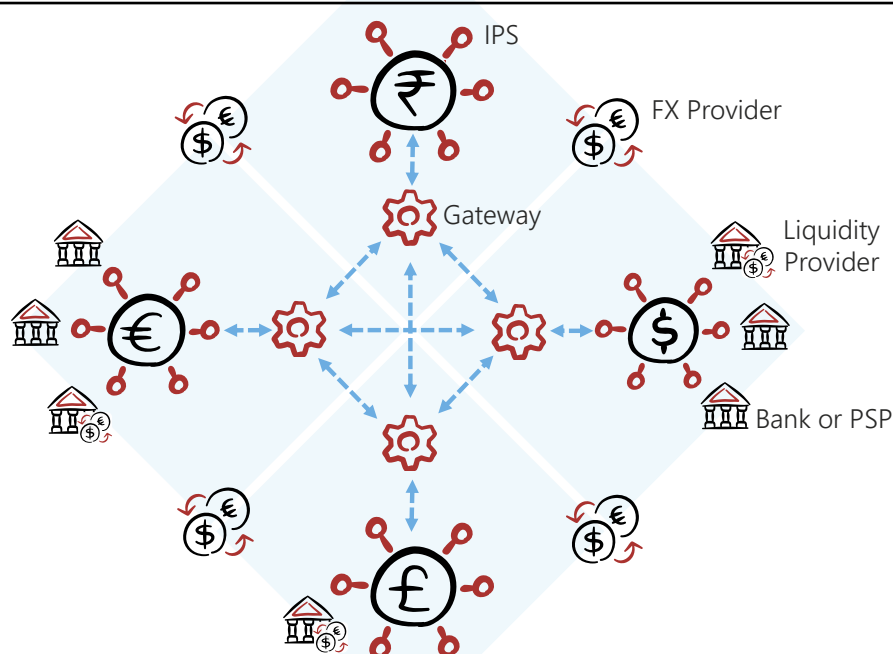
Senders can use their existing banking app. Aliases that are valid for domestic payments (eg phone numbers) will also work internationally through Nexus. Users do not need to, and cannot, sign up with Nexus directly.

The Nexus Gateway

The proposal is for each IPS to operate a Nexus Gateway. Each Gateway will communicate with Nexus Gateways in other countries to support the key functions required to successfully make a cross-border payment. These key functions are:

- **currency conversion** – Nexus coordinates with FX Providers to ensure that the sender’s currency is swapped for the recipient’s currency. These FX Providers compete to offer the best rates;
- **messaging** – Nexus translates between the different message formats used in different IPSs, while ensuring that critical data⁶ is not lost in translation and transmission;
- **pre-validation** – Nexus is designed to proactively eliminate the most common sources of delay and cost in traditional cross-border payments, *before* any money is moved. It does this by checking all of the factors that normally cause a payment to fail, and supporting the banks involved to resolve those issues automatically whenever possible. This means that the sender has a much higher degree of certainty that when they click “send payment”, the payment will go through with no unexpected delays or failures;
- **coordination** – Nexus coordinates a payment across two different IPSs and handles any failures; and
- **compliance** – Nexus enables all banks in a payment ecosystem to request additional information about the sender or recipient if required for sanctions screenings or other compliance checks. It aims to avoid manual interventions whenever possible.

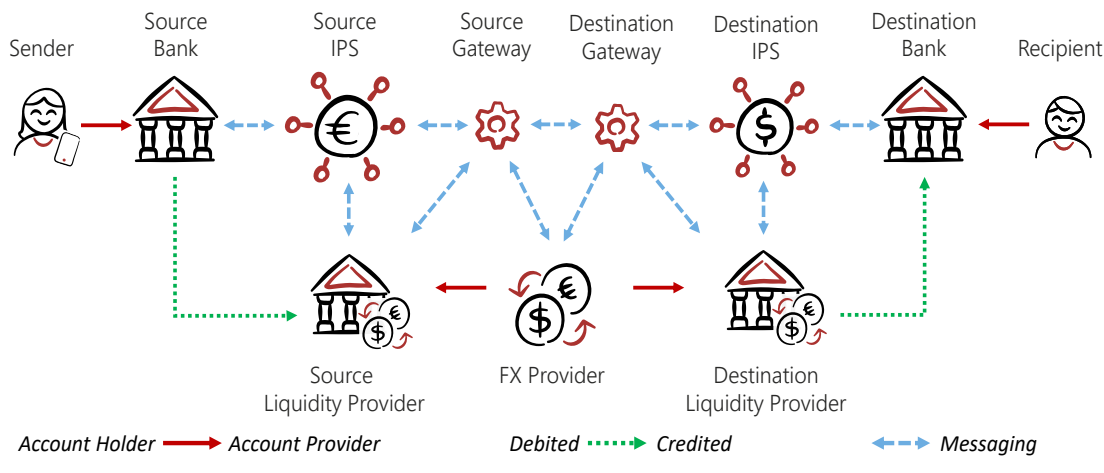
Figure 2: Nexus Gateways connect IPSs to IPSs in other countries



