Visa Government Solutions
Research Insights
December 2024

Digital identity and payments:

Synergies for enhancing public services and economic opportunity

VISA

Case studies, comparisons, statistics, research, recommendations and information in this Whitepaper (the "Information") are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. Visa is not responsible for your use of the marketing materials, best practice recommendations, or other information, including errors of any kind, contained in this document. Materials and recommendations should be independently evaluated in light of your specific business needs and any applicable laws and regulations. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific organizational needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Visa is under no duty to update or revise this Whitepaper in any way.

All intellectual property rights, including but not limited to copyrights, and the ownership and title to this Whitepaper and the information contained therein are owned by and vest exclusively in Visa. Third parties shall not have nor acquire any rights in such intellectual property and shall not copy, distribute or make any other use of the Whitepaper and the Information contained therein.

All brand names and logos are the property of their respective owners, are used for identification purposes only, and DO NOT imply product endorsement or affiliation with Visa.

Contents

Executive summary

Billions of people globally do not have a digital identity that allows for simple and secure identification and authentication online.[1] In an increasingly digitised global economy, this is an important gap to close because ready access to digital services can be a critical enabler of financial inclusion and economic development — even developed economies could see a gross domestic product (GDP) uplift from deploying digital identity systems.[2]

By providing individuals with a verifiable means of proving who they are, digital identity systems can unlock access to essential services and economic opportunities for those in urban or remote communities. Governments can harness digital identity to deliver services more efficiently (while reducing frictions like fraud), and companies can leverage digital identity to comply with identity-related regulations more efficiently, improving their service to customers. The COVID-19 pandemic amplified the need for digital identity, particularly given the high volumes of benefits being disbursed to people and small businesses.

Some countries and regions are working on implementing systems that go beyond basic identification to offer enhanced functionality, security and user control. Trust is crucial for the adoption of all digital identity systems because it directly impacts users' willingness to participate and share their personal information. Without trust, individuals may be reluctant to use the systems, fearing the potential misuse of their data and breaches of privacy. Trust can encourage citizens to engage with digital services, leading to higher adoption rates and more effective implementation of e-governance initiatives. Partnership with the private sector is a key to success for digital identity systems, since the private sector can provide the useful and frequent use cases needed to help build trust in and adoption of the systems. Trust is built with high-quality user experiences, strong consent frameworks, and an expectation that digital identities and the associated data are protected at the highest security level. Governments will therefore need to consider their approach to using biometrics as a mechanism to validate identity attributes, the pros and cons of centralised vs. decentralised biometric storage design, and what data is required when and by whom.

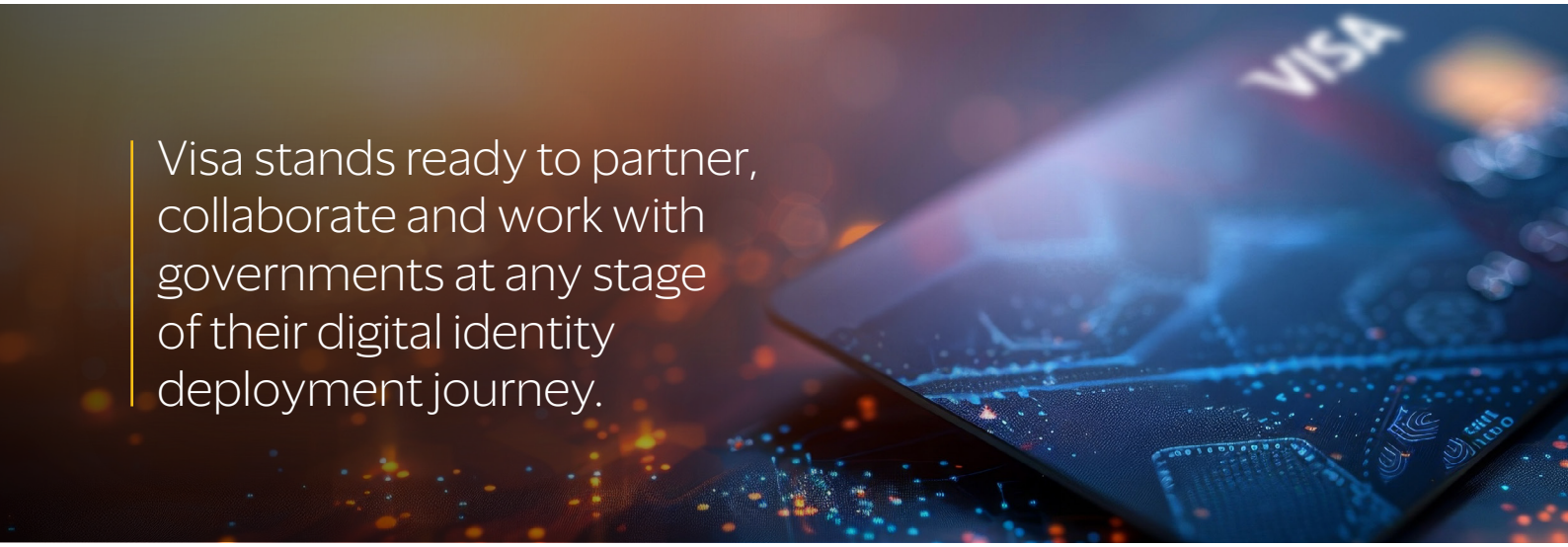
Digital payments have expanded into many aspects of our lives over the past decade, assisted by notable improvements in convenience, availability and security. End-users who can easily authenticate their identity for financial transactions, especially when these transactions are either received from or made to governments, could be more likely to appreciate and adopt digital identity systems. When a government establishes a trust framework with appropriate legal obligations and protections that enable both the private and public sectors to rely on digital identity, these identity systems can enable more secure and inclusive Know Your Customer (KYC) processes, increasing accessibility to public or private sector services, potentially reducing identity theft and financial fraud risks. Increased security and certainty around an individual's identity can support expansion of commerce, simplification for stakeholders and greater inclusiveness. With a verified digital identity linked to a payment credential, users can authorise transactions quickly and securely. As payments support the uptake of digital identity, and digital identity further improves payments user experiences, security and efficiency, a virtuous cycle can be created.

1. Source: World Bank. 850 million people globally don't have ID—why this matters and what we can do about it. 6 February, 2023.
2. Source: McKinsey Global Institute. Digital identification: A key to inclusive growth. 17 April, 2019.

