Monetary Authority of Singapore

FOUNDATIONAL DIGITAL INFRASTRUCTURES FOR INCLUSIVE DIGITAL ECONOMIES

— CONTENTS —

— FOREWORD —

The digital revolution is radically transforming the way we live and work. Digital solutions have helped to enhance the economic and social well-being of millions of people around the world.

The next stage of the digital revolution is to move beyond fragmented digital solutions to digital infrastructures that will spur more pervasive digitalisation across economies and societies.

Digital infrastructures will enable interoperable solutions and seamless services – to reach more people and businesses, at lower cost and greater convenience. Public foundational digital infrastructures will be critical for inclusive economic and social development.

Much like how physical infrastructure spurred the advent of the industrial economy, foundational public digital infrastructures will accelerate the growth of the digital economy.

This report sets out the four key pillars of a foundational digital infrastructure: Digital Identity, Authorisation and Consent, Payments Interoperability, and Data Exchange. These are the four essential ingredients to enable end-to-end digital transactions; they collectively meet the foundational needs of a digital economy.

Take digital payments, for example. Only a foundational digital infrastructure comprising these four pillars will enable us to effectively and efficiently tackle the big pain points in digital payments, especially cross-border: know-your-customer checks; verifying accounts; sanctions screening; cheaper, faster, and more secure payments.

The report starts with a survey of the available literature on establishing digital infrastructures and related policies, and goes on to provide an in-depth analysis of the role of digital identity in the development of digital infrastructure in Brunei, Cambodia, Ghana and Kenya.

The four countries are in different stages of digital infrastructure development and were motivated by different considerations. Brunei is launching a single portal to access a wide variety of services, with a vision to digitally transform the country. Cambodia is building a digital infrastructure with digital identity at the core, to let end-users share data across different government ministries. Ghana has just introduced a national identity card, which marks the starting point for its journey towards a universal national identity system. Kenya has introduced a national identity database to consolidate different data identity silos and is now looking to build other public services on this system.

This pioneering collaborative work was made possible with the support of the Monetary Authority of Brunei Darussalam, National Bank of Cambodia, Bank of Ghana and the Central Bank of Kenya as well as Mastercard.

We hope this report will help players in the financial sector and broader technology community to better understand the key value drivers of a strong digital infrastructure, and inspire them to explore the digital infrastructure potential for cross-border use.

Ravi Menon, Managing Director, Monetary Authority of Singapore

BACKGROUND

01

The current world population now stands at over seven billion people and almost 60% is now using the internet[1] to access information and to communicate. Economic transactions are increasingly performed digitally or facilitated through digital means, with profound impact on trade, jobs and the future of work. A rural farmer can bypass the middle-man and sell directly to consumers, and a digital worker can provide his services to anyone anywhere in the world.

Digitalisation is a great leveller of opportunities and enables countries to leapfrog and improve the economic and social well-being of its people. There are many examples where improving access to knowledge and services have accelerated and enabled inclusive economic development. It is imperative that governments provide the basic fundamental digital services to its people affordably and quickly, to enable them to partake in the global digital economy.

With a clear view of the benefits of digitalisation, there have been efforts by governments, non-profit organisations, and impact foundations in harnessing the power of foundational digital platforms to improve people's lives.

Digital infrastructures refer to the systems, applications, and hardware that allow users and their devices to digitally interact with one another and includes the expansion of use from PCs and smartphones to connected homes, cars, wearables and beyond.

This digital infrastructure effectively sits 'on top' of the internet and provides for the basic requirements to accelerate the digital economy. First, it supports increased access to public and private services – for people, businesses and public institutions. Second, it creates trust in a non-physical environment to enable everyone to interact and transact in a way that is authenticated and therefore safe. Third, it drives open markets by creating level playing fields that stimulate innovation in the interest of both growth and choice for users. Finally, it has the very real potential to lower cost by finding more adaptive and efficient ways of delivering digital services at scale.

The global trend and rapid digitisation clearly accelerates demand for the right infrastructure. Compounded by the COVID-19 pandemic, more awareness, higher need, and a greater urgency for this common good exists. In that context, **policy makers must act** to support their people across their health, social, and economic needs. This paper shows how a digital infrastructure can meet those seemingly ambitious (but absolutely foundational) needs in a way that sets a framework for their digital economy by building and delivering both public and private sector services.

Unlocking the key value drivers requires a strong digital infrastructure that is underpinned by four key pillars or requirements:

- **Digital Identity:** Digital identity is about establishing confidence and trust at both ends of the digital interaction. Every participant must be confident the party at the other end is who they say they are. Mechanisms need to be established to ensure authentication and validation of individual's identity while providing privacy and security of information. And this requires trust in the system that mediates that interaction.

- **Authorisation and Consent:** Digital interactions should be transparent, secure, and efficient. By providing interactions that recognise the importance of authorised and

1 Source: International Telecommunication Union https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

transparent use of data, as well as models that leverage individual consent, data will be able to be used and shared in accordance with the purposes that it has been provided and in a manner that is expected and understood by individuals. There is a range of techniques and tools that can be built into digital infrastructures that allow individuals to better understand how their information is being collected, used and shared; and there are mechanisms that also permit individuals to own, manage and control their personal and sensitive data.

- **Payments Interoperability:** For payments to function globally, mechanisms must be established to ensure interoperability of systems. Payments interoperability is concerned with the mechanisms by which two banks (or appropriately supervised entities) clear and settle payments between their customers. Interoperability is a complex and multi-dimensional topic that encompasses governance, technical and branding components.

- **Data Exchange:** Supported by initiatives like Open Banking, data exchange is the means by which individuals or businesses consent to have their financial and potentially other data made available to third parties to use for the benefit of that individual or business. Data exchanges function by being made available from a data provider (e.g. a financial institution) to the chosen functionality that needs to use the data for the benefit of the individual, such as a payment solution predicated upon the individual's consent or acknowledgment. Data exchange enables payments, financial planning, the creation of a digital identity, the creation of credit files, and other services necessary to enable a digital economy.

In contrast to the internet infrastructure, setting up a digital infrastructure involves more than merely technological standards. In digital payments (including cards) for example, domestic and cross-border financial value exchanges are built on trusted networks that are governed by legal, business, and technical agreements and standards to safeguard trust in the network. As data is becoming increasingly valuable in the digital economy, there is a strong rationale to apply 'digital payment-like' governance and mechanisms to ensure trust in digital infrastructures. This ultimately results in a digital infrastructure that allows end-users to control both their money and data in a trusted manner, by placing the individual at the centre of the digital ecosystem.

Within this whitepaper is an evaluation of how several countries are currently implementing their digital infrastructures, showing how the local market context, culture, laws and approach towards issues such as privacy, security, digital identity and data use impacts design decisions. Through interviews with relevant stakeholders in a select number of countries in Africa and Asia, an overview is provided of their vision, ambition, where they are in their journey, and how they might move forward individually, and potentially as a community. Four key insights are drawn from the interviews: First, policy makers shape a broad vision of the benefits of a digital infrastructure, but face challenges in taking a holistic perspective on how to execute that vision. Second, government bodies are taking a leading role in initiating the digital infrastructure and digital identity, mostly driven by the ministry already responsible for the national identity program. Third, technology is only one part of the puzzle - balancing local regulatory, technology, and business requirements is important for a harmonised, networked solution. Lastly, to ensure

widespread market adoption, it is critical to focus on building trust with the end-user.

Policy makers who are considering developing a digital infrastructure solution for their respective market will need to look at creating a common strategic understanding, defining the right regulatory enablers, making use of relevant adoption accelerators and liaising with relevant stakeholders to ensure a fit-for-purpose model and solution design.

A final point to note is the value of tempering a natural inclination by governments to regulate in the interests of innovation. While there will sometimes be clear need to act in the interests of a country where there has been some form of market failure, the best motivation for innovation has historically been commercial. Technological developments are regularly delivered by companies who have identified a gap in a market where end users (consumers, businesses or governments) have a need that is not being met. Innovation for innovation's sake is folly. Innovation must deliver something that is both required and desired.

That's not to say government has no role to play here. Ensuring the climate is right for investment in innovation is vital. Singapore has long been the global benchmark having found the right balance between encouraging investment in new technologies (for example in financial services) while also protecting its people from high risk bad actors. That takes active engagement both within the bureaucracy as well as at an Executive level.

A future phase and version of this document is envisaged that will further examine digital identity progress in other countries, e.g. across the continents of Europe, Latin America and North America, including the digital identity potential for cross-border use, along with further detailed insight on the other three pillars of a digital infrastructure. MAS will also collaborate with the BIS Innovation Hub in Singapore to explore the opportunities to improve cross-border payments by integrating them with cross-border access to digital identities.

METHODOLOGY FOR THE WHITE PAPER

02

2.1 CONTENT IN THE CONTEXT OF SINGAPORE AND OTHER COUNTRIES THAT HAVE ALREADY DEVELOPED SOME OF THE NECESSARY DIGITAL INFRASTRUCTURE

This paper has been published by the Monetary Authority of Singapore and has been written in collaboration with industry experts. The data collection and analysis strategy started from an explorative analysis of the relevant available literature and a desktop review of a wide range of existing practices in other countries that are in the process of establishing digital infrastructures and related policies. This first stage aimed to gain insight in the overall status on the role of digital infrastructure in the development of digital society, and discover relevant practices and developments in the different countries. The second stage involved in-depth fact gathering and analysis of four countries.