6 Such as personal data required for the purpose of sanctions screening.

Participants in the Nexus network

Figure 3: Relationship between participants in the Nexus network



The Nexus network is made up of the following participants and actors:



Sender & Recipient

The Sender and Recipient can be individuals or small or medium-sized businesses who currently use IPSs to send domestic payments – so-called “retail” payments. Since most IPSs place caps on the size of single payments, Nexus is not designed to be used to make payments between very large corporates or financial institutions, so-called “wholesale” payments.



Instant payment system operators (IPSOs)

IPSOs provide infrastructure that enables senders and recipients to make instant domestic payments, ie between two accounts in the same country.



Source Bank & Destination Bank

The Sender and Recipient both hold accounts with IPS members. These will be banks and – in some countries – non-bank Payment Service Providers (PSPs). In a Nexus payment, the Source Bank is the Sender’s bank, and the Destination Bank is the Recipient’s bank. In most cases, all banks in a country will be directly or indirectly connected to the IPS and able to send and receive payments through it.



The Nexus Gateway

To connect the IPSs together, each IPS must install and operate a Nexus Gateway. The Nexus Gateway is software which coordinates processes such as compliance, FX conversion, message translation and the sequencing of payments between two countries. Each Gateway connects to the domestic IPS infrastructure on one side and to Nexus Gateways in other countries on the other side.



FX Providers

Each Nexus payment requires an FX Provider which would be a regulated financial institution that is willing to accept the Source Currency and pay out the Destination Currency.

FX Providers inform Nexus of quotes for the rate at which they are willing to swap one currency for another. They compete to offer the best rates to ensure a dynamic market.

If the FX Provider is a bank or PSP which is already a member of the Source and Destination IPS, it can directly receive the Source Currency from the Source Bank and pay out the Destination Currency to the Destination Bank.



Liquidity Providers

In cases where the FX Provider is not a member of both or either IPS, the FX Provider can use accounts that it holds with Liquidity Providers in the Source or Destination Country. Liquidity Providers are simply existing IPS members (including banks and PSPs) who are willing to provide "vostro/nostro" accounts to FX Providers who are not members of that IPS.

When a Nexus payment is processed:

- the Source Bank makes a payment to the Source Liquidity Provider via the domestic payments system in the Source Country. The Source Liquidity Provider then credits the vostro account of the FX Provider; and
- the Destination Liquidity Provider debits the vostro account of the FX Provider, and pays out funds to the Destination Bank via the domestic payments system in the Destination Country.

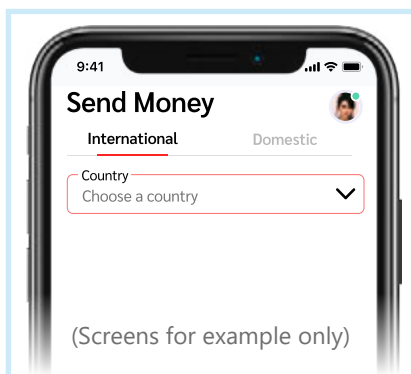
The Nexus Gateway acts as an instructing party for Liquidity Providers, meaning that it can accept and initiate payments on their behalf.

Some participants can play multiple roles. For example, if an FX Provider is a member of both the Source IPS and Destination IPS, it can act as its own Liquidity Provider. Likewise, the Source Bank may act as FX Provider for its own payments through a Liquidity Provider in the Destination IPS.

A payment through Nexus

The walkthrough below shows how a sender would make a payment through Nexus, using their existing banking channel (eg an app), and the steps taken by Nexus behind the scenes. Before the payment starts:

- **Nexus collects the service level description (SLD) for each IPS.** The SLD describes the functionality available in the Destination IPS, such as the account number format, alias format(s), the maximum value that can be sent and whether confirmation of payee is available. Each IPS defines their own SLD and shares this with Nexus.
- **Nexus compiles the quotes from FX Providers.** Nexus stores quotes provided by multiple FX Providers, who compete to offer the best rates at any time.