The virtuous connection between payments and digital identity further emphasises the need for the public and private sectors to work in partnership. Governments should define the rules and regulations for digital identity and ensure legal equivalence and consistency to reinforce predictability and certainty for the private sector — and to protect individual rights in connection with digital identity. Governments also have a role to play in establishing standards by regulating for outcomes, citizen protection, consent, liability, certainty, etc. — and by allowing the private sector to implement the correct security attributes within existing frameworks for the specific commerce applications.

One of these collaborations involves the FIDO Alliance and passkeys — a type of cryptographic credential that eliminates the need for users to remember complex passwords when they log in to systems and applications. Visa is now integrating the use of secure biometrics-based authentication in payments through Visa Payment Passkeys™ — a technology based on the FIDO collaboration which works across all of an end-user's payment credentials. At its core, the recently announced Visa Payment Passkeys™ Service binds an account credential with a device, enabling an end-user to use the same biometrics they use to unlock their device for payment authentication. Once this authentication is performed, the payee can use a secure payment credential, which is a tokenised card number identified uniquely to their device, creating an authenticated payee for transactions across the payment rails on which they are transacting. It is possible to envision a parallel for digital identity — the same mobile device may also hold digital identity credentials that have been attested by identity providers and verification relying parties. Visa's ongoing work on Payment Passkeys may help facilitate a mutually reinforcing relationship between payments and digital identity that could benefit all stakeholders and end-users.

The public and private sectors can continue to work together to create trustworthy digital identity capabilities that offer end-users enhanced experiences across a wide variety of everyday use cases and public services — all while improving efficiency and stewardship of resources. Visa stands ready to partner, collaborate and work with governments at any stage of their digital identity deployment journey. Visa brings global and local payments expertise, fraud and risk mitigation experience, secure data management knowledge, and a strong focus on reducing friction for all stakeholders. In an increasingly connected world, now is the time to design and deploy digital identity systems nationally that are recognised globally.



Digital identity is a foundational infrastructure for economic development

Digital identity brings key benefits to governments, people and businesses

As of February 2023, the World Bank believes that 850 million people globally[3] still do not have an official identification. Even more people do not have a digital identity[4] — an online representation of their identity that allows for identification, authentication and authorisation. The World Bank, through its Identification for Development (ID4D) initiative, has long supported the development of inclusive and trusted digital identification systems, and the World Bank views digital identity as a key enabler for accessing financial services, healthcare, education and other critical services.[5] Other development entities such as the United Nations Development Programme[6] and the Bill & Melinda Gates Foundation[7] have also cited the importance of digital identity as an enabler of access and an important tool to fight poverty. Digital identity systems empower individuals by giving them greater control over their personal data and enabling participation in the formal economy.

"Digital identity ... holds significant potential to advance inclusive access to financial and government services, commerce, economic activity, health services and much more."[8] These systems enable governments to deliver services more efficiently, reduce fraud, and enhance speed and accuracy of disbursements in social protection programmes. The World Bank has also highlighted key private sector benefits: "Digital ID systems can help companies reduce operating costs associated with regulatory compliance (e.g., electronic know your customer — eKYC), widen customer bases, generate new markets, and foster a business-friendly environment more broadly."[9] One way to evaluate the benefits of digital identity is to consider the costs of the current situation. In 2023, the U.S. Financial Crimes Enforcement Network (FinCEN) observed that "$212B in transactions flagged in 2021 Suspicious Activity Reports (SARs) were tied to some form of breakdown in the identity verification process."[10] Box 1 contains a more expansive account of possible digital identity benefits for all stakeholders.

3. Source: World Bank. 850 million people globally don't have ID—why this matters and what we can do about it. 6 February, 2023. | 4. Source: Ibid.
5. Source: World Bank. Identification for Development. Page accessed 3 September, 2024. | 6. Source: UNDP. How digital can close the 'identity gap'. 2022.
7. Source: Bill & Melinda Gates Foundation. Digital IDs are an effective tool against poverty. 2023. | 8. Source: Visa Economic Empowerment Institute. Policy enablers for advancing digital identity frameworks: Insights and recommendations for public and private sectors. September 2021. | 9. Source: World Bank. Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable. 14 August, 2019. | 10. Source: Wilson Center. (Digital) Identity Crisis: The US Needs a National Strategy for Digital Identity to Enhance Economic Competitiveness and Mitigate Cybersecurity Risks. 24 October, 2023.

Box 1 — Digital identity as foundation for digital life

Digital identity plays a crucial role in a country's digital infrastructure, serving as a foundational element for various digital services and interactions. Here is a non-comprehensive overview of the benefits of digital identity:

- **Data-driven policymaking**
  Provides insights for better government planning and service delivery.
- **Digital economy**
  Facilitates secure online transactions and supports e-commerce growth.
- **Financial inclusion**
  Facilitates easier access to banking and financial services, especially for underserved populations.
- **Digital catalyst**
  Can enable digitalisation efforts across sectors.
- **Access to government services**
  Enables correct identification of people eligible for benefits and facilitates secure and efficient access to e-government services (when digital identity is executed across public sector functions).
- **Healthcare**
  Enables secure access to personal health records and streamlines healthcare delivery.
- **Education**
  Supports online learning platforms and verification of academic credentials.
- **Voting systems**
  Can enable secure electronic voting, potentially increasing participation.
- **Public safety**
  Aids in identity verification for law enforcement and emergency services.
- **Social services**
  Streamlines delivery of social benefits and reduces fraud.
- **Travel**
  Allows end-users to store and share key documents (like boarding passes) and identify themselves when making hotel reservations.

Implementing robust digital identity frameworks has the potential to uplift entire economies. The McKinsey Global Institute studied the economic benefits of digital identity before the COVID-19 pandemic and estimated that widespread adoption could unlock economic value equivalent to 3–13 percent of GDP in some countries by 2030, depending on the country's starting point and implementation approach. While the benefits were greatest for developing economies — an average of 6 percent of GDP, there were still significant economic benefits for mature economies — an average of 3 percent of GDP.[11] The pandemic further highlighted the need for digital identity and the possible gains from implementing digital identity systems, particularly given the high volumes of benefits being disbursed to people and businesses. Two years after the initial estimate, McKinsey found that "the potential economic gain from building robust digital financial infrastructure is about 20 percent greater now than it was before the pandemic."[12]

In the following sections, this paper will examine how governments have approached the implementation of digital identity and the importance of trust for adoption. This paper will then turn to how a key use case — payments — can drive adoption of digital identity systems and how the private sector can help governments realise the potential of this foundational infrastructure for uplifting everyone.

