paymentsnz

in partnership with

DIGITAL IDENTITY.NZ

PAYMENTS DIRECTION

Digital Identity workshop insights and recommendations 2024

Contents

This document is produced by Payments NZ Limited (Payments NZ) and must not be copied, reproduced, or distributed, in whole or in part, without the consent of Payments NZ.

Payments NZ has relied on publicly available information and information provided to it by third parties in the production of this document. While Payments NZ has made every effort to ensure that the information contained in the document is accurate, it takes no responsibility for any errors or omissions in relation to the information contained in this document and Payments NZ will not be liable for any loss sustained in reliance on the information in this document. If you wish to rely on such information, you should obtain your own independent advice.

Digital Identity workshop insights and proposed recommendations

Executive summary

In the rapidly evolving landscape of digital identity, it is imperative to understand the challenges, opportunities, and best practices. The Digital Identity Workshop held on 9th May 2024 brought together industry experts, thought leaders, and stakeholders to explore the intricacies of digital identity, particularly within the realm of payments. This workshop is the start of a Payments Direction exploratory sprint into Digitial Identity for payments. This paper synthesises the insights, proposed recommendations, and future directions discussed during the workshop.

As we navigate this digital frontier, it's essential to ensure that identity systems are inclusive, interoperable, secure, and privacy-enhancing. The workshop aimed to address these issues, provide actionable strategies for industry stakeholders and to identify further areas of exploration for Payments Direction.

Payments NZ's Next Generation (Next Gen) payments programme is also exploring the potential for a Next Gen payments platform to connect to and leverage digital identity capabilities. This could help ensure safe payments processing and enable the use of verifiable credentials in payments use cases. While the workshop had a much broader focus across the digital identity ecosystem, its insights will support Next Gen's further conversations.

Structure

The Workshop was structured to explore the landscape of digital identity in finance, covering six key topics, with discussions also covering KYC/KYB. Each topic was addressed through a combination of presentations, discussions, and brain-storming sessions, allowing participants to engage deeply with the subject matter.

The Workshop utilised a collaborative approach, with attendees split into groups to work on each of the seven key topics. Employing a simplified design thinking process alongside brainstorming and discussion, participants engaged in parallel sessions to delve deeply into the intricacies of each topic.

Each group was tasked with exploring specific challenges and opportunities within their assigned topic. They began by identifying key issues and potential solutions, followed by brainstorming innovative ideas. Through structured discussion and sharing of insights, participants worked collaboratively to develop actionable recommendations. This parallel format allowed for a comprehensive exploration of all seven topics simultaneously, fostering cross-pollination of ideas and perspectives among attendees.

Statements for consideration at the workshop

1. **Reusable identity credentials**

   The concept of reusable identity credentials offers convenience, increased privacy and security to users. Onboarding users once and creating a secure and trusted digital identity credential allows individuals to authenticate themselves seamlessly across different platforms and services without the need for repetitive verification processes.

2. **Privacy and control**

   Customers have the ability to determine how, where, and when their information is used within their digital identity. Verifiable credentials create the opportunity to bolster privacy and give individuals greater control over their data usage.

3. **Digital Identity credentials (data) that will improve payment experience**

   Digital identity credentials can enhance the payment experience by reducing friction and enhancing security. Different types of credentials can be utilised to improve specific payment use cases, such as facilitating the purchase of restricted goods or providing accurate address information for delivery.

4. **Collaborative fraud prevention**

   Financial institutions who collaborate with other stakeholders, including retailers, e-commerce businesses, payment service providers, and within the payments networks can more effectively combat fraud. Sharing data and insights can strengthen fraud prevention capabilities and mitigate risks across the entire financial ecosystem.

5. **Continuous innovation in identity verification**

   Fraud tactics are continually evolving, so financial institutions must innovate continuously in identity verification methods. This includes exploring emerging technologies such as decentralised identity solutions to enhance security and trust in digital transactions.

6. **Strong Customer Authentication (SCA) requirements**

   Implementing robust digital identity solutions with advanced authentication methods, including biometrics, behavioural analytics, and multi-factor authentication, not only enhances the security of financial transactions but also increases the likelihood of preventing illegal activities, reducing fraudulent transactions, minimising financial and societal harm, and improving overall customer experience.