2.2 DATA COLLECTION AND CASE STUDIES FOR OTHER COUNTRIES THAT ARE BEGINNING THEIR DIGITISATION JOURNEY

To gather additional evidence and supplement the information collected through desk research and submitted by industry experts contacted in the research process, additional interviews were conducted with experts from several countries (Brunei, Cambodia, Ghana, Kenya) for a more in-depth analysis of the role of digital identity in the development of a digital infrastructure. For each country, information was collected on what the market opportunity and objectives were, the local demand, pre-conditions, and what other aspects might be needed to facilitate trust with local citizens. The study team also aimed to achieve a fair representation of good practice and demonstrate where innovation is taking place. The in-depth analysis allowed the researchers to further investigate the motivations and outcomes of the introduction of a digital identity. Information was collected through interviews with experts from Government communities of the different countries. The number of interviews and profiles of the interviewees varied across countries, but the researchers strived to ensure a balanced set of interviews.

THE IMPORTANCE OF A DIGITAL INFRASTRUCTURE

03

3.1 WHY COUNTRIES NEED A DIGITAL INFRASTRUCTURE

Digital transformation in society at large (public and private) is essential for economic progress. As we have almost maximised our economic output from raw materials, the alternative economic growth opportunity is digital. Therefore, it is important to shift from the physical transaction world towards a digital space that can deliver improvements, enrichment, convenience, low costs and more efficiency for public and private services. Four strategic topics should be considered to shape the route to a digital infrastructure. These topics are highlighted below.

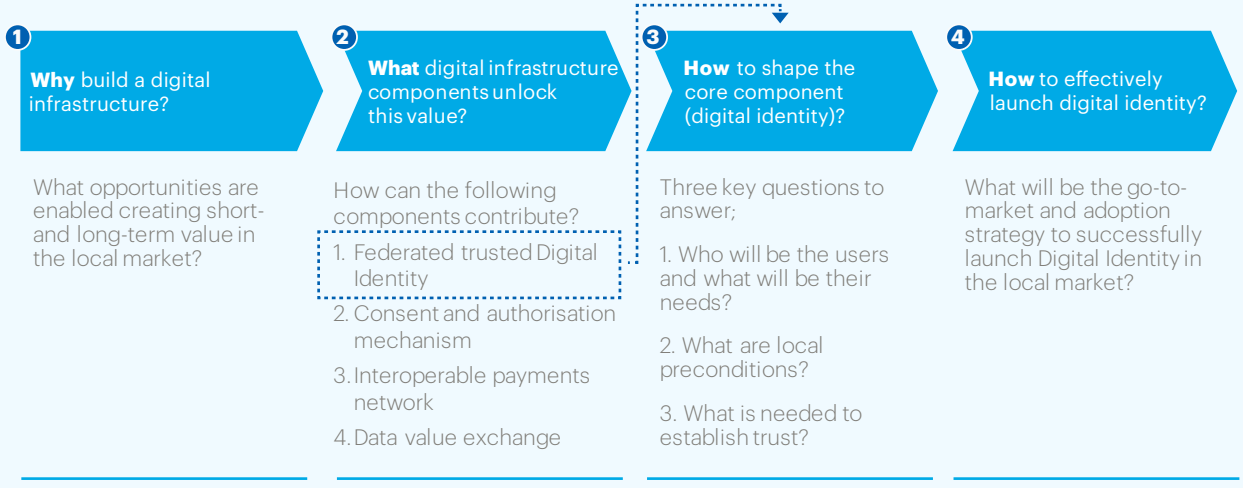
3.2 A STRATEGY FOR A DIGITAL INFRASTRUCTURE

Understanding the importance of and unlocking value in the digital economy requires a strong digital infrastructure. This will provide end-users more choice and more innovative services with which to interact and transact online. It also helps relying parties to build services on top of a common platform, stimulating innovation and avoiding siloed domains across organisations and sectors[2]. To realise this opportunity, a trusted standard layer is required on top of the internet where individuals, businesses and public end-users can find, access, act interoperably, and transact digitally. This enables service providers to rely on a trusted approach, avoiding siloed domains across sectors and organisations.

The second step is to understand the underlying components of a digital infrastructure and how these systems work together. The picture below shows a conceptual representation of four key digital infrastructure components.

The digital infrastructure strategy can then be developed, considering policy and regulatory requirements and the pre-conditions noted in the next section.

Figure 1: Four step approach with a focus on digital identity as a core component to design a digital infrastructure



2 Source: "Digital identity: towards shared principles for public and private sector cooperation", World Bank 2016

3.3 PRE-CONDITIONS FOR CREATING A DIGITAL INFRASTRUCTURE

Local preconditions need to be considered when creating a digital infrastructure solution. Some preconditions can work as **enablers** – what is already locally present which can be built upon? And some as **constraints** – what should be considered that may restrict the solution design?

Local preconditions determine the starting point for a digital infrastructure solution. Often there already exists an infrastructure, for example, official identity documents for physical identity, such as a passport, driver's license, or a birth certificate. Official registers often complement these documents to administer which documents are issued to whom, and whether these documents are still valid. In most cases, a digital identity can be built based on this existing physical identity infrastructure.

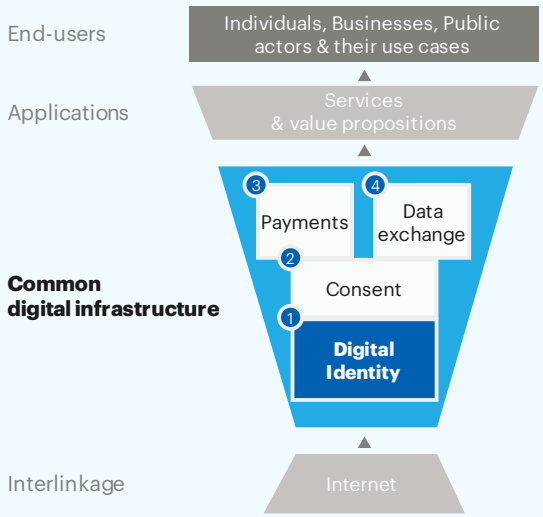
Established legal frameworks may also put forward requirements for cybersecurity, anti-money laundering, data privacy, and data protection for consideration.

3.4 GOVERNANCE OF A DIGITAL INFRASTRUCTURE

Governance of digital infrastructure can be considered at both an overall policy level and at a technical level.

Policy related governance includes regulation of communications, network and information security, payments, required levels of consent, rules to prevent money laundering, digital identity, and issues concerning digital access and education and skills. Governance at a policy level should consider the wider societal impacts of digital infrastructure and the necessary interaction with physical services, particularly the delivery of government services. This policy area also needs to

Figure 2: Four key components deliver the digital infrastructure for service providers to build value propositions to end-users



1. **Digital identity** enables end-users to represent themselves and others in the digital economy
2. **Consent** enables end-users to control their data and money when they digitally interact and transact with their service providers of choice
3. **Payments** ensures end-users can control and exchange their financial assets
4. **Data exchange** enables end-users to make their data available and accessible to any service provider of their choice for a set period of time

address digital-government issues, such as using digital infrastructure policy to make the activities of government agencies more efficient and simplify citizen and business contact with the government, for example using digital identities. Policy also should encourage investment in the country's digital infrastructure. A clear, stable regulatory framework is a key factor in protecting the interests of citizens and facilitating the growth and functioning of digital infrastructure.

Technical governance sits within each of the above-referenced four pillars to establish mechanisms for regulation, and standards setting and interoperability at the consumer and business level. Governance at a technical level can support operators to build and develop digital infrastructure, but it can also hinder innovation if the governance is too proscriptive and is not technology neutral. For example, setting technical standards for what and how data can be passed amongst systems can make it easier to effectuate data exchanges, digital identity and payments, but standards that drive to specific software would inhibit the ability to implement new technologies.

FOUR PILLARS OF A DIGITAL INFRASTRUCTURE

04

There are four essential components or "pillars" needed to support an effective digital infrastructure in a country. These are: digital identity, consent, interoperability and data exchange. This section of the paper discusses these pillars in more detail.

4.1 DIGITAL IDENTITY

4.1.1 PURPOSE

Core to the digital infrastructure is a trusted **digital identity**, enabling individuals, businesses and public institutions to represent themselves and act with permission on behalf of others in the digital economy. It is described as a common, trusted, and reusable way of transferring data. Reusable, as it eliminates the need for multiple passwords and identity-verification procedures. A digital identity allows people to use a single means of authenticating themselves across multiple digital services (including websites, apps, devices), by including identity attributes and identity documents in their underlying data[3].

This data collectively defines an individual and can be used to identify an individual, business, or public institution. The purpose of a digital identity is wider than identifying one of said end-users in a common manner. It can also confirm the end-user's ability, whether from a legal perspective or otherwise, to access a service or perform a particular task. Service providers, such as universities or banks can also add attributes to the identity by providing verifiable claims on, for example, academic records, education certificates, and income statements. Hence, this enriches the digital identity with enhanced information beyond attributes provided by a passport.

4.1.2 DESIGN/REQUIREMENTS

Connected to this identity, are mechanisms that ensure the proper use of identity and other personal data elements. Two common mechanisms are authorised uses of data such as those necessary to provide adequate security, fraud prevention and other controls; as well as other uses that are anticipated and expected due to the nature of the data use. Such legitimate uses of identity and personal data need to be explained in a clear and transparent manner so that individuals understand the use of their data for these purposes, and the data used for these purposes must be narrow and proportionate to achieve the specific purpose. For all other uses, most digital systems rely on a series of notice and consent models to ensure individuals engaged in a digital system understand the use of their information.