Box 1 sources: Visa analysis and synthesis, including information from: European Commission (2024); ITU (2021); McKinsey Global Institute (2021); Wilson Center (2023); World Economic Forum (2021a and 2021b) | 11. Source: McKinsey Global Institute. Digital identification: A key to inclusive growth. 17 April, 2019. | 12. Source: McKinsey Global Institute. COVID-19: Making the case for robust digital financial infrastructure. 26 January, 2021.

There is no single path countries take on their digital identity journeys, but mobile capabilities have emerged as key enablers everywhere

Digital identity is a representation of an individual that provides for the legal equivalence of in-person identity validation, authentication, authorisation, and signature time-stamping. A digital identity uses trusted data from an authoritative source to initially verify an individual's identity and then authenticate that individual each time their identity is used. A good digital identity system is formed from components that work together to ensure security, usability and privacy. See Figure 1 for some commonly recognised attributes of digital identity systems. Fuller descriptions for the attributes are provided in Appendix 1.

Figure 1 — Common attributes of digital identity systems

Core identity management

- Unique identifier
- Identity proofing
- Lifecycle management
- Revocation and recovery
- Identity wallets

End-user empowerment

- Consent management
- User control
- Accessibility
- Self-sovereign identity (SSI)
- Selective disclosure
- Contextual identity

Governance and compliance

- Governance framework
- Trust framework
- Auditability
- Audit trails

Security and authentication

- Authentication mechanisms
- Security measures
- Privacy protection
- Biometric integration
- Multifactor authentication
- Continuous authentication
- Adaptive risk assessment

System design and performance

- Interoperability
- Scalability
- Flexibility
- Cross-border interoperability
- Federated identity
- Decentralised architecture
- Privacy-enhancing technologies
- Revocable credentials
- Recovery mechanisms

Source: Visa analysis

Digital identity systems can be implemented in a variety of ways, each with their own advantages and drawbacks. There are, for example, centralised systems, decentralised ones and federated systems. Governments should consider factors such as digital literacy, infrastructure readiness, security schemes, interoperability, global standards, and how to create public trust when designing their digital identity strategies and systems.[13] Some nations might focus on specific sectors and then see a broader use of identity grow from that. India's Aadhaar system, to name an important example, started as a unique identification number for welfare distribution, but it has since expanded to many other areas (such as tax filing and healthcare) and therefore become a pillar of India's digital infrastructure.[14] In many cases, the national (or regional) vision for the digital economy can be also very influential in the digital identity journey. These visions and plans can take a decade or more to realise, but digital identity is a critical foundation to build on. Public-private partnership is a key to success for digital identity systems, since the private sector can provide useful and frequent use cases needed to help build trust in and adoption of these systems.

Governments should consider factors such as digital literacy, infrastructure readiness, security schemes, interoperability, global standards, and how to create public trust when designing their digital identity strategies and systems.

Countries that have started on their digital transformation journeys more recently have found that mobile capabilities have shifted the environment considerably. Two seismic shifts in end-user capabilities are underway and are critical market dynamics for the future of digital identity:

1 The future of digital interactions is mobile, and it is already here.

Mobile devices can store a variety of credentials for digital use. Several parts of the world skipped over desktop computers and landline telephones to become mobile-first, and this is being increasingly normalised in many more places today. Over the next few years, we are likely to see most commerce being driven via mobile devices. Accelerated by the pandemic across all countries, e-commerce has been growing faster than in-person commerce for years, and over 80 percent of e-commerce is now mobile commerce, with that share expected to continue growing.[15] With the emergence of digital wallets on mobile devices, Visa also anticipates that the trend of consumers preferring to make face-to-face payments via their phones will continue to expand and indeed accelerate.

2 Secure digital interactions can be enabled with commonly used technologies.

In places like the European Union, where smartphones make up over 80 percent of the market,[16] this means most consumers can perform on-device authentication using secure inherence factors such as a fingerprint or a facial scan. A known, trusted and user-authorised device (once authenticated) can become a part of the security regime relied upon by public and private sector entities when seeking to verify identities and authenticate the devices people use to interact with them. This forms part of a multilayer risk management system. See Box 2 for further discussion on biometric identification risks and challenges.

13. See, for example: McKinsey Global Institute. COVID-19: Making the case for robust digital financial infrastructure. 26 January, 2021.
14. Source: Unique Identification Authority of India. About your Aadhaar. Page accessed 15 October, 2024.
15. Source: Juniper. Global eCommerce Payments Market: 2024–2029. August 2024. Report accessed 23 October, 2024.
16. Source: GSMA. The Mobile Economy Europe 2023. 22 November, 2023.

Ukraine's Diia digital identity system launched in 2020 and is a powerful example of a deployment taking advantage of this new environment. The Diia mobile app transforms smartphones into digital wallets for official documents like passports, driver's licenses and vehicle registration — all of which are included in the 14 total official document types as of 2023. The app uses smartphone cameras for document scanning and facial recognition for identity verification. Diia also enables mobile-friendly access to over 70 government services such as tax filing, document signing and property registration. All digital documents in Diia now have the same legal force in Ukraine as their plastic or paper counterparts.[17]

Belgium's itsme® app provides a good example of public and private sector partnership in digital identity. Launched in 2017, itsme® allows users to prove their identity, sign documents and securely log in to various services using their smartphone. itsme® combines high-level security with user-friendly design, supporting both public sector uses and private sector applications as diverse as banking, insurance claims and online gaming.[18] The app is widely adopted in Belgium for banking, government services and authenticating online transactions.

AI will have a considerable impact on many countries' digital identity and digital transformation journeys.

Bhutan's National Digital Identity (NDI) implementation is also a good example of a system that connects the government, individuals and the private sector in their digital interactions. One of the objectives was to provide a unified and integrated user interface to access both public and private services from the outset to help resolve fragmentation.[19]

Artificial intelligence has been around for decades but has seen considerable advances in certain applications in recent years. AI will have a considerable impact on many countries' digital identity and digital transformation journeys. AI has already affected many domains of digital identity (especially biometrics) and will continue to do so. Many countries have explicit AI strategies that also relate to their digital transformation objectives.

Trust is critical for digital identity adoption

While there are some leaders in digital identity, global progress has been rather slow due to complex challenges such as privacy, security, digital literacy, legal frameworks and interoperability, which often require significant time, resources and coordination to address. Additionally, the sensitive nature of personal data means that governments must proceed cautiously to avoid mistakes that could erode public trust.