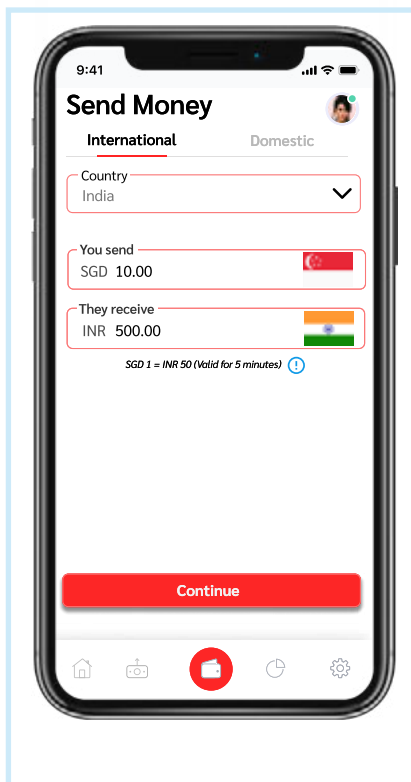


The sender first logs into their existing banking app. There is no separate Nexus ID or app.

They select the Destination Country.

Nexus retrieves the Service Level Description (SLD). After the Sender has selected the Destination Country, the Source Bank will ask Nexus for the SLD of the Destination IPS. This is so that it can ask the customer for the correct information eg an alias or account number, and possibly the Recipient's name depending on the type of confirmation of payee offered.

Nexus retrieves a quote. The Source Bank will also ask Nexus for quotes for payments to the Destination Country. It can ask for the best quote available, or specify one FX Provider including, in some cases, itself.



The Sender is shown the current FX rate.

They enter the amount they wish to send (in the Source Currency), or the amount they want the Recipient to receive (in the Destination Currency).

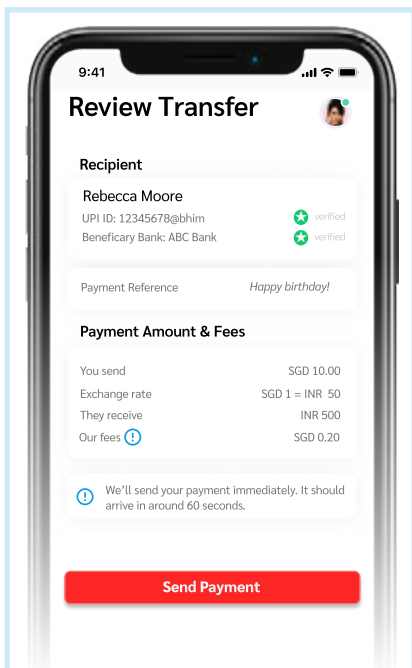
The Recipient will receive exactly the amount shown, although the Destination Bank may separately charge fees for processing the payment.

The image displays three sequential screenshots of a mobile application's 'Payee Details' screen. The first screenshot shows a dropdown menu labeled 'Send Payment to'. The second screenshot shows a list of input fields: 'Phone Number', 'UPI ID', and 'IFSC Code & Account Number'. The third screenshot shows the 'Send Payment to' dropdown set to 'UPI ID', a 'Recipient's UPI ID' field with the value '12345678@bhim' and a warning icon, and a 'Payment Reference' field with the placeholder 'Reference or message'. A red 'Check Payee Details' button is at the bottom, and a navigation bar is at the very bottom.

The Sender then enters account details or an alias (such as a phone number). Any alias that is valid in the Destination Country will also be valid through Nexus.