4.1.3 CAPABILITIES

Eliminating the need for multiple passwords and identity verification procedures, a digital identity allows people to use a single means of authenticating themselves across multiple digital services, encompassing websites, apps, devices, and more. This allows the user to verify themselves to a relying party, who requires verification to provide a good or service to the end user. The identity is owned, managed, and controlled by the individual, meaning they have the right to access, correct, and delete their identity data and the right to recourse if their rights are violated. As there is no single government, technology company, financial institution, or even industry sector that can effectively deliver a digital identity service by itself for all possible use cases, orchestration of the network across multiple parties is required

3 Source: "Platform for good digital identity", World Economic Forum 2019

within a multi-stakeholder ecosystem. This network allows data exchange between the end users, relying parties, identity verification providers (organizations that are able to verify user identity data, such as a government for a passport) and personal data storage providers (who securely store the data, such as a personal mobile device). **Section 6** will illustrate in greater detail the digital identity pillar, including examples of use cases and models for an identity verification network.

4.2 AUTHORISATION AND CONSENT

4.2.1 PURPOSE

For digital systems to work effectively, most countries and regions have put into place a system of regulations, laws and other requirements to ensure individuals understand how their information is being used in each digital context. The purpose of these requirements is to ensure transparency of information for the individual as well as ensure greater accountability for all the organizations (both public and private enterprises) that may use personal and sensitive data to effectuate a transaction or service.

One of the most common methodologies of providing transparency and for receiving an individual's authorisation is giving an individual some sort of notice and then asking for a consent for the use set forth in the notice. There are various models of notice and consent that have been deployed by a range of systems. The most common is an explicit notice and **consent mechanism** that enables end-users to have a choice in how their data is used when they digitally interact and transact with their service providers of choice. This gives individuals the ability to feel in control of their data, to provide consent[4] to the data being shared or payments being initiated. Only with this type of user-centric design, will individuals feel the value of staying in control. This method is also a high-trust model in that it allows individuals the ability to exert specific control over their interactions and transactions in the digital economy. Another methodology that some systems are deploying is the concept of data-vaults. This method also gives an individual control over the use of their data, but it allows a more dashboard type of interaction.

4.2.2 DESIGN/REQUIREMENTS

All authorisation and consent mechanisms require clear and transparent disclosures relative to how and what information will be collected, used and shared. For the digital environment to function and to generate trust by the individuals who use the systems, transparency is key to ensuring all parties understand their responsibilities to each other. Depending upon the sensitive nature of identity and personal data and how that information is to be used, and/or how widely it will be shared or published, it is important that all parties understand the need for security of information, good data minimisation practices (collecting, using and storing only the data that is required to create and provide a given service) and that all parties disclose, either initially or upon request, all uses of data. To further achieve trust and user control, privacy and security enhancing technologies should be adopted whenever possible to minimise the exchange of personal and sensitive data in the clear, in order to provide the protections all parties require.

4.2.3 CAPABILITIES

Consent services usually rely on a dashboard or data vault that can provide users with

4 Source: "A Blueprint for Digital Identity", World Economic Forum 2016

information on what data will be used for which purposes and with which service providers. Upon enrolling in a consent service, an individual selects a series of services that they would like their data to be used for or shared with, and grants permission or consent for the use of their data for a series of transactions or services. This type of permission can be for an unlimited amount of time or contain an expiry date and it still permits the individual to set the level and type of sharing of information and the types of use. An individual can log back into the data vault or dashboard at any time to change their settings or permissions and/or select new services with which to share their data. This type of method has the benefit of eliminating the friction of repeatedly interrupting data flows to obtain consent from an individual. It also has the draw-back that individuals may not necessarily review their personal dashboards on a frequent basis to ensure they remember or completely understand the implications of their consent and the related data sharing.

4.3 PAYMENTS INTEROPERABILITY

4.3.1 PURPOSE

To facilitate seamless payments between both digital-to-digital and digital-to-physical environments, **interoperability** of **payment networks** is needed. Interoperability is a complex and multi-dimensional topic that comprises governance, technical and branding components. Governance includes the set of rules and contracts that allow the parties to participate in the clearing and settlement process (typically known as a "scheme"). Governance may be established by industry or by law. Technical components are the infrastructure by which payment (or related) messages are exchanged and the formats, networks, security protocols and mechanisms that ensure the clearing and settlement functions can execute in a risk free and timely manner. Brand recognition allows interoperability from a customer perspective. The brand communicates the qualities and purpose of the underlying service.

4.3.2 DESIGN/REQUIREMENTS

For payment interoperability to work well in a market, the following aspects should be considered:

- **Who can access the scheme**: Access to a payments scheme is often not limited to banks. Companies and third-party solution suppliers (gateway providers) may also have access, subject to the rules and structure of the scheme. Countries such as UK and Sweden provide examples of where direct corporate access is supported.

- **Level playing field and ease of access**: The cost of entry for a scheme should be fair, equitable and transparent. This includes on-boarding and ongoing participation. Smaller banks or new entrants to the industry should not face unduly high or inappropriate barriers to entry.

- **Innovation**: The design of the scheme and its infrastructure should encourage innovation. Ease of access and message standards are key. The intent should be to enable new use cases to be identified and implemented by the market independently of the underlying payment scheme(s).

- **Consumer protection**: The design of the scheme should ensure consumer protection measures, such as data protection and fraud detection are included in the initial design.

- **Batch (scheduled) versus real time (on-demand)**: There is a significant move towards real-time payment infrastructures across the world. Yet batch still has significant benefits where real-time is unnecessary, such as monthly salary payments.

- **Risk management**: Risk is a key concern for payment schemes. Mechanisms to eliminate settlement risk, manage reputational risk and to enable banks to manage credit risk all are required.

- **Substitution**: Substitution is an important factor for reducing risk and enabling customer choice. The ability to substitute one payment scheme for another (for example, having both real time and batch payments) helps mitigate the risk of technical bank or scheme failure. Substitution also enables consumer and merchant choice through ensuring multiple channels for payments.

- **Message standards**: Common open standards, now typically based on ISO 20022 help banks and other institutions streamline their systems and enable service and product development by vendors. A common message standard enables substitution.

- **Security**: Security standards directly support the integrity and contractual framework for a payment scheme. Standards should be of enough strength to combat the latest threats, and should deliver authentication, confidentiality, data integrity and non-repudiation. Non-repudiation is key to supporting the contractual and liability framework for the scheme.

4.3.3 CAPABILITIES

These considerations should lead to a design that allows services to be overlaid on top of the local clearing and settlement infrastructure. Two examples, proxy alternatives to bank account numbers and new services such as Request to Pay (RtP) demonstrate why these considerations are necessary.

Proxy based services use an alternative identifier (such as mobile number, email address or other) in place of an account number when initiating a payment. This can be helpful as it enables an alternative well known and convenient identifier to be used, keeping the bank account details secure. It also operates independently of the actual account and associated bank (in other words, the account holder can move their account to another bank, and the payments will follow so long as the single proxy/account relationship is updated). Two examples of proxy services are:

- PAYM in the UK where a central proxy database is maintained by the banks. This database associates a mobile number proxy with the bank account details. Payment to a mobile number can be requested via mobile banking apps.

- Bank Giro Numbers (BG Numbers) in Sweden. These are assigned to businesses only. They act as a proxy and are associated with the business bank account details. In this case, the BG Number remains hidden even from the paying bank and is known only to the business customer and their bank. This works particularly well for businesses with a large retail customer base (large billers), as any change in banking relationship results in the payments simply following that new relationship.

In the second example, RtP services are enabled by the ability of a Clearing and Settlement scheme to support payments in generic and end-use independent manner. In the UK, RtP has been implemented as a free-standing infrastructure using APIs to enable banks to orchestrate the RtP process. Where that process reaches a "pay conclusion" authorised by the paying customer, then the paying bank can initiate the payment across Faster Payment System (FPS).

4.4 DATA EXCHANGE

4.4.1 PURPOSE

Data exchange enables end-users to make their data available and accessible to their service providers for a set period and purpose. Data can be exchanged to allow financial planning through apps and by financial advisors, allows for easier compilation of information to file taxes or to apply for loans based on authenticated information. Data exchanges can also support payments by authenticating accounts to their owners and enabling digital identity by exposing information to authenticate an individual. The data to be exchanged can include loan details, transaction data, demographic data and asset holdings. Like the other pillars supporting the digital infrastructure, data exchanges will require technical components and governance components.