One powerful way to build confidence is by leveraging the trust in digital payments that has been developed over decades.

17. Source: Government of Ukraine. Digital Country. Page accessed 2 September, 2024.
18. itsme. itsme, super easy and super secure. Page accessed 20 August, 2024.
19. Bhutan NDI. We enable trusted interaction between individuals and service providers. Page accessed 28 August, 2024.

Box 2 — Considerations for the use of biometrics in digital identity systems

Capturing and storing biometric information about a person — such as face and fingerprints — is an essential part of establishing a foundational identity and provides the basis for identity documents such as passports and identification cards. Biometric information is often used in digital transactions to identify or authenticate a person in a convenient way. However, due to the sensitivity of biometric information, care must be taken on how it is used, stored and shared.

Using biometrics for **user identification** (1-to-N matching) introduces several key changes compared to the current use of **biometrics for verification** (1-to-1 matching) that change risk management considerations. Note: These options are different from device biometrics — where the person is authenticating to the device by using biometrics stored on the device, such as Touch ID or Face ID. For device biometrics, the biometric traits are only evaluated locally on the mobile device; this confirms "same person as registered their face on the device" — not the identity of the person.

1 Data security

Biometric data can be broken down into two categories: biometric traits, which are complete and fixed representations of a person's biometric (e.g., image of a face), and biometric templates, which are mathematically derived representations of a person's biometric and can be deleted or revoked. Biometric traits are unique, private and cannot be reissued if compromised. Given the sensitive nature of biometric traits, any centralised solution must not store them.

A template means that the biometric traits are reduced to numbers which describe the distance between elements of the biometrics. These numbers can further be encrypted in such a way that it is not possible to re-create the biometric trait (such as the face) of the person and that only entities that are authorised can encrypt and use the biometric template.

The possibility of biometric templates being compromised and subsequently used in fraud attacks implies that any biometric identification solution needs to deploy security measures to protect the templates as well as render compromised templates unusable. This includes the highest levels of encryption to protect templates and the underlying traits as well as incorporating liveness tests to minimise the possibility of verifying identity with stolen biometric templates and creating a process to delete and re-enrol biometric templates when a compromise is detected. The technology available to fraudsters is evolving fast and there is evidence that fraudsters have been able to defeat liveness detectors and use compromised biometric templates or deepfakes to complete authentication or identification, which further increases the data security risk.[20]

20. The Verge. Liveness tests used by banks to verify ID are 'extremely vulnerable' to deepfake attacks. 18 May, 2022.

2 Privacy

When biometrics are used for verification (1-to-1 matching), the biometric template is typically stored locally on the user device, and the device conducts the verification. Alternatively, the biometric template is stored at a secure server. The user presents a credential (for instance a card, mobile number or username), and their biometrics (e.g., their face) are compared against a known picture (biometric template) of the person (for instance, their biometrics are captured and hashed into a biometric template during the identity verification process of onboarding the person).

When biometrics are used for user identification (1-to-N matching), solutions typically include a central repository of biometric templates to do the matching. This means that government agencies or private companies that provide this service will collect and store biometric templates and, in some cases, raw biometric data for millions of users. This has significant data transportation, encryption, storage and privacy implications.

3 Bias and fairness

Several biometric solutions (e.g., facial recognition) are known to perform better on certain demographics. For example, fingerprint recognition is less accurate for children under 12 and adults over 70 because their fingerprints are less defined or still evolving.[21] Variation in the accuracy and precision of outputs from machine-learning-based solutions can be further exacerbated by potentially biased datasets that are used to train the algorithmic models at the heart of biometric solutions — particularly where there is variability in the quality and robustness of data inputs from across demographic groups. A scalable solution must meet expected performance metrics equally for all demographics and follow best practices for fairness. Visa recognises bias as one of the greatest risks posed by AI, and we proactively monitor and mitigate bias through a multilayered governance and accountability structure for the models and algorithms that can feed into biometric solutions.

21. IEEE Transactions on Information Forensics and Security. Fingerprint Recognition of Young Children. July 2017.

4 Technology neutral legal frameworks

The regulatory landscape associated with biometrics use is evolving fast. One of the challenges associated with biometric identification is the number of participants involved and the resulting lack of clarity around where the liability sits. With biometric identification solutions, the number of companies/actors that will access the biometric template is potentially large. Biometrics may be collected on devices produced by certain vendors, and the templates will be produced and stored by solution providers that will likely not be consumer-facing. The processing and federation of the templates may involve even more vendors. This distributed model will mean that the number of potential failure points could be large. It is therefore imperative for governments to consider concurrently the technical infrastructure design, data security and the legal framework that governs digital identity management, stakeholder commitments and citizen protections.

5 Performance and accuracy

With biometric verification uses cases, scaling the solution should have lower impact on the 1-1 matching performance. However, when addressing biometric identification use cases, the current accuracy of widely available biometric methods may not be suitable for large-scale user identification. Within smaller pools of individuals, current technology can be reliable, but for a fully interoperable solution spanning millions of consumers, accuracy must be improved. A rate of false positives of 1 percent of 1 million individuals is still 10,000 falsely identified individuals. A viable solution should: (a) meet a minimum standard of accuracy, (b) utilise a second factor of identification when it cannot achieve the necessary level of confidence and (c) work within a robust liability framework in case a false positive does occur.

6 Interoperability

Where biometrics have been deployed in the world of commerce, most of the solutions are not interoperable. They work only at merchants that use the solution from the vendor that has deployed the solution. This is not unlike national digital identity biometrics deployed to date where largely there is a lack of common standards used by national or state agencies. This lack of interoperability requires users to register their biometrics with many providers, further exacerbating data breach risks and challenges in interoperability — not to mention providing a poor customer experience.