Nexus takes the alias or account details and communicates with the Destination IPS or Destination Bank to perform the following checks:

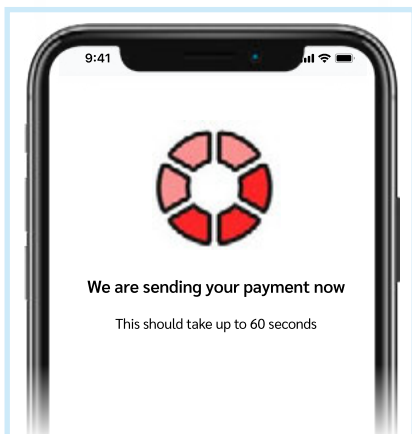
- account validation** – the Source Bank will ask Nexus to validate the account against the specifications outlined in the SLD of the Destination IPS. This involves: (a) mapping any alias used to an account number; (b) checking that the recipient's bank is enabled to receive Nexus payments; and (c) checking that the recipient's account is technically able to accept payments, ie that it is not closed or frozen.
- confirmation of payee** – this process allows the Sender to verify that the holder of the Destination Account is actually the person or business they intend to pay. Some confirmation of payee models require the sender to provide the expected name and then compare this to the real name which has been verified by the Destination Bank. The Destination Bank reports back the degree to which the two names match. Other models simply retrieve the real name from the Destination Bank and return it, possibly partially masked for data protection. The real name or match status is then shown to the Sender.
- sanctions pre-screening** – the banks involved in a Nexus payment perform screening on the Sender and Recipient according to regulatory requirements. If either Sender or Recipient trigger an alert, the banks can communicate through a Nexus-provided API to request further information about the Sender or Recipient. This further information can be sent back to the requesting bank immediately or simply included in the final payment instruction.



When all the checks above have been completed, there is a much higher degree of confidence that the payment will successfully complete.

Now the Sender is shown the name of the Recipient, based on the confirmation of payee process, where available. They are also shown any fees charged by the bank.

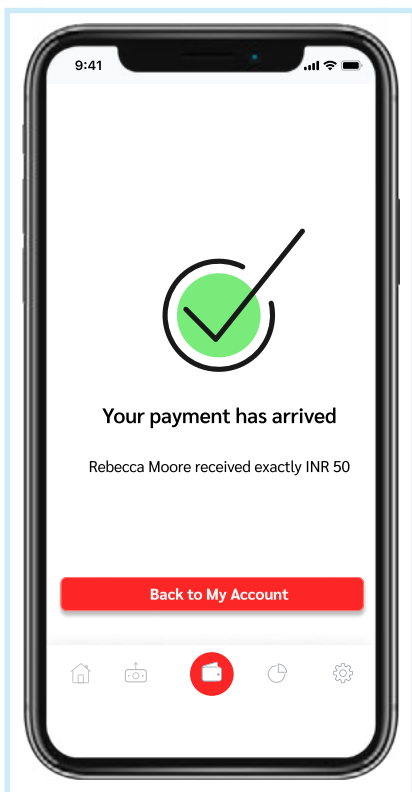
The sender clicks "send payment".



Final payment instruction – the payment instruction can now be sent from the Source Bank to the Source IPS.

Once the payment is complete in the Source IPS, 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.

The payment should be processed within 60 seconds in most cases.



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



Visit nexus.bisih.org to see step-by-step message flows and further details on each step in the process.

The Nexus Scheme



A payment scheme is a set of procedures, rules and technical standards that govern how payments are executed. Local IPS schemes cover only domestic payments, so the **Nexus Scheme** is necessary to cover the cross-border aspects of Nexus payments.

The Nexus Scheme would apply directly to: (1) IPSs who wish to offer Nexus payments; and (2) FX Providers. Other IPS members, including the Source and Destination Banks and Liquidity Providers, would instead sign up to an addendum to the local IPS scheme containing some additional rules that apply only to payments sent via Nexus.

Establishing a payment scheme is a significant undertaking requiring legal work and negotiation between different stakeholders. To limit the potential complexity, the Nexus Scheme is intended to have limited scope and only define the necessary requirements to ensure safe and reliable cross-border payments. It would aim to avoid or minimise any changes to local IPS schemes. Importantly the scheme would not change the clearing and settlement processes of the local IPSs. It will also not set access criteria for Source and Destination Banks – any participant who is a member of a specific Nexus-enabled IPS will be eligible to send payments through Nexus.

The Scheme would need to specify the responsibilities of all participants and actors in the Nexus network and would require all actors to comply with relevant local laws and regulations, including countering the financing of terrorism (CFT) measures through sanctions screening. The Scheme would also specify what happens in cases where the rules around payment disputes or recalls are different in the two local schemes.

The Scheme would not specify the fees that Nexus participants could charge, but it would emphasise the need for transparency in the way fees are displayed to the Sender and Recipient. It would also discourage offering “free” payments by hiding the fee in the FX spread.