4.4.2 DESIGN/REQUIREMENTS

For Data Exchanges to function well in the context of a local digital economy, the specific purposes for which the data exchange will be applied, and the following design criteria, should be considered:

- Security requirements to ensure that the exchange of data is secure yet flexible enough to allow for implementation of the latest technology
- Privacy requirements to ensure that users are provided transparency on use of the data, consent to the transfer and use of their data, and can revoke that consent
- Technical standards to allow for interoperability so that the data transfer mechanisms built, such as APIs provide the same data of enough quality in the same format for defined use cases
- Standards for authenticating the individual or business to their accounts and data to limit fraudulent access and to limit the sharing or retention of banking credentials
- Incentives for data suppliers (e.g. financial institutions) to make data readily accessible in a timely manner since lack of incentives can create barriers to the exchange of data
- Parity of data access for individuals and small business to obtain the full economic benefit for all participants in the ecosystem
- Parity of treatment for ecosystem participants to allow for competition amongst data providers (e.g., financial institutions), data aggregators (i.e., technical intermediaries and service providers), and users of the data (such as the payment functionality provider)

4.4.3 CAPABILITIES

The capabilities to enable data exchanges include:

- APIs and similar data transfer functionality to allow for the actual exchange of data amongst the data providers, any intermediaries and the end user of the data
- Authentication capabilities to authenticate the individual and businesses to their accounts in a safe and secure manner that limits fraud
- Standards setting bodies, either led by industry or by government, to establish the aforementioned standards
- Data governance and management capabilities to transform the data provided into actionable insights for specified use cases e.g. as needed to support analyses to prevent fraud

ONE PILLAR IN DEPTH - DIGITAL IDENTITY: A FOUNDATIONAL COMPONENT OF A DIGITAL INFRASTRUCTURE

05

In order to support a digital infrastructure, there is a clear need for a verified identity that can be accepted across multiple digital touchpoints to ensure that all parties involved in an interaction can trust the other participants. Digital identity is grounded in a collection of data attributes that define the individual or organisation. This collage of data, when bound to the user, verified, and made securely accessible while under a user's control, is the essence of digital identity. Its primary purpose is not just to identify someone, but more importantly to confirm their entitlement to access a service or perform a task. For example, something that allows an adult to prove they're old enough to buy alcohol without revealing a date of birth; or allows them to rent an automobile without producing a license, or access governmental benefits or health services without the need for multiple paper forms of identification.

5.1 OPPORTUNITIES AND VALUE DRIVERS ENABLED BY DIGITAL IDENTITY

A well-organised digital identity enables the transformation of society and creates social and economic growth[5]. Key in this transformation is to put end-users in functional control of their data, digital money, and simply put, their digital life. This ensures end-users are at the centre of new value creation opportunities that will emerge in the digital economy.

Digital identity is a typical example of a two-sided market, as it serves both end-users and relying parties. End-users want to use the goods or services of the relying party; for example a merchant or government entity. Simultaneously, relying parties want to know who the end-user is and verify their access to

Figure 3: The digital identity empowers end-users and relying parties in the 'next evolution' of the digital economy

5 High levels of ID adoption could unlock economic value equivalent to 3 to 13 percent of GDP in 2030. Source: "Digital Identification, a key to inclusive growth", McKinsey, April 2019

the goods and services. A trusted third party takes the role to vouch for both the end-user and the relying party and fulfils their needs, shown below, to enable trusted interactions and transactions in the digital economy.

financial services include use cases to support end-users with access to financial products and services. Examples include an individual going through the online onboarding process for a bank account, loan or mortgage, or verifying someone's income for credit checks. Additional examples which have a higher frequency of use are authentication of payments and recurring, secure logins to the digital channels of a financial services provider.

Digital Identity can be used frequently in **education**. The digital services that are available within this area support end-users' interactions with schools and universities online. Example use cases include online applications for university, registering for courses and exams, or offering discounts for students for services or products. Tuition payments is also a major use case, where children and students are provided with educational tools, such as computers and tablets. These tools can then be returned at the end of a school year or be replaced by another set of tools when promoted to the next level of education. Linking tuition to educational tools is an example of payments being linked to identity. Education credentials, certificates, and degrees could also be attributes within an individual's digital identity.

Within the **health sector**, digital services are available to support citizens as they interact with hospitals, pharmacies, and other medical entities. Example use cases are sharing and processing of medical records, receiving medicines based on personal medical prescriptions or making medical appointments digitally.

There are many opportunities to use a digital identity in the **private sector**. For example, authenticating for online gaming and shopping, verifying age when accessing an age-restricted digital service, signing up as a taxi driver on a digital platform and registering as a host or guest on a home sharing platform.

Finally, in the **public sector**, digital services enable end-users to interact with the government online. With a digital identity, end-users could submit tax forms and pay fines digitally, and register a new address after relocation. Items such as birth and death certificates, passport issuance, driver's license and other official identity documents can be arranged online rather than in person.

A digital identity enables access to the larger digital infrastructure and provides **people with access** to broader public and private digital services across multiple sectors, which can help stimulate socio-economic growth and promote inclusion:

- Financial inclusion by providing people access to financial services (loans, credit, savings) through online enrolment
- Access to social benefits, health services, education, and more by verifying access rights and by managing people's social, medical and academic records
- Further digitisation of the economy by driving (cross-border) transactions

Verified digital identities **create trust** in a non-physical, remote context by providing certainty about one's identity. Thanks to digitisation, there are more of these interactions and consequently an increased number are susceptible to risk. Establishing trust in both the network and the related exchanges between

Providing citizens a digital identity as a basis for social-economic reach and growth

An example of **India's Aadhaar solution:**

From the start, Aadhaar, which means foundation in local language, was designed to reach even the most excluded residents of India to possess an official identity. Since 2009, the Unique Identification Authority of India (UIDAI) has enrolled over 1.2 billion people in Aadhaar with a unique identity including biometric inputs.

A major driver for the adoption of the Aadhaar Identity was the governmental need to deliver financial subsidies, benefits and services to its citizens. Although Aadhaar Identity has had challenges in its security and privacy along their journey, it currently, offers a wide variety of trusted services, from authenticating presence in educational class and proof of eligibility for benefits and services. Also, Aadhaar is extended to Financial Services as it supports banks in identifying clients to comply with KYC and AML.

Aadhaar has evolved since launch especially surrounding the Acts passed by parliament and through other legislation surrounding Data Privacy and Protection that are currently before the Indian parliament although currently held up due to the impact of COVID-19 in direct response to concerns raised surrounding the intended use of the Aadhaar solution. This is also permitting a widening of scope to other regulated entities to offer Aadhaar as an option for non-commercial authentication and KYC.

end-user and relying party, lowers transaction risks and therefore transaction costs. Digital identity mechanisms encourage sharing only the information necessary to use the service. This reassures companies that they are only receiving the data they need and promotes trust in the system.

For example, in online e-commerce payments both a consumer and a merchant can trust the exchange. Even though the merchant may not have a prior relationship with the consumer, and does not recognise the consumer's email, device, or shipping address, the digital identity network provides a level of assurance as well as clear allocation of responsibilities and liabilities. Trust in the network lowers transaction risks and therefore transaction costs. Illustratively, it enables:

- Trust in multiple parties participating in the sharing economy
- Trust across devices (phones, wearables, smart home devices, automobiles) as a forerunner to the connected society promised by the "Internet of Things" (IoT)
- Seamless travel in a trusted network of mobility and hospitality providers
- Trust in identity attributes provided by authoritative sources to streamline enrolment procedures, such as Know Your Customer (KYC)[6]

6 According to a study by The Open Identity Exchange, Digital Identities can lead to up to £10 billion savings in the UK related to inefficient KYC processes and identity fraud. Source: "Digital Identity in the UK, the costs of doing nothing", Open Identity Exchange, April 2018

Coupling payment security to identity as a global, interoperable, and trusted security method

An example of **EMVCo 3DSecure2.X:**

Within the payment space, global standards are widely adopted through global standards organisations such as EMVCo. For eCommerce authentication the most recent solution is EMVCo 3D Secure 2.X. This is a global security standard where merchants and payment issuers collaborate to prevent fraud either through enhanced data being provided (device being used for shopping, email account, etc.) Through sharing this additional information, a level of risk can be associated. If multiple facts of the data are suspect (device has not been used previously, email address does not match) the digital interaction can be chosen for a step up by the Card Issuer to challenge a cardholder for an authentication if fraud is suspected. The first version of 3D secure had a significant downside, where consumers where facing friction leading to conversion loss in the payment though the frequent use of challenges often based on passwords.

With version 2.X and above, this friction is significantly reduced as in the background all kind of data is shared allowing predictive identity checks to be undertaken without interfering the consumer checkout experience. However, if fraud is suspected then it still supports a challenge where deemed a priority. Challenges are commonly directed to mobile phone-based solutions with biometric challenges becoming more common.

EMVCo 3D Secure is an example of an interoperable solution, which support cross border traffic. Because it can be licenced from EMVCo, it is not restricted to global card schemes and works for domestic solutions as well.

To ensure people trust the system they need to be protected from misuse, and a clear regulatory framework should not only set responsibilities and liabilities. Institutions need to set up safeguards in order to enforce the framework, ensure privacy by design and protect end-users' data that resides in the eco-system. Examples are monitoring potential fraudulent transactions, safeguarding identity and data attributes, and preventing misuse of Personal Identifiable Information (PII).

A digital identity also enables end-users to **control their digital assets**. As these are owned by the end-user, explicit consent should be provided before any of these assets are transferred across parties. A transparent consent mechanism helps to drive this control. When end-users can access, consolidate and share their data with service providers of choice, they can elect those which make their lives easier.

Digital infrastructure to help individuals safely and easily share verifiable personal data with a house rental company

An example of **MyInfo** as part of **SingPass:**

'Digital to the core and serves with the heart', so reads Singapore's 2023 vision. As part of this vision, the National Digital Identity (NDI) program enables Singapore residents to transact digitally with the government and private sector. Using a digital identity called SingPass, several use cases are enabled such as onboarding of new customers, authentication of customers and digital authorization and signatures.

One recent enhancing initiative called MyInfo enables individuals and legal entities to manage the use of personal data for simpler transactions. MyInfo acts as the reliable and independent source for the purposes of verifying the customer's personal attributes. These attributes range from verified name, address, phone number, income and employment. Participating service providers who rely on MyInfo do not need to rely on additional documents or photographs to verify a customer's identity.

As example, people usually need to provide hard-copy transaction data of their balance account to a house rental organisation to prove they can pay their future rent. With MyInfo, Singaporeans can now share a verifiable claim on their income with a house rental organisation. This results in great customer experience, secure transfer and data minimisations. In the end, Singaporeans are in full control of who they have given permission, i.e. consent, to access their data. Also, MyInfo provides an overview of historical transactions and the possibility to revoke historical consent.