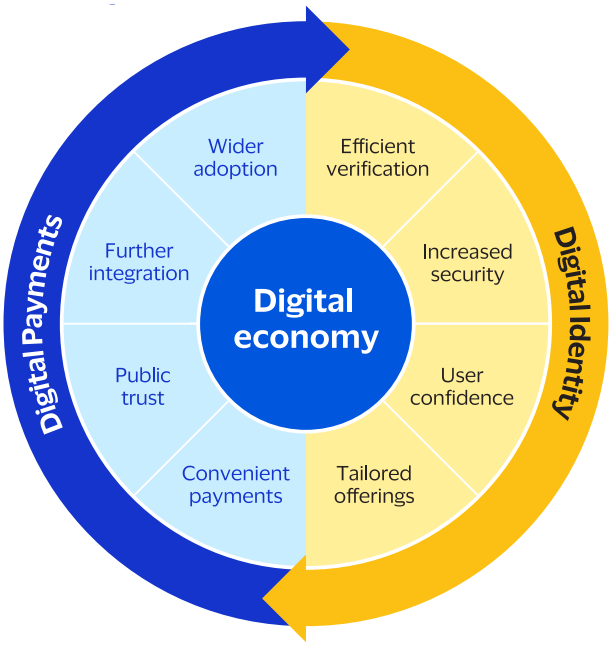
Source: Visa analysis; including insights from the Information Commissioner's Office (United Kingdom) and National Institute of Standards and Technology.

Payments are a natural extension of digital identity, and Visa can help drive adoption

There can be a mutually reinforcing relationship between payments and digital identity

The private sector can play a crucial role in driving adoption by helping consumers understand the benefits of having a digital identity "firsthand" through compelling and frequent use cases, such as renting a car or buying medicine. With technological expertise and proficiency in security, compliance and user experience, specific parties in the private sector should be considered important partners to governments. Payments — especially those using digital wallets — are ideal for accelerating the adoption of digital identity systems, creating a virtuous cycle that benefits both domains.

Payments can help drive digital identity adoption by offering a clear and immediate value proposition: Payments are a part of everyday life, and they often involve authentication processes that digital identity will help enhance. The frequency of payment transactions creates numerous opportunities for end-users to interact with and become comfortable with biometric authentication processes.



In the future, citizens may be asked to verify their identity for some higher-risk purchases, or when a periodic verification might be required. They complete this verification process using a familiar biometric experience they use everyday, on their device. The familiarity of using biometrics to perform tasks on their device will be the same simple process to verify it is them completing a payment. This linkage between identity verification and payment authentication is likely to drive increased trust in digital identity technology and processes in other contexts (e.g., eKYC). Financial institutions and payment providers may further promote digital identity adoption by integrating these systems into their services. Digital identity integration improves security, reduces fraud and streamlines customer onboarding, demonstrating the practical benefits of digital identity to a wide audience.

This virtuous cycle accelerates growth and adoption for digital identity and digital payments alike. As digital identity systems become more widespread due to their use in payments, they become more valuable for other applications. Simultaneously, as digital identity systems improve, gain trust and — over time — become integrated into payment authentication, they could make digital payments even more secure and efficient. Many governments are now exploring the design and issuance of central bank digital currencies (CBDCs), and digital identity will be key to the use of this new form of digital public money. Digital IDs will provide a secure and efficient means of verifying users' identities, enabling proper Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance.

> Payments offer a familiar and frequent way to use digital identity. In turn, digital identity systems can enhance payments in several ways. This virtuous cycle accelerates growth and adoption for both.

Visa and the private sector are working with the public sector to support digital identity standards

To reiterate, the public and private sectors both have roles to play in achieving the benefits of digital identity. Governments should create predictability and certainty for the private sector and protect citizens' rights for digital identity. Governments also have a role to play by introducing regulation designed for outcomes, citizen protection, consent, liability, etc. — and allowing the correct security standard to be determined by the private sector for the right commerce application. Not all scenarios where identity verification is needed require that full identity information be disclosed. Via EMVCo, Visa developed the standards for payment tokenisation and contactless payments with similar outcomes by design. These standards have had a profound effect on the expansion of secure digital commerce for citizens and reach for merchants across payment networks. Visa is working with standards organisations such as ISO, W3C, OIDF, EMVCo, FIDO to develop the necessary technologies to deliver the identity ecosystem and to ensure that IDs and wallets can work with and be interoperable with payment infrastructures. Open standards create a platform for innovation and a promise of interoperability. Some important areas of digital identity collaboration are detailed in the following examples, which include the role Visa is playing.

Open standards create a platform for innovation and a promise of interoperability.

Box 3 — Visa's collaborations in the digital identity ecosystem

eIDAS and the EU Digital Identity wallet

eIDAS (electronic IDentification, Authentication and trust Services) is a regulation in the European Union which creates a framework for secure digital identities and electronic transactions across EU member states. eIDAS requires each member state to issue a digital identity (eID) to people and businesses (natural and legal persons). These digital identities must conform to certain specifications and enable EU citizens to use their national eIDs across borders throughout the European Economic Area (EEA). eIDAS was first introduced in 2014 and updated in 2024 as eIDAS 2.0. eIDAS 2.0 introduces the concept of European Digital Identity Wallets, aligning with self-sovereign identity principles. These wallets allow users to store and manage their digital identities and credentials, giving them more control over their personal data. These wallets must conform to specific standards (e.g., OIDC4VC, ISO18013-5) to ensure interoperability across industries and borders. eIDAS also establishes a trust framework for electronic signatures, seals, timestamps and website authentication. The EU Digital Identity (DI) wallets must deliver identity services at the highest assurance level (Level of Assurance High), satisfying the customer identification requirements for bank account opening and health services.

The eIDAS regulation requires the private sector to adopt EU DI wallets for strong user authentication. This includes use cases such as onboarding, login, age verification, KYC for account opening, and payment authentication. Payment is considered a key use case to drive adoption of the EU DI wallet by making it useful for a range of activities relevant to citizens, businesses and governments. EU member states must ensure that their citizens and businesses can have an EU DI wallet by end of 2026, while the private sector must be able to support the EU DI wallet by end of 2027. While businesses must provide consumers the ability to use the EU DI wallet for identity proofing and login, it is voluntary to use for the citizen.

Visa is currently the domain expert for payments in the EU Digital Identity Wallet Consortium (one of the consortiums piloting the use of the EU DI wallet as part of the European Commission-managed large-scale pilots) and is leading the work to define how the wallet can be used for payment authentication for e-commerce and payment initiation for in-person and e-commerce, cards and accounts.

Payments are considered a key use case to drive adoption of the EU DI wallet by making them useful for a range of activities relevant to citizens, businesses and governments.