7. **KYC, KYB and KYE integration**

   Organisations already integrate Know Your Customer (KYC) processes into digital identity verification, to gain a comprehensive understanding of their customers, improving due diligence and reducing the risk of fraudulent activities. Also integrating Know Your Business (KYB) and Know Your Employee (KYE) processes into digital identity verification can provide a comprehensive understanding of both the business entities and individuals involved in financial transactions. This enhances due diligence and reduces the risk of fraudulent activities.

Te Ao Māori and Inclusion Considerations

This theme emphasised the importance of ensuring we are a Te Tiriti o Waitangi honouring partner by embedding Te Ao Māori and inclusion across all proposed solutions and frameworks from the outset. The goal was to promote self-determination and agency, drawing from principles such as Māori Data Governance and Universal Design [1]. Attendees were encouraged to consider how their ideas and solutions could be made more inclusive, ensuring they addressed the needs of all individuals, including those who are marginalised or have specific requirements. By integrating these considerations into their discussions, attendees aimed to avoid further entrenching disadvantage and exclusion, fostering a more equitable and accessible digital identity ecosystem.

[1] Te Kāhui Raranga https://www.kahuiraraunga.io

Summary of workshop key insights

Te Ao Māori considerations and perspectives

- Importance of incorporating Te Ao Māori perspectives into trust frameworks.
- Creating safe digital spaces for all users, considering privacy and inclusivity.
- Recognising the significance of māori identities, such as iwi/hapū identity, in the trust ecosystem.

Future Perspectives

- Focus on proactive measures to remove fraud from the system.
- Aligning identity solutions with human behaviour rather than just technology.
- Embracing open standards for collaborative, equitable solutions.

Reflections and Insights

- Incremental approaches are essential for implementation.
- Industry-led initiatives are crucial for success.
- Simplification and clear explanation of concepts are needed.
- Exploring business verification opportunities and addressing cyber protection concerns.

Challenges, Solutions, and Opportunities

- Education and adoption challenges require integrated solutions.
- Integrating identity solutions into trusted applications.
- Challenging jargon and emphasising the role of scheme operators.
- Exploring non-personal identity verification and the identity of things.
- Addressing consumer fraud and promoting data minimisation.

Overview of key contributors at the workshop

Kaye Maree Dunn: Making Everything Achievable

Kaye Maree Dunn brought a wealth of experience and expertise in digital identity solutions to the workshop. Her contributions focused on cutting-edge approaches to making digital identity accessible and usable for everyone, regardless of background or circumstance. Kaye Maree's insights underscored the importance of inclusivity and accessibility in digital identity systems. She emphasised designing and implementing solutions that benefit all users, particularly those from marginalised communities. Through her session, attendees gained a deeper understanding of how to create digital identity frameworks that provide the potential for application of iwi data, as well as the importance of hapū and iwi in deciding how Māori data is shared, demonstrating how to promote equity and provide practical benefits across diverse user groups.

Clair Barber, Tobias Looker, and Preet Patel: MATTR

Representing MATTR, Clair Barber, Tobias Looker, and Preet Patel discussed the critical concept of bi-directional trust, highlighting not just the identity of individuals but also the identity of organisations. They shared a demonstration showcasing the future of privacy, emphasising respect for identity and other credentials to enable high-assurance interactions across various contexts and channels. Key architectural components demonstrated included:

- Apps acting as secure channels, such as government or banking apps.
- Different cross-channel journeys, including online, in-person, and with physical documents.
- The role of bi-directional trust and the utilisation of ecosystem capabilities and trusted registries.

This demonstration illustrated how these components underpin high-assurance outcomes and help combat fraud, phishing, and scamming. Their session provided a comprehensive look into how MATTR envisions privacy and security in digital identity evolving, offering attendees a glimpse into practical applications and future possibilities.