The **Nexus Scheme Manager** is the governance entity that manages the scheme and maintains relationships with IPS Operators and FX Providers. The Scheme Manager also develops the software for the Nexus Gateway or contracts with a third party to do this. However, the day-to-day operations of Nexus Gateways would be managed by the respective IPSs.



Visit nexus.bisih.org to see further detail on the aspects the Nexus scheme would need to cover.

Risk management in Nexus



Nexus is designed to build on the strong and robust risk management capabilities already present within domestic IPS schemes.

Most IPS schemes mitigate credit risk and settlement risk within the domestic payment system by using: (1) pre-funding and collateral arrangements; or (2) immediate settlement in central bank money. Nexus can build on this risk management to limit credit and settlement risk.

Foreign exchange risk in Nexus is necessarily limited because the time period between a quote being provided and the payment being completed is only a few minutes. However, there are some cross-border exposures between FX Providers and their Liquidity Providers. These risks must be managed bilaterally between these parties.

The Destination Liquidity Provider, who must pay out funds to the Destination Bank, also faces some liquidity risk. This is because it does not control the rates offered by the FX Provider and therefore cannot control the demands on the liquidity it holds at the Destination IPS. However, this risk can be managed via an agreement and communication between the FX Provider and Destination Liquidity Provider.



Visit nexus.bisih.org for a detailed summary of the credit, FX, settlement and liquidity risks faced by each participant.

Design choices to future-proof domestic payment systems for cross-border payments

IPSs are not usually built with cross-border payments in mind. This means that some design choices which are appropriate for domestic payments make it harder to provide cross-border payments. The Nexus Gateway can help overcome, or work around, some of these legacy design choices. However, where IPSs are being upgraded, rebuilt or designed from scratch, the following design choices can future-proof them for cross-border payments.

1. Use the ISO 20022 standard for payment messages

Different payment systems and bank systems use different data formats, meaning the data in a payment message can be corrupted or truncated as it is converted from one format to another. Some local message formats do not allow enough space to carry the additional information required for cross-border payments. Poor quality data can cause problems with processing and increase the number of false alerts resulting from sanctions screening, adding costs and delay.

The ISO 20022 standard for data messages provides a better structure and more space for payments-related data.⁷ It is being adopted across a range of payment systems, including the SWIFT cross-border network, and is already used by some domestic IPSs.

Nexus will use the ISO 20022 standard for data messages when sending cross-border payment messages. It will also provide message translation for IPSs that do not use ISO 20022, as well as storing “overflow” data that will not fit into domestic payment messages. However, where the domestic IPS can migrate to ISO 20022 for its domestic payment messages, there are advantages for end users, IPS members and for cross-border interoperability.

2. Move to pre-validation of payment instructions

In many payments processes, problems with data in the payment message are only identified after the payment has been sent, meaning the payment must be cancelled, returned to the sender bank and then reinitiated, hours or even days after it was initially sent.⁸

It is preferable to identify reasons why the payment would fail before the sender clicks “send payment”. This gives the sender more certainty about whether the payment will be successful or not. Nexus would use functionality provided by the IPS and its members to: (a) validate that the destination bank is online and functioning;

⁷ www.iso20022.org/about-iso-20022

⁸ The cross-border payments messaging network, SWIFT, have recently introduced a pre-validation process for SWIFT payments. www.swift.com/our-solutions/swift-gpi/pre-validation-gpi-payments

and (b) validate that the recipient's account is able to receive payments and is not dormant or frozen. IPSs and their members can make sure this information is available when designing or upgrading their systems.

3. Provide confirmation of payee functionality

Confirmation of payee improves the user experience by giving the sender reassurance that they are sending money to the correct account, either by showing them the real name on the recipient's account, or confirming that the real name is similar to or exactly matches the name that the sender provided. This is particularly important in cross-border payments, where users may be entering account numbers or aliases in unfamiliar formats, or long international bank account numbers (IBAN) that can be difficult to check character-by-character.

Importantly, confirmation of payee helps to reduce:

- **payments sent to the wrong account** – for example, where the sender has mistyped the account details, but the mistyped details are still a valid account, meaning that the payment goes through, but goes to the wrong recipient. The account validation process above will catch any errors where the account does not exist at all, but not errors where the account exists but belongs to the wrong person.
- **fraud** – authorised push payment fraud occurs when the sender unwittingly sends a payment to account details provided by a fraudster. Authorised push payment fraud has been a significant problem in domestic payments, at great cost to victims and banks. It is even more important to provide safeguards to prevent cross-border payments being used for authorised push payment fraud, where the different legal regimes will increase the complexity of recovering funds lost to fraud.