FIDO Alliance and passkeys

The FIDO (Fast IDentity Online) Alliance is working on passkeys as a more secure and user-friendly alternative to traditional passwords. Passkeys are a type of cryptographic credential that eliminate the need for users to remember complex passwords and provide stronger protection against phishing and credential stuffing.[22,23] They provide a standard way to authenticate, improving both security and user experience in digital identity management. Major technology companies are implementing passkey support into their platforms in the hopes of increasing widespread adoption of this technology in digital identity ecosystems.[24] Visa, a board member of the FIDO alliance, is working to deploy passkeys for payment transactions in a way that allows end-users to rely on biometric authentication regardless of where they use their card to deploy passkeys for payment transactions in a way that allows end-users to rely on biometric authentication regardless of where they use their card. The recently announced Visa Payment Passkeys™ Service binds an account credential with a device, enabling an end-user to use the same biometrics they use to unlock their device for payment authentication. See the next section for more on Visa Payment Passkeys.

The OpenWallet Foundation and consumer choice

The OpenWallet Foundation (OWF) is an initiative of the Linux Foundation focused on public-private sector collaboration in developing open-source code for components enabling secure, interoperable and privacy-preserving digital wallets. The OWF does not aim to produce a wallet, but rather to provide a foundation in the form of open-source code components for organisations to use in building their own wallet solutions. This approach supports the development of diverse and innovative wallet applications while maintaining secure code and infrastructure that is common and interoperable. The foundation's work facilitates the creation of wallets capable of storing and managing digital identity credentials securely. OWF's current focus is on delivering code components to enable the EU DI wallet. Visa is a founding member of the OpenWallet Foundation and currently chairs the board.

OIDF and standards for identity services

The OpenID Foundation (OIDF) is a nonprofit organisation working to advance open standards for digital identity. It develops and maintains the OpenID Connect protocol, which allows users to authenticate across multiple platforms using a single identity. OIDF focuses on improving security, privacy and interoperability in digital identity solutions and wallets. Visa is a participant in OIDF efforts and sits on the board.

22. Source: National Cyber Security Centre. Use of credential stuffing tools. Page accessed 25 October, 2024. Credential stuffing takes advantage of people reusing username and password combinations across different accounts. By fraudulently gaining valid combinations for one site, and successfully using them on other sites, an attacker can access legitimate accounts. The primary motivation is financial, but it can lead to identity theft.
23. Source: FIDO Alliance. Introduction to Passkeys. Page accessed 24 October, 2024.
24. Source: FIDO Alliance. Live Implementations of Passkeys. Page accessed 24 October, 2024.

Visa's Payment Passkeys can further help payments be a flywheel for digital identity adoption

Visa has long worked to build trust in digital payments, and this has created strong network effects on adoption by end-users. Passkeys, as described before, are a type of cryptographic credential that eliminate the need for users to remember complex passwords and that provide stronger protection against phishing and credential stuffing. Visa has been a key innovator of modern digital payment credentials. Device-bound tokens, which secure the consumer's cardholder data, have strong provenance (record of ownership) associated with them, and they can be presented, authenticated and transacted via a more intuitive and easy-to-use user experience. They have also been deployed widely in digital payment wallets in mobile devices. Visa is now enabling access to secure biometrics-based authentication through Visa Payment Passkeys.

At their core, Visa Payment Passkeys are on-device biometrics-based access keys that enable users of smart mobile devices to prove that they are the legitimate owners of the device. Once this authentication is performed, the user can then be allowed access to a secure payment credential, which is a tokenised card number bound uniquely to the device, as well as the payment method underlying it. Visa envisions a parallel for digital identity — the same smart mobile device will also hold digital identity credentials that have been attested by identity providers and that will enable verification that can be utilised by relying parties.

Passkeys are grounded in a well-known, robust cryptographic standard called public/private key cryptography. Passkeys may not always have device-bound provenance. In case of Visa Payment Passkeys, Visa establishes a unique link between the passkey and device for the cardholder's payment credential. This enables greatly simplified authentication user journeys for both identity and payments credentials. Proving 1) you are who you say you are, and 2) that you are authenticating a payment using your on-device biometrics on the same device that you enrolled the Visa Payment Passkey on.

Visa is working with organisations like the OpenID Foundation (OIDF), EUDIW (European Digital Identity Wallet) Consortium, W3C (World Wide Web Consortium) to support specifications for verifiable credentials. The OIDF is developing standards called OID4VC (Open ID for Verifiable Credentials) and OID4VP (Open ID for Verifiable Presentations) that can be used to present these credentials. This will enable future developments on any existing identity infrastructure, such as OIDC (OpenID Connect), as well as new identity systems that may emerge.

In either case, the common underlying Visa Payment Passkeys will be a mechanism for users to prove their identity and prove their intent in the context of payments and commerce. Importantly, they can also be used for providing consent. Visa Payment Passkeys can also be an enabler of future product innovations, such as Data Tokens, which can facilitate highly personalised engagement opportunities for merchants. Visa's work on Payment Passkeys will help augment the mutually reinforcing relationship between payments and digital identity to benefit all stakeholders and end-users.

8.5B

As an example, one can consider cross-border payments. The Visa Direct network already helps partners move money to over **8.5 billion endpoints** (cards, accounts and digital wallets) in **over 190 countries**.[25]