Rick Iverson and Dima Postnikov: ConnectID

Rick Iverson and Dima Postnikov represented ConnectID, an Australian-based service provider run by Australian Payments Plus (AP+). They shared the journey of launching ConnectID, a digital identity solution designed to help Australians protect themselves from fraud and identity theft. ConnectID operates as a secure bridge between organisations seeking identity verification and those providing it, without storing or accessing personal information. This unique approach ensures enhanced security and privacy by only facilitating identity verification when authorised by the customer.

Two of the Big Four banks in Australia, Commonwealth Bank and National Australia Bank, have adopted ConnectID. Customers of these banks will be among the first to use this new Digital Identity verification technology, with the other banks coming online soon.

ConnectID simplifies the process of identity verification, enabling customers to request verification from organisations they already trust. This reduces the need for customers to repeatedly share personal data across multiple platforms. Traditional methods of identity verification often require sharing extensive personal information, which poses significant security risks. ConnectID aims to mitigate these risks by limiting the data shared to only what is necessary for verification.

The introduction of ConnectID is timely, coinciding with the Australian government's efforts to implement the Digital Identity Bill. The legislation in Australia aims to create an economy-wide Digital Identity system, featuring a voluntary accreditation scheme for Digital Identity service providers and an expanded Australian Government Digital Identity System that includes private sector organisations.

Digital Identitys are crucial as Australians and New Zealanders increasingly transact online, leading to a rise in cyber incidents. In 2022, Australia had the fourth-highest cyber victim density globally. The cost of cybercrime is projected to reach $10.5 trillion by 2025, highlighting the urgent need for robust digital identity solutions.

During their session, Iverson and Postnikov demonstrated how ConnectID combines real-time verification with strict adherence to user consent, setting a new standard for security and privacy in identity verification. Attendees learned valuable insights into a cutting-edge solution that could be applied in other regions and contexts.

The contributions of Kaye Maree Dunn, MATTR, and ConnectID at the Digital Identity Workshop were instrumental in shaping the discussions and outcomes. Their expertise and innovative approaches provided attendees with a deeper understanding of the complexities and opportunities within the digital identity landscape. By highlighting inclusivity, bi-directional trust, and enhanced security, these sessions offered practical insights and actionable strategies for developing robust digital identity solutions in Aotearoa New Zealand that can cater to diverse user needs.

A brief history of digital identity initiatives in Aotearoa New Zealand

DIA Programme establishment and research

In 2018, the New Zealand government launched a two-year initiative led by the Department of Internal Affairs (DIA) to explore innovative approaches to digital identity. This programme aimed to establish the necessary rules and environment to leverage emerging technologies while addressing the evolving needs and expectations of citizens. Throughout 2019 and 2020, the Digital Identity Programme team conducted extensive research and engaged with key stakeholders and counterpart agencies in other jurisdictions. The insights gained from this comprehensive research and engagement process were crucial in formulating the Trust Framework principles.