- This lays the foundation for moving towards a digital economy based on a level playing field for data. As such, it has the potential to become the "data equivalent of GSM", where a user at one provider can communicate with a user of another provider via the same protocol.
- This enables the exchange of an individual's data with other parties on behalf of the end-user and avoids data being locked-in at a single party. This creates a fair and equal chance of success where businesses compete on value add, rather than volume of and access to data.

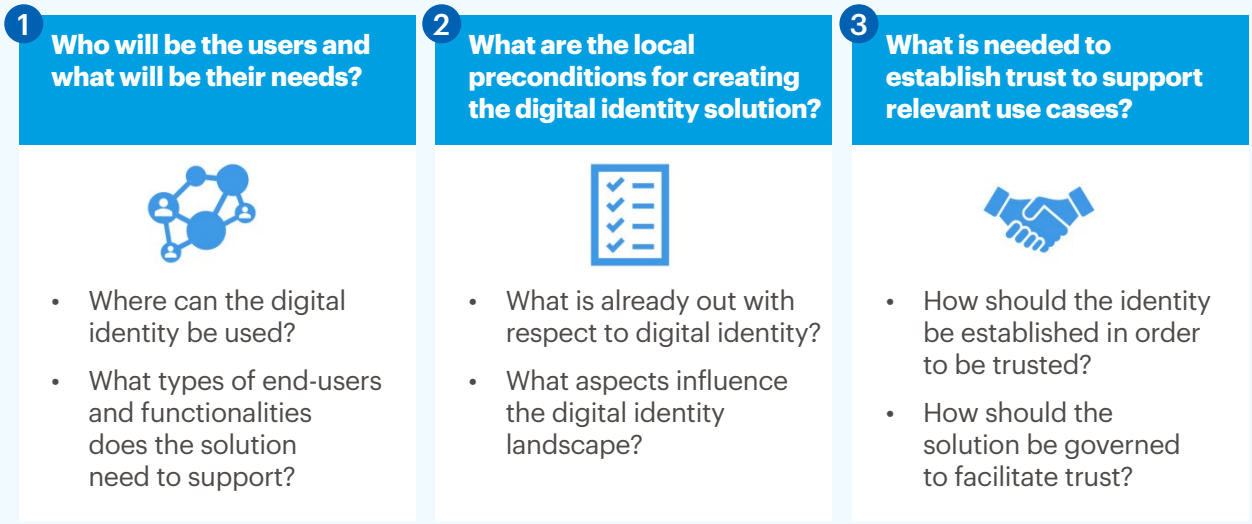
5.2 KEY QUESTIONS TO SHAPE THE DESIGN OF DIGITAL IDENTITY

Once the local need is established, three key questions need to be answered to shape the digital identity model and design the solution requirements.

Who will be the users and what will be their needs?

Each use case for digital identity has different characteristics.

Figure 4: Three key questions to ask before shaping a digital identity



Use cases vary with respect to the **end-user**. For example, opening a bank account should be possible for a wide variety of individuals who may differ due to culture, digital literacy, physical and mental abilities, linguistic backgrounds and preferences. It could also be an individual who is mandated to fill in a tax form on behalf of someone else who is unable to do so. It could be an individual that acts on behalf of a business or public institution, for example to obtain a certificate of conduct for a new employee.

The level of trust required to enable use cases can differ. Applying for a mortgage requires the mortgage provider to have a high level of trust regarding an individual's identity and corresponding attributes. Whereas a log-in to an eCommerce website involves relatively less risk and, therefore, requires less trust.

Use cases also differ in their **frequency of use of a digital identity**. For example, a log-in can happen multiple times a day per end-user, however, applying to a university is likely to happen only once or twice in a lifetime.

To meet the use case requirements, it is important to determine **where** the digital identity is needed, what **types of end-users** need to be supported and what **functionalities** need to be provided.

Where can the digital identity be used?

As stated previously, digital identity enables a wide variety of use cases, both in the public and private sector. Determining which parties will rely on a digital identity during the design phase will help ensure the solution meets their needs.

What types of end-users and functionalities does the solution need to support?

A clear decision needs to be made regarding the type of end-users involved. The first type of end-user is an individual acting on their

own behalf. Second, individuals can act on behalf of someone else. This requires a mandate structure with an appropriate legal and technological framework, such as for a person in a vulnerable group (including minors and those with disabilities), where a power of attorney may exist. Last, individuals can act on behalf of a legal entity. This results in business to business or business to government identity transactions. To enable this, there needs to be an authorisation mechanism in place where close alignment needs to be across multiple entities and registers. Creating interoperability between legal identifiers such as the 20-digit code as Legal Entity Identifier (LEI), and individual identifiers can contribute to this authorisation mechanism.

5.3 KEY ENABLERS INCLUDING TRUST AND ADDRESSING LOCAL MARKET PRE-CONDITIONS

Depending on existing capabilities and levels of trust, several roles may be fulfilled by current participants in the digital identity system. Typically, a national authority already has the statutory duty to issue and manage identity documents. This authority might be well equipped to fulfil a role in the digital identity solution, for example when acting as trusted provider to issue identity attributes. This role requires trust from both the end-user who is issued with the identity, and from the relying party, who needs to be reassured they are relying on the right data.

In some countries, mobile network operators or, for example, the postal service, have a dominant role in attribute sharing and verification, such as someone's name or address. To ensure the right level of verification, these entities may act as an identity verification provider to enable a transfer of their knowledge from the physical world into the digital world. Parties who already rely on identities in the physical world, such as customs, ministries of internal affairs, or private entities such as banks, may do so in the digital world to extend their services online.

Trust is key to ensure both end-users and relying parties will use the solution, and several factors influence this.

How should the identity be established and at what level should an end-user authenticate in order to meet the trust required at the relying party?

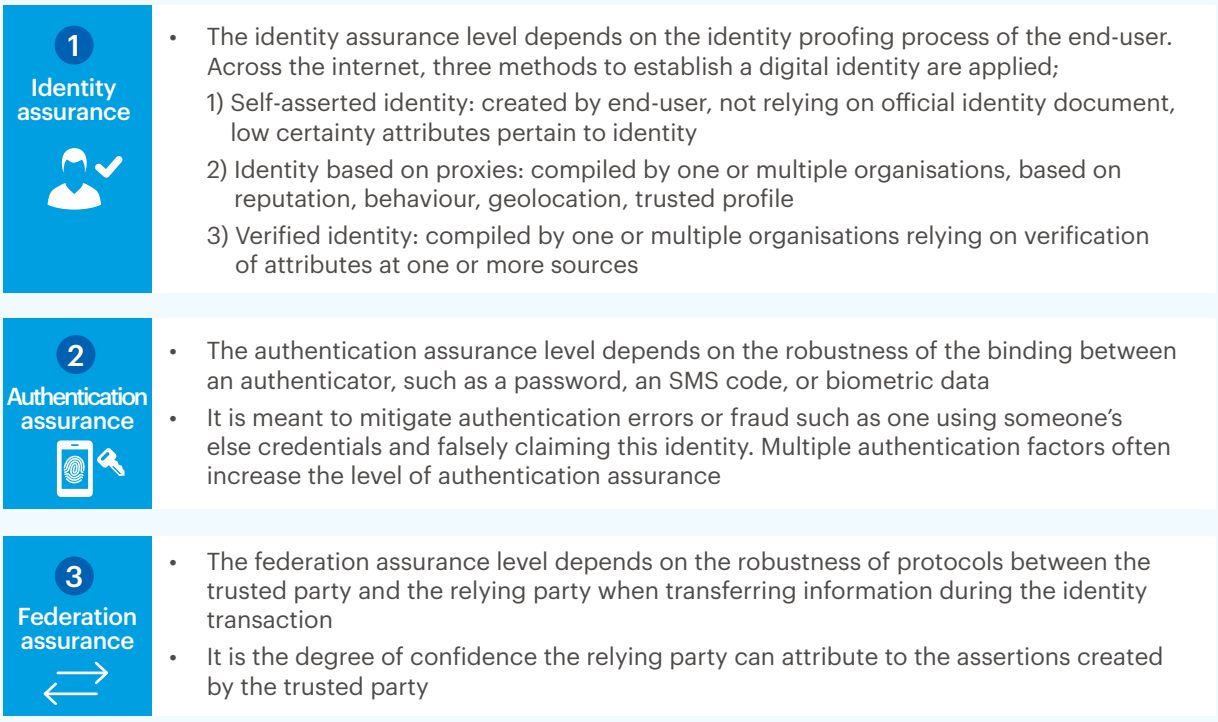
Depending on the use cases, different levels of trust are required for relying parties to accept the identity and offer a service. For example, agreeing on a mortgage contract with a bank requires a higher level of trust than performing a log-in on an e-commerce website.

Level of Assurance (LoA) plays a central role in creating this trust online. It is the ability to determine, with some level of certainty that a claim of an identity made by a person or entity is trusted to be the real identity. The LoA is described in international standards. An example of an international standard is NIST that promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life[7]. The figure below depicts a short description of the three components that determine the LoA: these are the **identity assurance**, the **authentication assurance** and the **federation assurance**.