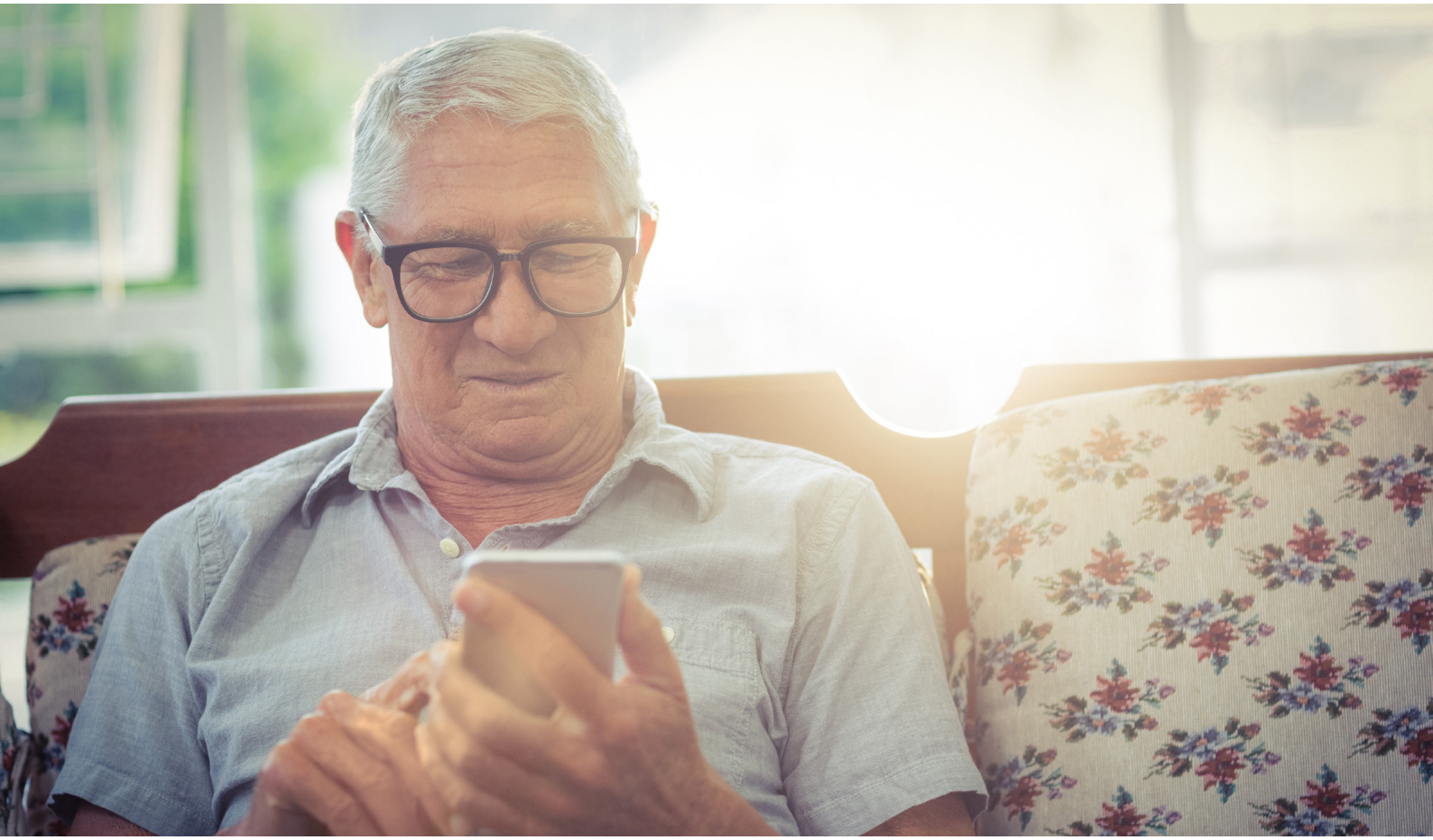
Using digital identity in the form of Visa Payment Passkeys with Visa Direct could significantly improve KYC and AML/CFT compliance processes for sending and receiving financial institutions, contributing to cost-effective cross-border transfers for remittance senders, small businesses and other end-users. Using Passkeys in concert with global networks adds to the virtuous cycle between payments and digital identity.

25. Source: Visa Direct, helping transform global money movement. Page accessed 12 September, 2024.

Visa is ready to partner

Digital identity that is inclusive for everyone, everywhere can be a common good and a fundamental part of a nation's digital infrastructure

Digital identity benefits people, businesses (small and large), and governments, and enhances numerous services — including education and health systems. There are great advantages to public and private sector collaboration in the associated design and deployment stages, as together they can create trustworthy digital identity capabilities that provide end-users access to improved services across a wide spectrum of life — all while lowering costs and improving efficiency. Visa brings a wealth of global and local payments expertise, fraud and risk mitigation experience, secure data management knowledge, and a record of open industry collaboration with a focus on reducing friction for all stakeholders. In an ever more connected world, now is the time to design and deploy digital identity systems nationally that are recognised globally.



Appendix

Appendix 1 — Details on common attributes of digital identity systems

Core identity management	Unique identifier	→ A unique, persistent identifier for each individual or entity; could be alphanumeric, biometric or a combination
	Identity proofing	→ Robust processes to verify the identity of individuals during enrollment; may include document verification, biometric capture and background checks
	Lifecycle management	→ Processes for identity creation, maintenance and eventual deletion; regular updates and attribute verification
	Revocation and recovery	→ Mechanisms to revoke compromised credentials; processes for identity recovery in case of loss or theft
	Identity wallets	→ While the specific implementation may vary between different digital identity systems, the concept of an identity wallet or similar user-controlled storage and management tool is fundamental to most approaches; wallets can be issued by public or private sectors for various use cases
End-user empowerment	Consent management	→ Tools for end-users to control who accesses their data and for what purpose; clear, user-friendly interfaces for granting and revoking permissions
	User control	→ Self-service portals or apps for users to manage their identity information; ability to view access logs and activity history
	Accessibility	→ Inclusive design to accommodate users with disabilities; support for multiple languages and cultural considerations
	Self-sovereign identity (SSI)	→ Allowing individuals to own and control their digital identities without relying on a centralised authority
	Selective disclosure	→ Allowing users to share only the specific identity attributes required for a particular transaction or service
	Contextual identity	→ Adapting the level of identity information shared based on the context of the interaction

Source: Visa analysis

Governance and compliance	Governance framework	→ Clear policies and procedures for identity management; compliance with relevant regulations (e.g., GDPR, CCPA)
	Trust framework	→ Established relationships between identity providers and relying parties; clear liability and responsibility allocation
	Auditability	→ Transparent logging of all identity-related activities
	Audit trails	→ Mechanisms to revoke compromised credentials; processes for identity recovery in case of loss or theft
Security and authentication	Authentication mechanisms	→ Multifactor authentication (e.g., password, biometrics, tokens); risk-based authentication that adjusts security levels based on context
	Security measures	→ Strong encryption and secure storage of identity data; regular security audits and penetration testing; incident response and recovery plans
	Privacy protection	→ Data minimisation principles to collect only necessary information; encryption for data at rest and in transit; anonymisation or pseudonymisation techniques where appropriate
	Biometric integration	→ Incorporation of biometric data such as fingerprints, facial recognition or iris scans for stronger authentication
	Multifactor authentication	→ Combining multiple verification methods (e.g., something you know, something you have, something you are) for increased security
	Continuous authentication	→ Ongoing verification of a user's identity throughout a session, rather than just at login
	Adaptive risk assessment	→ Using AI and machine learning to dynamically assess the risk level of transactions and adjust authentication requirements accordingly

Source: Visa analysis

System design and performance	**Interoperability**	→ Standards-based approach for compatibility with other systems; APIs for integration with various services and applications
	Scalability	→ Ability to handle a growing number of users and transactions; performance optimisation to ensure quick response times
	Flexibility	→ Support for different levels of assurance based on use case; ability to add or modify attributes over time
	Cross-border interoperability	→ Designed to work across different systems, platforms and national borders
	Federated identity	→ Enabling users to use the same digital identity across multiple platforms or services
	Decentralised architecture	→ Utilising technologies like blockchain to create decentralised identity systems that give users more control over their data
	Privacy-enhancing technologies	→ Implementing zero-knowledge proofs or other cryptographic techniques to allow identity verification without revealing unnecessary personal information
	Revocable credentials	→ The ability to revoke or update identity credentials without compromising the entire identity
	Recovery mechanisms	→ Robust processes for identity recovery in case of loss or compromise

Source: Visa analysis

Acknowledgements

Authors of this paper include Robert Walls, Piers Clough, Marie Austenaa, Parth Awasthi, Milja Radosavljevic.