Digital Identity services trust framework

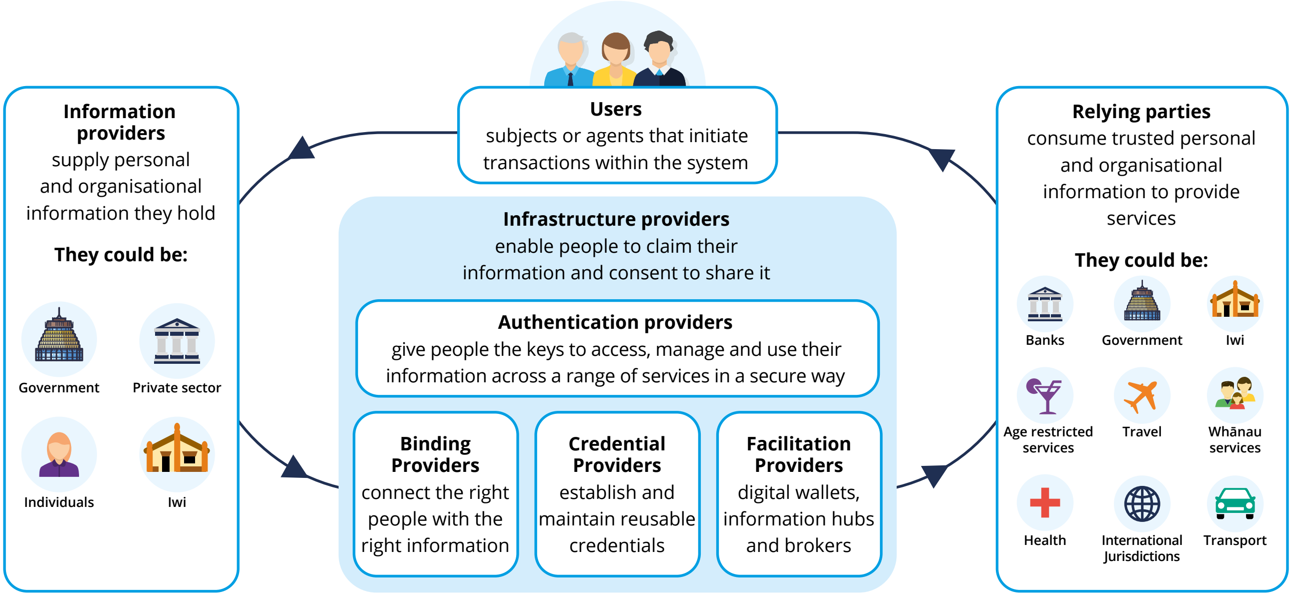
The Digital Identity Services Trust Framework is an opt-in regulatory framework that outlines rules for the delivery of accredited digital identity services. In July 2020, the New Zealand Cabinet agreed to establish the Digital Identity Trust Framework in legislation to address the issues identified during the research phase. The resulting legislation, the Digital Identity Services Trust Framework Act, will come into force on July 1, 2024. It is anticipated that the accreditation process will be available later in the year.

The Digital Identity Regulator Establishment Programme is currently working to establish the Trust Framework Authority under the Act, ensuring a robust regulatory environment for digital identity services in New Zealand.

Digital Identity New Zealand

Digital Identity New Zealand (DINZ) is committed to fostering a secure, inclusive, and user-centric digital identity ecosystem that empowers both individuals and businesses. The establishment of the Digital Identity Services Trust Framework represents a significant milestone in achieving this objective. By providing a strong regulatory foundation, the framework strives to continuously reflect the highest standards of security, privacy, and trust in the delivery of digital identity services.

DINZ's collaboration with the Department of Internal Affairs (DIA) and other key stakeholders has been instrumental in shaping the principles that support the Trust Framework. This collaborative effort underscores the organisation's dedication to integrating diverse perspectives and expertise to create a digital identity system that meets the evolving needs of society.



Information providers
supply personal and organisational information they hold

They could be:

Users
subjects or agents that initiate transactions within the system

Infrastructure providers
enable people to claim their information and consent to share it

Authentication providers
give people the keys to access, manage and use their information across a range of services in a secure way

Binding Providers
connect the right people with the right information

Credential Providers
establish and maintain reusable credentials

Facilitation Providers
digital wallets, information hubs and brokers

Relying parties
consume trusted personal and organisational information to provide services

They could be:

Digital Identity Trust Framework
Provides the rules and standards for compliance and interoperability between providers, services and international jurisdictions

General discussion overview

Workshop participants discussed the necessity of crafting a culturally sensitive and inclusive digital identity ecosystem that honors indigenous values and perspectives. They also discussed adoption challenges, how to address the challenges, possible delivery principles, and future opportunities. The general discussion on these topics are explored in this section.

Cultural considerations

The workshop highlighted the importance of integrating Māori Data Governance principles with the broader principles underpinning trust frameworks. Key points included:

- **Alignment with Māori principles:** There is a strong alignment and reinforcement between Māori Data Governance principles and trust frameworks, emphasising the life cycle of data as taonga (treasure).
- **Inclusivity of Māori identities:** To be inclusive of Māori, it is essential to establish processes for recognising whakapapa (lineage) and incorporating Te Ao Māori identities.
- **System design:** The design of the digital identity "system" must consider geographic locations and access to technology, ensuring flexibility to accommodate diverse needs. This flexibility equates to providing choices rather than forcing users into predetermined pathways.
- **Terminology and trust anchors:** The terms "credentials" and "Digital Identity" might not fully capture the inclusivity and flexibility needed. For example, a "digital" ID may be issued in-person. Additionally, recognising multiple trust anchors, including Māori as a route of trust, is crucial for inclusivity.