Determining the optimal level of assurance depends on two aspects. First, it depends on the **trust level required** for the **use case**. Often, a higher level of assurance comes at the

7 According to the National Institute of Standards and Technologies. Source: National Institute of Standards, available at https://www.nist.gov

Figure 5: Three key components to create a level of assurance



cost of convenience for the end-user. When the frequency of transactions is high and there is no sensitive information involved, for example with ecommerce logins or low value payments, often a lower level of assurance is applied. When the frequency of transactions is lower and risk of sensitive information is high, such as ordering prescriptive medicines or opening a bank account, the level of assurance is higher.

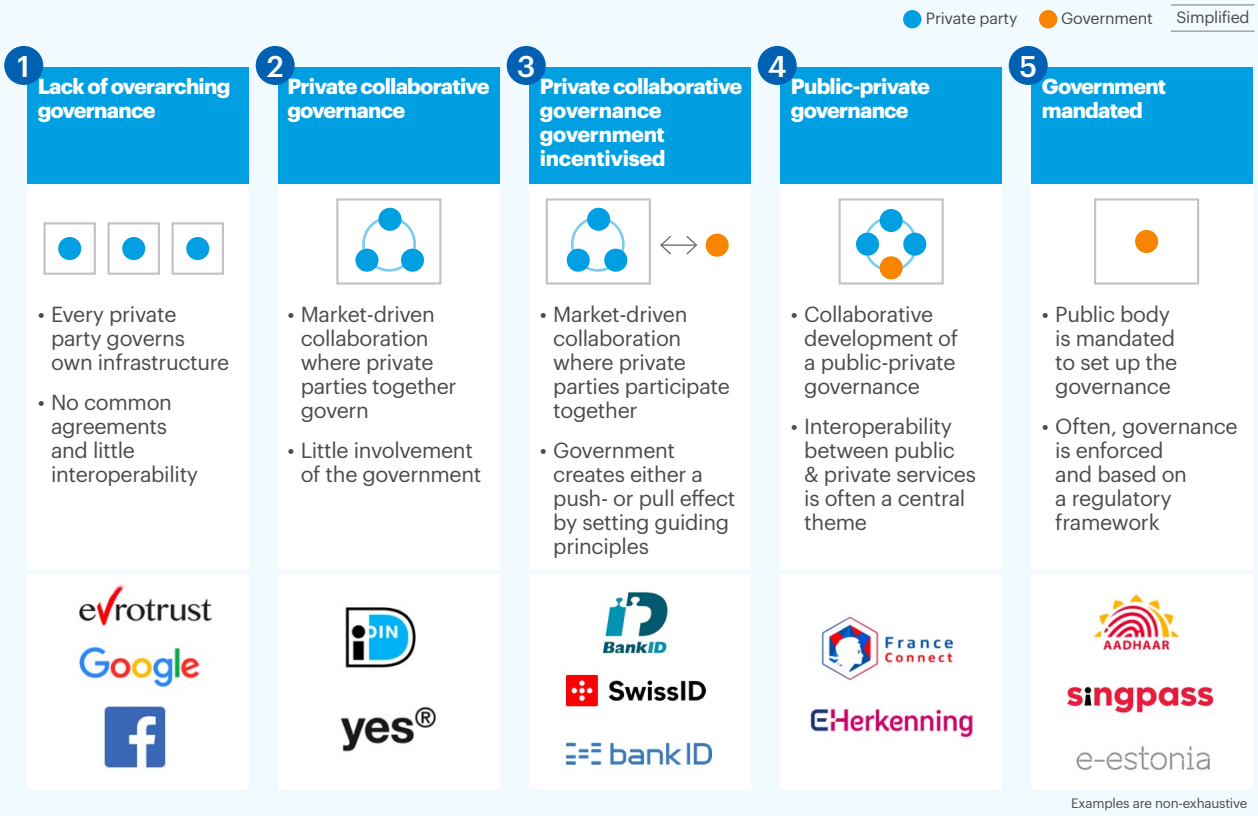
Second, are there **relevant sources** for **verification** available and accessible for the digital identity solution? For example, how many citizens own an identity to rely on? Are there official registers to verify the identity attributes? Do citizens have smart phones available which can act as a potential authenticator? Do relying parties need to invest in technology to accept the digital identity?

Local context often determines what solutions need to be supported for relying parties and end-users to facilitate the right level of trust.

How should the solution be governed to facilitate trust?

It is important to set up a solid governance framework to manage the digital identity solution. This governance consists of a (legal) entity which is assigned two tasks. First, the digital infrastructure, its design and standards need to be shaped in order to ensure all relevant stakeholders benefit in the right way with clear allocation of responsibilities and liabilities. Legal, technological, and business matters need to be addressed - such as data responsibility principles, data minimisation, data transparency, privacy considerations,

Figure 6: Optimal governance model depends on country context



security standards, and compensation models to help create trust across stakeholders. Second, this infrastructure, the design and standards need to be enforced and kept up to date. This is a continuous process which requires a permanent governance body to be in place. In practice we see five different models applied today with each having their own pro's and con's.

The optimal governance model depends on the country-level dynamics and is affected by several things. First, what other design choices are key, for example what identity registers are already available in the country and who is the owner of this register? If available, what parties have access to the national registers? Second, what does the country want to achieve with the digital infrastructure, is it only meant for public sector services or also used for private sector services? Third, what legislation currently applies in the country? Is this actively driven centrally by the regulator or are standards and rules more market-driven? Fourth, what are historical and cultural characteristics of the country? Beyond these four examples, there are many other contextual characteristics that determine the optimal local governance approach.

What technological design choices can contribute to the trust and acceptance?

After the governance body is established, several key technological design choices need to be discussed. Technological components can be really detailed, and it is beyond the

Example of two digital identity solutions – **eEstonia** and **BankID Sweden**

e-estonia

Estonia is one of the leading countries that launched a digital identity – almost two decades ago. Today, over 98% of the Estonians (1.3mio) currently have been issued a physical card which they can also use for authentication, data storage and sharing, and digital signatures, through its chip-based cards or using their mobile phone.

The model is built on a common data exchange layer, called X-Road. It enables citizens to log-in with their identity, provide consent and share attributes with governmental service through the online State Portal. Via this State Portal, citizens can see what entities have accessed their data, when this was accessed. They can provide consent and withdrawal for each data transaction enabling them to be fully in control.

The platform solution works cross-sectoral, enabling citizens to have a single identity for many areas, ranging from using it as a national health insurance card, logging into bank accounts online, online voting, checking medical records, and filling taxes.

BankID

The Nordics, too, have rather mature digital identity systems in place. The public sector issued digital identity methods many years ago. In addition, successful private sector solutions, mainly driven by financial institutions, are deployed in Scandinavia. Sweden, for example, has successfully implemented a digital identity model that works as a trust framework, owned by a coalition of banks. Over 80% of the Swedish population (8.2 million) has a digital identity and use BankID on a regular basis for a wide variety of private and public services, such as opening a bank account, declare taxes and sign digital contracts. In 2019, BankID Sweden processed more than four billion transactions for bank authentication, government log-in, verification and digital signing.

scope of this paper to address all of them. It is important to mention that no silver bullet exists for digital identity which means that there is no right or wrong answer to what technological components work best. Elements to consider are, amongst others, what type of identification and authentication is supported? How is the data stored? How is the connection established with all parties? How is the data protected and kept secure both during transacting and at rest?

Local interpretation of these details is required to find the optimal solution from a trust, cost, flexibility, and security perspective. Involving

relevant private and public stakeholders in this design process can help create a good product-market fit and steer towards a coherent and harmonised solution.

5.4 HOW TO LAUNCH – KEY FACTORS TO IMPROVE ADOPTION

A key factor of driving growth in transaction volume within the digital infrastructure is the creation of reach. To end-users, a digital identity is only relevant when it can be widely used at relevant relying parties of the services. To relying parties, investing in building applications on top of this digital infrastructure is only relevant when end-users are already using these services. The interoperability domain ensures that reach is optimised for each end-user and relying parties, thus optimising the potential for transaction volume growth.

This is an example of an indeterminable problem, where in the beginning there is little relevance for any party. At a certain level of adoption, a tipping point will be achieved. This is the critical mass of end-users and relying parties that ensure that end-user's primary choice will be the use of applications on top of the infrastructure.

Predicting the tipping point upfront is very complicated and depends on many variables, but certain actions can help increase the pace of adoption and reach the tipping point sooner.

1. Collaboration and commitment

It is important to shape the design of a digital identity while considering the needs of all relevant stakeholders. This collaboration ensures aspects such as interoperability and trust are safeguarded as the foundation of the infrastructure. Interoperability and trust safeguards can also apply to competing solutions. A governing body representing opinions and views of all involved parties can help support this collaborative effort.

2. Government endorsement

Service ubiquity is important in stimulating adoption. As a significant share of digital transactions lie within the government domain, government services can endorse and stimulate adoption across individuals and businesses. Renewing a driving license or filling tax forms are examples of government services that reach a large share of the population.

Adoption learnings from other digital identity solutions

In many European countries, government use cases are one of the main drivers for transaction volume of digital identity services. For example;

- the Dutch Government Identity service (DigID) was doing 308 million transactions with 13.7 million users (80% of total population) in 2018.
- under the Belgian identity service 'Itsme', on average a user has 3.3 digital identity transactions per month with the government
- in total about 14% of all transactions under BankID Sweden (expected to be ≈400 million in 2019) are with governmental service providers. Usage of BankID for filling out tax returns was a key adoption trigger for adoption by end-users as early as 2004

3. Trust in the identity

End-users and service providers need to trust the design of the digital identity. By creating a widely recognisable acceptance brand from the start, the existing trust in well-known brands of involved parties can be leveraged to kickstart a trusted brand. From this starting point, developing the new acceptance brand will increase recognisability of and trust in the digital infrastructure.