Data protection and privacy rules may pose an obstacle to using confirmation of payee in cross-border payments. This should be considered when setting up a confirmation of payee scheme and may also need to be addressed in banks' terms and conditions.

4. Support sanctions pre-screening

Traditional cross-border payments apply sanctions screening after the payment instruction has been sent. If an alert is triggered, a payment may be sent for manual review by a member of staff, and further information may be requested from the other bank, adding to administrative costs. On average, a false match against the sanctions list will result in a 24-hour delay to the payment.⁹

Sanctions screening is even more challenging in the context of instant cross-border payments, where there is no time for manual review of payments that trigger sanctions screening alerts. To address this, Nexus includes a number of design features to support the sanctions screening undertaken by the banks as part of the payment

9 risk.lexisnexis.co.uk/insights-resources/white-paper/kyc-sanctions-remediation-the-impact-of-inefficiency

process.¹⁰ These features are intended to reduce the percentage of payments that trigger unnecessary alerts and increase the percentage of alerts that can be resolved automatically, without manual intervention. The design features include:

- **pre-screening** – Nexus asks banks to undertake sanctions screening before the final payment instruction is sent wherever possible. This is intended to pre-emptively identify if additional information is required to assess whether an alert is a true or false match, rather than simply rejecting the payment after the instruction is sent.
- **ensuring better quality data** – Nexus will reject payments that do not have the minimum set of data required by FATF Recommendation 16.¹¹
- **retrieving the recipient name from the destination bank**, wherever possible. When senders are asked to provide the recipient’s name, they can introduce inaccuracies (eg through typos or using a short name rather than the full legal name). The destination bank has already verified and saved the full legal name of the recipient, as per their identity documents. Using this accurate and verified name is less likely to trigger false alerts against sanctions lists.
- **enabling banks to request further information from each other** – if the pre-screening triggers an alert, banks can ask each other to provide the further information that they would need to eliminate false matches. This additional information can be sent between banks automatically using Nexus’s API-based request for information process, or simply attached to the final payment message. The aim is for this process to take place automatically with no human intervention in most cases. Again, data protection and privacy regulations need to be considered here.

The functionality involved in these features may present challenges for banks running legacy systems but could be supported by more modern API-based sanction screening software.



See nexus.bisih.org for further detail on each of these design choices

¹⁰ Nexus does not perform sanctions screening itself; this remains the responsibility of the banks involved in a payment, specifically the Source Bank, Source Liquidity Provider, Destination Liquidity Provider and Destination Bank.

¹¹ www.cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers

Next steps for Nexus

This blueprint is intended as a starting point, to be further refined and improved through technical research and engagement with IPS operators, banks and payment service providers. Building a real-world Nexus network, gateway and scheme would require a coordinated effort with these players alongside central banks and regulators. Further work would be needed on the governance model, oversight and scheme specification, and addressing legal differences between jurisdictions. There are a number of possible ways forward:

- one concrete next step would be for at least three IPS operators to collaborate in a **technical proof of concept**, linking their IPSs together to process cross-border payments following the Nexus approach. This would help to test and refine the blueprint against the real-world requirements of different IPSs, ensuring that the design is workable for multiple IPSs and is therefore a scalable basis for a cross-border payment network;
- an alternative approach is for a number of IPS operators to develop the flows, APIs and capabilities described in the Technical Docs (available at nexus.bisih.org) into an **open standard (or protocol) for IPS interoperability**. This could support industry-led efforts to link IPSs even in the absence of a Nexus Scheme and infrastructure; or
- most ambitiously, seed funding could be provided to set up an **implementation entity** to build the Nexus software and scheme as a public good to improve cross-border payments. Alternatively, the same funding could support a well-positioned IPS operator to lead the build and implementation. If this approach is taken, it would be essential to engage with IPS operators, banks and PSPs, and end users to ensure that the service delivers something that would be widely adopted. It would be advisable to start this step only after the technical proof of concept mentioned above.

The BIS Innovation Hub welcomes feedback and suggestions to enhance the blueprint. The team can be contacted at singapore.centre@bisih.org



The full blueprint is available from nexus.bisih.org. It provides much more detail on the functionality required by IPS operators and their member banks and PSPs, including message flows and API specifications for communication between IPSs.