Challenges

The workshop identified several challenges in the adoption and implementation of digital identity solutions:

1. **Education:** A major hurdle for adoption is educating customers about how their data is used, how digital identities are created, and the implications of data collection methods such as facial scanning.
2. **Adoption:** There is a need to build trust and achieve critical mass adoption among both consumers and relying parties. Understanding how Digital Identity services can and should be used is essential for broad acceptance.
3. **Market creation:** Creating a market for reusable credentials is challenging due to the need for widespread education and adoption. The concept of reusable credentials implies a robust network effect, which requires significant initial user and relying party engagement.

Solutions to the challenges

The workshop proposed several solutions to address these challenges:

1. **Integration with trusted apps:** Integrating identity solutions into existing, trusted applications can drive adoption. For example, users might verify their ID through their bank during a loan application, rather than downloading a separate identity wallet app.
2. **Consumer confidence through familiarity:** Consumers are more likely to trust and adopt Digital Identity solutions when their initial experiences occur with known and already trusted issuers, such as their usual bank.
3. **Clarifying jargon:** Simplifying and clarifying terminology, such as what "credentials" mean, can help users better understand and trust digital identity solutions. For example, an airpoints card, if used as a verifiable identity piece, could be more inclusive and promote better understanding.
4. **Role of scheme operators:** Scheme operators, such as ConnectID in Australia, are crucial for establishing trust, rules, and guardrails within the digital identity ecosystem.

Delivery principles

The group emphasised the importance of momentum and collective commitment in driving the implementation of digital identity solutions. Key principles included:

1. **Market demand:** The group indicated there is market demand for a digital identity solution in the payments space, however this will need to be further validated through the next stages of discussion.

2. **Collective commitment:** Implementing collective commitment within the industry is challenging but necessary for success.
3. **Scheme operators:** A scheme operator is needed to ensure trust and coordinate efforts within the industry.
4. **Multiple schemes:** Accepting that there may be multiple schemes and that not everyone trusts the same entities is important for inclusivity.
5. **Coordination and momentum:** Coordinating industry efforts is slower but yields better outcomes. Maintaining momentum is crucial to avoid analysis paralysis.

Opportunities

The workshop identified several opportunities for the future of digital identity:

1. **Non-personal, or business entity identity verification:** Starting with non-personal entities for identity verification can help build trust and address fraud more effectively.
2. **Identity of things:** In the longer term, considering the identity of devices and things, Most devices and things have identifiers such as serial numbers, IP addresses and so on, that help bind an instance to a transaction, person or event, such as road tolls such as road tolls charged based on license plate recognition, could expand the scope of digital identity.
3. **Mandates attached to identities:** Attaching mandates, such as power of attorney, or parents acting on behalf of children to identities could streamline experiences and enhance trust.
4. **Consumer fraud prevention:** Targeting consumer fraud through digital verification services can immediately improve security and trust.
5. **Clarifying purpose and scope:** Ensuring that digital identity solutions are not creating a single national ID or providing social credit systems. The DISTF Act envisions services that reduce the amount of sensitive personal information shared, and places control of sharing in the hands of the consumer.

Key topics for consideration

During the workshop, participants examined and discussed seven key statements, exploring their implications and outcomes. Each statement generated insightful conversations, and the results of these discussions are detailed in this section.

1. Reusable identity credentials

Statement: The concept of reusable identity credentials offers convenience, increased privacy and security to users. Onboarding users once and creating a secure and trusted digital identity credential allows individuals to authenticate themselves seamlessly across different platforms and services without the need for repetitive verification processes.

Discussion points: Improve convenience, privacy, and security for users through seamless authentication across platforms.