4. Standardisation

A common language that all service providers can understand and interpret is vital to supporting the creation and sustained development of a digital economy. Governance of the digital identity should be dynamic to allow for improvement in rules and standardisation over time. Identity, data, and payment schemes have shown they continuously evolve and respond to changing needs of users. Further standardisation of the infrastructure will improve understanding, usability and connectivity, all of which will drive adoption. Use of open standards will also prevent the risks of vendor or technology lock-in, examples are OpenID connect and OAuth in identity.

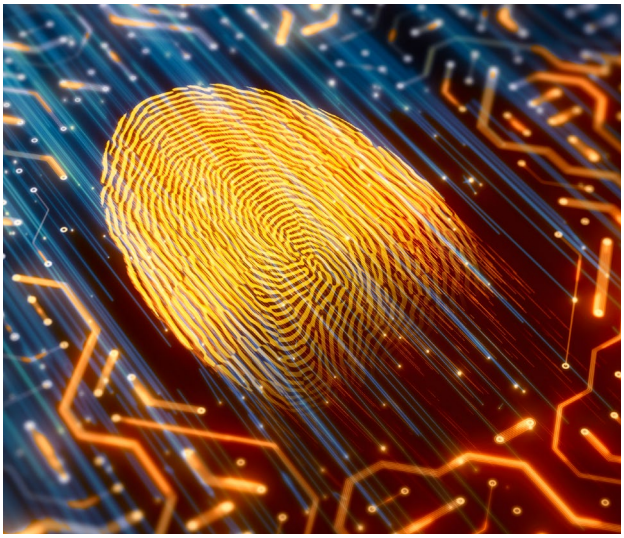
5. Involvement of the private sector

The private sector can play a role in the implementation of the digital identity. For many markets, money and motivation to develop an appropriate infrastructure should be provided by the private sector in consultation with the right public sector partnership. Participants should be aware of possible slow uptake of services in the digital identity. Adoption of the digital identity is an exponential process, which starts slowly and grows due to the increase in functionalities and applications. It is important to create reasonable estimates in transaction volumes and private sector involvement in order to build a viable business case, also for non-monetary value.

6. Transparent communication

As with every innovation, developing an identity solution will cause friction from involved parties. Clear communication, including a "hearts and minds" sell to end-users can change attitudes from resistance to a demand for speedy acceptance. To facilitate trust, communication goes beyond explaining the benefits. It should also cover key concerns such as – *Where is my data stored? How is this protected? What data is exactly stored? How will and can it be used for and where can it not be used for? Is there also a legislation underpinning these questions? How is this legislation enforced?* – transparent communication to citizens is crucial in creating trust.

The next chapter will review four case studies from countries that are currently undertaking efforts to establish a digital infrastructure, with digital identity as a core component.



BETTER UNDERSTANDING DIGITAL IDENTITY IN AFRICA & ASIA: 4 CASE STUDIES

06

During the 2019 Afro-Asia FinTech Festival, delegates from many countries were brought together by the Monetary Authority of Singapore (MAS) to talk about the need for a digital infrastructure to support their digital economy. Two findings resulted from that meeting - first, countries differ in opportunity size for a digital infrastructure, and second, countries differ in their execution timing.

Some countries recognised the high urgency for, and high value of, a digital infrastructure, having just started to shape their roadmaps. This enabled a great opportunity for further engagement to explore their approach to digital infrastructures and digital identity.

In recent months, interviews have been conducted with representatives of four specific countries to better understand their vision, ambition, where they are in their journey, and how to move forward both individually and potentially as a community.

6.1 KEY INSIGHTS FROM THE CASE STUDIES

By looking at this select number of countries at different stages of design, development and roll-out of their digital identity solution, the following key insights have been identified:

1. Governments shape a broad vision on the benefits of a digital infrastructure, but face challenges in taking a holistic approach on execution

All four countries recognise the major benefits of having a full digital infrastructure in place, linking payments to identity and having consent and data exchange mechanisms.

While implementing this vision, some countries are starting to initiate programs in one or two component domains (e.g. digital identity or payments), but these programs are sometimes run in isolation and lack a governance body that harmonises and oversees the broader roadmap. Therefore, synergies across the component domains are left unexploited. A notable paradox is that countries see major benefits in one federated, single solution, but in pursuing this, find themselves challenged in coordinating and harmonising different stakeholders.

2. Government bodies take a leading role in initiating the digital infrastructure and digital identity, mostly driven by the ministry already responsible for the national identity program

In many countries the Ministry of Interior is leading the development of a digital identity as a natural extension of their national identity. In some cases, the ministry has already started rolling out digital identity though the basis of a reliable identity register is not yet fully in place or lacks end-user reach. As a result, identity inclusion and insufficient levels of assurance prevent advanced use cases such as eKYC. Having a so-called 'golden-source' in place with verified identities would provide a solid base for further development of a digital identity.

3. Technology is only one part of the puzzle - balancing local regulatory, technology, and business requirements is important for a holistic, networked solution

When initiating a digital infrastructure, countries invest time and resources to increase their knowledge of global initiatives, intending to rely on established best-practices elsewhere.

Figure 11: Country statistics

	GHANA	KENYA	CAMBODIA	BRUNEI
Digital Identity Status	Rolled out physical Ghana Card, which provides foundation for a digital identity for public and financial services	Introduced the National Integrated Identity Management System (NIIMS)(popularly referred to as the Huduma Namba)	Started to investigate building a digital infrastructure with digital identity at the core to let end-user share data across ministries	Started to launch a single portal to access a wide variety of services in order to digitally transform their country
General				
Population (million)	**30**	**47.6**	**16**	**0.46**
Population 16-65	**82%**	**55%**	**66%**	**75%**
GDP (billion)	**$67**	**$96**	**$27**	**$13.8**
Connectivity				
Smartphone (share of pop.)	**29%**	**34%**	**65%**	**88%**
Cellular network coverage	**87%**	**117%**	**91.5%**	**95%**
Bank account (share of pop.)	**42%**	**30%**	**40%**	**80.5%**
Digital banking services (share of pop.)	**49%**	**79%**	**32%**	**71.0%**
Identity infrastructure				
Official ID document	**National ID** **Passport** **Birth Certificate**	**National ID** **Passport** **Driver's license** **Birth Certificate**	**National ID** **Passport** **Birth Certificate** **Family book** **Residence record**	**National ID** **Passport** **Birth Certificate**
eID present	**Yes, Ghana Card**	**Yes, Huduma Namba**	**Yes, CamDigiKey**	**Yes, e-Darussalam**

Leading solutions were often referenced during country interviews – such as X-Road and e-Estonia in Estonia, Indian Stack and Aadhaar in India, SingPass and MyInfo in Singapore, and government identity models from China. In the selected countries, some technology is already being implemented. However, technology requirements are only one of several elements to consider. As indicated by the interviewed countries, local implementation is a major challenge. Harmonisation and coordination across departments is difficult to oversee. A solid regulatory framework should also be in place before the technology element is deployed locally. In the studied countries, the regulatory frameworks were often not mature, resulting in data privacy and data protection concerns. Lastly, local needs, execution experience, knowledge and physical infrastructure differs significantly making it hard to adopt roadmaps of mature solutions.

4. To ensure adoption, countries are mainly working on establishing end-user trust in their solution

To ensure adoption of a digital identity solution requires trust from both end-users and relying parties. From the end-user perspective, policy makers seek to advance trust in the digital identity solution by educating and communicating the advantages of the digital identity to citizens. From the relying party perspective, applying the digital identity often starts with government departments. Connecting private parties to the solution is in most cases assumed, but this is typically a longer-term ambition. Nevertheless, there is strong interest from regulated private parties such as banks and MNOs to adopt the digital identity solution to enable compliance with resource-intensive KYC regulation. By connecting private parties to the solution, end-user adoption will be stimulated.

This paper will now move on to consider four country case studies. It's important to note that each of these countries has a different starting point, as well as many context-specific influences, so comparisons between them should be avoided.

6.2 CASE STUDY - DIGITAL IDENTITY IN BRUNEI

1. What is the digital identity opportunity and objective?

The government of Brunei Darussalam (hereinafter referred to as Brunei) has recognised the need to digitise government services and sees a national digital identity as being a key part of this transformation, especially in terms of providing security and convenience to its citizens. The government would like to continue apace with ongoing technological advancement, particularly in building a national digital identity that provides assurance and security for online transactions. Being a small country, Brunei can aim to develop a harmonised digital identity solution to avoid fragmentation of systems or siloed solutions at various levels. This includes government ministries and institutions that provide access of services requiring the use of digital identity to all public and private sectors.

2. What is the local demand for digital identity use cases?

A national database containing everyone's digital identities will improve the efficiency of government services and benefit the residents of Brunei. However, digital identity for Brunei is not the end goal, it's really a vehicle to help people and businesses access what they want to access (e.g. open a bank account). It also has the potential to re-shape customer experiences via the adoption of principles that enable, for example the collection, use and sharing of payment data and other personal information.

Currently, most government departments are managing their own identification

BRUNEI STATISTICS

General:

Population:	**0.46 million**
Population 16-65:	**75% population**
GDP:	**$13.8 billion**

Connectivity:

Smartphone:	**88% population**
Cellular network coverage:	**95% country**
Bank account:	**80.5% population**
Digital banking services:	**71.0% population**

Identity infrastructure:

Official ID documents:	✓ **National ID** ✓ **Passport** ✓ **Birth Certificate**
eID present:	**Yes, e-Darussalam**

systems through various projects. Examples of explored use cases include the possibility of using facial recognition to track students' attendance by the Ministry of Education, and the development of an AI-driven tracking app by the Ministry of Health for the purpose of contact tracing during the COVID-19 pandemic. While each of these initiatives may create their own digital identity solution, it is hoped that they will pave the way for a collaboration between ministries that drives towards a national digital identity solution.