The authors would like to thank the following colleagues for their input and review: Matthieu Charpentier, Jalpesh Chitalia, Julie Jones, Henna Kapur, Andreas Efthymiou, Gilles Verstraeten, Chad Harper, Rami Amin, Tod Frincke, Charles Crossley.

References

All data sourced and referenced within the paper was checked against the appropriate sites and was available and current at the time of publication.

Bill & Melinda Gates Foundation. (2023). Digital IDs are an effective tool against poverty. gatesfoundation.org/ideas/articles/mosip-digital-id-systems. [Accessed 20 August, 2024].

Bhutan NDI. We enable trusted interaction between individuals and service providers. bhutanndi.com/. [Accessed 28 August, 2024].

European Commission. A digital ID and personal digital wallet for EU citizens, residents and businesses. ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home. [Accessed 24 September, 2024].

FIDO Alliance. Introduction to Passkeys. passkeycentral.org/introduction-to-passkeys/. [Accessed 24 October, 2024].

FIDO Alliance. Live Implementations of Passkeys. passkeycentral.org/resources-and-tools/live-implementations. [Accessed 24 October, 2024].

Financial Action Task Force (FATF). (2020). Guidance on Digital Identity. fatf-gafi.org/publications/documents/digital-identity-guidance.html. [Accessed 17 September, 2024].

GSMA. The Mobile Economy Europe 2023. (2023). gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/11/GSMA-Mobile-Economy-Europe-2023.pdf. [Accessed 13 October, 2024].

Government of Ukraine. Digital Country. ukraine.ua/invest-trade/digitalization/. [Accessed 2 September, 2024].

IEEE Transactions on Information Forensics and Security. Fingerprint Recognition of Young Children. (2017). ieeexplore.ieee.org/document/7782364. [Accessed 27 October, 2024].

Information Commissioner's Office. Biometric data guidance: Biometric recognition. ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition. [Accessed 28 October, 2024].

Information Commissioner's Office. How do we process biometric data fairly? ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-fairly/. [Accessed 24 September, 2024].

International Telecommunication Union (ITU). (2021) Knowing your customer electronically: Guidance on digital ID acceptance. itu.int/hub/2021/08/knowing-your-customer-electronically-guidance-on-digital-id-acceptance/. [Accessed 18 September, 2024].

itsme. itsme, super easy and super secure. itsme-id.com/en-BE. [Accessed 20 August, 2024].

Juniper. (2024). Global eCommerce Payments Market: 2024–2029. juniperresearch.com/research/fintech-payments/ecommerce/ecommerce-payments-market-report/. [Accessed 24 October, 2024].

McKinsey & Company. (2021). COVID-19: Making the case for robust digital financial infrastructure. mckinsey.com/industries/financial-services/our-insights/covid-19-making-the-case-for-robust-digital-financial-infrastructure. [Accessed 26 September, 2024].

McKinsey Global Institute. (2019). Digital identification: A key to inclusive growth. mckinsey.com/~/media/McKinsey/Business Functions/McKinsey Digital/Our Insights/Digital identification A key to inclusive growth/MGI-Digital-identification-In-brief.pdf. [Accessed 25 July, 2024].

National Cyber Security Centre. Use of credential stuffing tools. ncsc.gov.uk/news/use-credential-stuffing-tools. [Accessed 25 October, 2024].

National Institute of Standards and Technology. Biometrics. nist.gov/programs-projects/biometrics. [Accessed 28 October, 2024].

The Verge. (2022). Liveness tests used by banks to verify ID are 'extremely vulnerable' to deepfake attacks. theverge.com/2022/5/18/23092964/deepfake-attack-facial-recognition-liveness-test-banks-sensity-report. [Accessed 14 October, 2024].

Unique Identification Authority of India. About your Aadhaar. uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html. [Accessed 15 October, 2024].

United Nations Development Programme. (2022). How digital can close the 'identity gap'. undp.org/blog/how-digital-can-close-identity-gap. [Accessed 2 September, 2024].

Visa. Visa Direct, helping transform global money movement. usa.visa.com/products/visa-direct.html. [Accessed 12 September, 2024].

Visa Economic Empowerment Institute. (2021). Policy enablers for advancing digital identity frameworks: Insights and recommendations for public and private sectors. usa.visa.com/content/dam/VCOM/global/sites/visa-economic-empowerment-institute/documents/veei-policy-enablers-for-digital-id.pdf. [Accessed 11 July, 2024].

Wilson Center. (2023). (Digital) Identity Crisis: The US Needs a National Strategy for Digital Identity to Enhance Economic Competitiveness and Mitigate Cybersecurity Risks. wilsoncenter.org/article/digital-identity-crisis-us-needs-national-strategy-digital-identity-enhance-economic. [Accessed 2 October, 2024].

World Bank. (2019). Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable. World Bank. worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable. [Accessed 24 July, 2024].

World Bank. (2023). 850 million people globally don't have ID — why this matters and what we can do about it. World Bank. blogs.worldbank.org/en/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about#:~:text=Yet%20according%20to%20new%20estimates,starting%20with%20counting%20the%20uncounted. [Accessed 24 July, 2024].

World Bank. Identification for Development. id4d.worldbank.org/. [Accessed 3 September, 2024].

World Economic Forum (WEF). (2021). How digital identity can improve lives in a post-COVID-19 world. weforum.org/agenda/2021/01/davos-agenda-digital-identity-frameworks/. [Accessed 13 August, 2024.]

World Economic Forum (WEF). (2021). 5 reasons to participate in digital identity ecosystems. weforum.org/agenda/2021/11/5-ways-a-digital-identity-ecosystem-could-help-people-and-business/. [Accessed 13 August, 2024].