Proposed recommendations:

- Develop standardised frameworks for reusable identity credentials to ensure interoperability.
- Encourage widespread adoption by offering incentives to businesses that integrate with reusable credential systems.
- Educate users about the benefits and safety measures associated with reusable credentials.
- Consider a wallet proposition integrated into existing experiences.
- Promote data minimisation, ensuring verification without unnecessary data transfer.
- Consider onboarding at different levels of assurance, starting with less stringent identity proofs.

2. Digital Identity credentials for enhanced payment experience

Statement: Digital identity credentials can enhance the payment experience by reducing friction and enhancing security. Different types of credentials can be utilised to improve specific payment use cases, such as facilitating the purchase of restricted goods or providing accurate address information for delivery.

Discussion points: Reduce friction and enhance security in payment transactions.

Proposed recommendations:

- Develop specialised digital identity credentials tailored to specific payment use cases.
- Implement technologies such as tokenisation and biometric authentication to enhance security.
- Collaborate with payment processors and retailers to streamline the integration of digital identity credentials into payment processes.

3. Privacy and control

Statement: Customers have the ability to determine how, where, and when their information is used within their digital identity. Verifiable credentials create the opportunity to bolster privacy and give individuals greater control over their data usage.

Discussion points: Increase privacy and control over personal data for customers.

Proposed recommendations:

- Implement verifiable credentials with granular control over data sharing.
- Provide user-friendly interfaces for managing data permissions and consent.
- Educate users about their rights and options regarding data privacy and control.

4. Strong Customer Authentication (SCA) requirements

Statement: Implementing robust digital identity solutions with advanced authentication methods, including biometrics, behavioural analytics, and multi-factor authentication, not only enhances the security of financial transactions but also increases the likelihood of preventing illegal activities, reducing fraudulent transactions, minimising financial and societal harm, and improving overall customer experience.

Discussion points: Enhance security and improve customer experience in financial transactions.

Proposed recommendations:

- Implement advanced authentication methods such as biometrics and multi-factor authentication.
- Educate customers about the importance of SCA and how it protects their transactions.
- Continuously monitor and adapt to emerging threats to maintain effectiveness.

5. Collaborative fraud prevention

Statement: Financial institutions who collaborate with other stakeholders, including retailers, e-commerce businesses, payment service providers, and within the payments networks can more effectively combat fraud. Sharing data and insights can strengthen fraud prevention capabilities and mitigate risks across the entire financial ecosystem.

Discussion points: Strengthen fraud prevention capabilities across financial ecosystems.

Proposed recommendations:

- Utilise digital identity-based authentication methods to reduce the risk of methods such as passwords or SMS.
- Establish information-sharing partnerships among financial institutions, retailers, and payment service providers.
- Implement real-time fraud detection systems that leverage shared data and insights.
- Develop standardised protocols for sharing sensitive information (such as web or app metadata) while ensuring compliance with privacy regulations.

6. Continuous innovation in identity verification

Statement: Fraud tactics are continually evolving, so financial institutions must innovate continuously in identity verification methods. This includes exploring emerging technologies such as decentralised identity solutions to enhance security and trust in digital transactions.

Discussion points: Enhance security and trust in digital transactions through innovative identity verification methods.

Proposed recommendations:

- Invest in research and development of emerging technologies such as decentralised identity solutions.
- Foster a culture of innovation within financial institutions by incentivising experimentation and collaboration.
- Regularly assess and update identity verification systems to stay ahead of evolving fraud tactics.

7. KYC, KYB, and KYE integration

Statement: Organisations already integrate Know Your Customer (KYC) processes into digital identity verification, to gain a comprehensive understanding of their customers, improving due diligence and reducing the risk of fraudulent activities. Also integrating Know Your Business (KYB) and Know Your Employee (KYE) processes into digital identity verification can provide a comprehensive understanding of both the business entities and individuals involved in financial transactions. This enhances due diligence, reduces the risk of fraudulent activities and reduces costly and time-consuming manual processes.

Discussion points: Aim for a comprehensive understanding of customers, businesses, and employees involved in financial transactions, reducing the risk of fraudulent activities.

Proposed recommendations:

- Integrate KYC, KYB, and KYE processes into digital identity verification platforms.
- Develop APIs and standardised protocols for seamless data exchange between different verification systems.
- Ensure compliance with regulatory requirements while streamlining due diligence processes for customers and businesses.

Potential opportunities for action

The workshop participants proposed various potential opportunities for action, emphasising the importance of incorporating Te Ao Māori perspectives, launching a pilot project, and developing a comprehensive education and adoption plan. They highlighted the need for a simplified and standardised approach, future research and collaboration, as well as exploring a KYB (Know Your Business) project. The following section details these suggestions.

1. **Inclusivity and Te Ao Māori perspectives**
   - Collaborate with experts to incorporate cultural considerations.
   - Ensure that digital identity solutions are accessible and inclusive for all users.
2. **Create a Digital Identity pilot project with relevant NZ banks already working with ConnectID in Australia**
   - Partner with ConnectID to understand the work they have done to date with CBA and NAB
   - Proposed launching a pilot project in NZ with relevant banks based on roll out in Australia.
3. **Education and adoption**
   - Develop educational resources for consumers and businesses.
   - Encourage the adoption of digital identity solutions through integration with trusted applications.
4. **Standardisation and simplification**
   - Establish clear standards and terminology.
   - Create a comprehensive glossary accessible to the public.
5. **Future research and collaboration**
   - Further research on non-personal 'Know Your Business' identity verification.
   - Collaboration with stakeholders to develop comprehensive solutions.
6. **Explore the possibility of starting with KYB project**
   - Conduct an assessment to identify the specific requirements for integrating KYB processes within existing digital identification platforms and business registries such as: NZBN (MBIE); the Companies Register; the Bill Payee and Direct Debit registers (Payments NZ); and Legal Entity Identifier (a global standard for identifying parties to financial transactions).
   - Collaborate with industry stakeholders, including financial institutions, regulatory bodies, and technology providers, to explore the scope and objectives of a possible pilot.
   - By further developing these proposed recommendations, financial institutions have the opportunity to strengthen security, enhance customer experience, and mitigate risks in digital transactions. Collaboration, innovation, and a commitment to privacy and security will be essential in shaping the future of digital identity in finance.

Overarching considerations

These recommendations would also aim to incorporate for the following considerations.

1. Security and Privacy: Prioritise robust security measures and privacy controls throughout the development and implementation phases to build trust among users and stakeholders.
2. Interoperability: Ensure that the digital identity scheme is interoperable with other government and private sector systems to facilitate seamless transactions.
3. User-Centric Design: Focus on user-friendly design and accessibility to encourage widespread adoption and minimise barriers to entry.
4. Continuous Innovation: Stay abreast of emerging technologies and continuously innovate to enhance the digital identity ecosystem.
5. Collaboration: Foster ongoing collaboration between the public and private sectors to address challenges and leverage collective expertise.

Conclusion

The Digital Identity Workshop provided valuable insights into the challenges and opportunities surrounding digital identity in the payments sector. Many activities are currently underway to guide the creation of a secure, inclusive, and efficient digital identity framework for payments in Aotearoa New Zealand. The industry has a significant opportunity to build on this foundational work, developing a robust, user-centric digital identity environment that addresses current issues, unlocks new business value, and provides better, safer experiences for New Zealanders.

Attendees put forward six key recommendations for next steps and focus areas. We are actively seeking industry feedback to validate that these actions warrant further exploration and effort.

Payments NZ, through Payments Direction, will incorporate this feedback and outline proposed next steps and timeframes.

For further details and inquiries, please contact Payments NZ.

Acknowledgments

We extend our gratitude to all the speakers, presenters, and participants whose contributions made this workshop a success. Special thanks to Colin Wallis, Digital Identity New Zealand, James Little, Department of Internal Affairs, Kaye-Maree Dunn, Making Everything Achievable, Rick Iverson and Dima Postnikov, ConnectID, Clair Barber, Tobias Looker, and Preet Patel, MATTR, for their contributions and invaluable insights.

paymentsnz

DIGITAL
IDENTITY.NZ

+64 4 890 6750
payments.direction@paymentsnz.co.nz
www.paymentsnz.co.nz