There is a known need to, rightfully, be aware of particularly sensitive data like that in education and health and at present, Brunei lacks the appropriate data protection and privacy legislation. The regulator is keenly aware that data is a sensitive issue and is currently in consultation to develop the necessary legislations and regulations. Ministries too are asking for guidance on data use, not least for cross department sharing of information. It is hoped that legislation will be in place within the next 12-24 months.

From a service perspective, the government aims to create a single portal for residents to access and view information such as pensions and health records, and for example, to make tax payments. For financial services, in the long term, eKYC should rely on the national digital identity to reduce fraud and identity theft and enable a secure digital signature. For residents, it is important that their digital identity is secure and can be trusted. The consumer's privacy, security and protection must be top of mind as the digital identity is developed, and whilst education can help address fears and a lack of understanding of how it all works, the final implementation of the ongoing data protection legislation that is being drafted will help to address this challenge. At the moment, the long-term plan is to create a secure and safe digital identity platform, in which users have control over how their identity data can be managed (following the Estonian model), and then to explore many of the more innovative potentials of a robust digital identity platform.

3. What and who needs to be supported with the digital identity?

Whilst the creation of a universal government portal accessed using a single digital identity is a large undertaking, the need to put citizens in control of their identity data is also something that needs to be addressed. As such, public awareness and education is crucial. There are challenges around resource and technical expertise and therefore, external assistance may be required to realise the plan.

Once created, a digital identity could be used at several ministries. The development of this digital identity and associated database is still in its infancy, although the existing e-Darussalam government services platform provides a solid foundation. However, there is still a need to create a clear roadmap towards digital identity which reflects and protects Bruneian society, its citizens, and its values.

4. What are local preconditions for digital identity?

There are several preconditions in place in Brunei. The e-Darussalam platform provides a starting point for a national digital identity or government gateway. The use of digital payments and banking platforms are also increasing in Brunei, and moves are being made by the Autoriti Monetari Brunei Darussalam to support the creation of a digital payments hub that would allow seamless

interoperability across all digital payments. It aims to launch in 2021. With a national digital identity solution in place, this would have wider uses, especially in processing applications for financial services.

Related to the use of data and cross-border data sharing, appropriate legislation should be in place. Brunei is already consulting on the development of a data protection and data privacy framework as part of the enabling environment for their digital identity.

Both the government and the financial sector are adopting more digitisation of services for the public for better efficiency and productivity. Continuous engagement with respective counterparts in other countries can help to expedite the process by adopting best practices.

5. What is needed to facilitate trust in a digital identity?

Currently, there are legislative gaps regarding data protection and data privacy which the regulator (AITI) is aware of. These are being addressed and should be resolved in the next 12-24 months and the impact of this on the launch of a digital identity is currently being reviewed. This approach will help to ensure the trust of the end user. The authorities recognise that different levels of security may be required for the use of a national digital identity depending on what it will be used for. This ranges from a simple log-in to extend a driver's licence at the Land Transport Department, to accessing confidential personal health records at the Ministry of Health. Brunei is aware of the potential issues of creating a centralised database - and therefore only want to capture 'non-sensitive' information that would be used when individuals apply for a service - information that people would normally be sharing with/through a government agency.

Ultimately it is the user who would be able to provide consent, or deny access to it. Residents need to have high level of trust that there will be no misuse of their personal data. Therefore, the government must be extra vigilant in gaining that trust and be accountable in safeguarding people's personal data when creating a national digital identity.

6. What does Brunei's digital identity roadmap look like?

Brunei established the Digital Economy Council in March 2019 with the objective of facilitating policies to guide Brunei in its drive towards a "Smart Nation". The draft Digital Economy Masterplan is a living document at time of writing, and some of its priority projects include digital identity and digital payments. A digital payments hub is in pipeline, and aims to enable interoperable, seamless payments so users can interact with other users regardless of their financial / payment provider and mobile provider. With stakeholder engagement from both government ministries and the private sector, this platform could accelerate the development of the retail payment network, further pushing Brunei towards digital payments and transactions. And importantly, from a consumer point of view, a government platform is seen to be more trustworthy.

Brunei is also studying solutions in other countries, ranging from China to Singapore (SingPass, NETS) and Estonia (e-Estonia, X-road). It's apparent that the government is committed to adopting cashless alternatives,

and a robust, secure digital identity that will be seamlessly integrated into everyday life. As well as enabling a more inclusive society with online accessibility available for all, this will be accompanied by an educational program focused on the benefits of living in a digital world. As Brunei plans its digital identity solution, creating a clear vision and developing the necessary functionalities to successfully underpin it will be key.

6.3 CASE STUDY - DIGITAL IDENTITY IN CAMBODIA

1. What is the digital identity opportunity and objective?

The need to establish a digital identity solution in Cambodia is driven by plans to digitise both the government and the broader economy. Although there is yet no formal top down national plans for the establishment of a digital identity in Cambodia, several key objectives are already clear. The first, to enable digital government service delivery, is perhaps the most critical as it is viewed as a key driver for economic growth. Other objectives include improving social and financial inclusion and participation, stimulating growth in e-commerce as a result of more secure, and more convenient digital transactions and payments, improved security and law enforcement, and finally, enhanced collection of taxes.

Aside from providing the infrastructure for a range of public and private services, a digital identity will, in the longer term, contribute to KYC ('know your customer') capabilities for banks to combat money laundering and financing for terrorism.

2. What is the local demand for digital identity use cases?

Aside from those mentioned above, a key objective for Cambodia is establishing a payment gateway. Currently, the access and use of digital financial services is gradually accelerating due to the high level of mobile phones with internet access (doubling of e-wallet and bank account based money transfers from 2018-2019 and a growth in share of money transfer amount to GDP from 97.7% in 2018 to 213.2% in 2019). However,

CAMBODIA STATISTICS

General:

Population:	**16 million**
Population 16-65:	**66% population**
GDP:	**$27 billion**

Connectivity:

Smartphone:	**65% population**
Cellular network coverage:	**91.5% urban (70% rural)**
Bank account:	**40% population**
eWallet services:	**32% population**

Identity infrastructure:

Official ID documents:	✓ **National ID** ✓ **Passport** ✓ **Birth Certificate** ✓ **Family Book** ✓ **Residence record**
eID present:	**Yes, CamDigiKey**

increasing comfort and confidence for payments is expected to take time and will also require further development of services offered to Cambodian citizens. So far, several emerging Cambodian fin-, insure and Agri-techs such as Wing, PayGo, TrueMoney and BIMA have started to offer such digital services. As providers develop these services, it is important to ensure they are underpinned by a strong data governance framework that puts consumers in control of their data and that they adopt principles to encourage responsible innovation and inclusive growth. Payment data is considered as personal information under privacy laws in many jurisdictions across the world and beyond legal compliance, it is critical to place the individual's confidence and trust at the centre of the services being provided.

Banks and the private sector are also aiming for faster registration processes using smartphones. As well as individuals, a digital identity will support SMEs in improved access to funding and stimulating economic growth.

In the private sector, use cases focus on support in e-commerce to be more secure, reliant and convenient.

3. What and who needs to be supported with the digital identity?

Cambodia is at the start of creating a digital infrastructure and has researched major global digital identity and infrastructure initiatives, such as the open-source Estonian X-Road model. As a result, CamDX, a data exchange layer was introduced in Cambodia and a government service for online business registration running on CamDX was launched recently with support from the Ministry of Economy and Finance. With support from the Ministry of Economy and Finance and the Central Bank, a government first approach is being taken, with the intent to provide the gateway and underpinning building blocks for all citizens. It will enable individuals as well as business owners a single sign on connectivity to access government services, both at a

national and local level. At present, Cambodia is in the process of establishing appropriate governance of this infrastructure to ensure proper guidance and control.

4. What are local preconditions for digital identity?

Cambodia has limited preconditions for establishing a digital identity and is very much at the beginning of its digital identity journey. The government recognises the need to establish the wider legal, regulatory and governance frameworks to enable a digital infrastructure. While e-commerce legislation already exists including those for the use of digital signatures, there is no existing data protection and data privacy legislation. The Ministry of Interior is considering establishing a National Steering Committee to tackle this, and other digital identity topics in consultation with a wider stakeholder group. This is viewed as an essential step to underpin subsequent engagement and enrolment of citizens, including the ability to demonstrate the benefits and understanding of citizen needs and priorities which may differ from those of the government.

Cambodia would like to create a digital identity that is scalable across services (e.g. government, financial services, health) and ensuring local preconditions support the development of a digital identity across all sectors is important.

5. What is needed to facilitate trust in the digital identity?

The government plans to establish a shared interoperable platform as the single source of truth, through which government services can be accessed. Currently, there is a national identity database hosted by the Ministry of Interior. Cambodia is developing a CamDigiKey app, which will provide consumer access to the platform through mobile devices with a digital identity stored on a secure enclave of the Trusted Execution Environment of the Mobile Operating System. The intention of this design is to engender trust in the system and avoid any unintended data access or misuse. This platform should also incorporate globally recognised regulatory and privacy standards to underpin the communication strategy that is proposed to generate trust and assurance in the system – all of which will encourage adoption by the public.

6. What does Cambodia's digital identity roadmap look like?

11 million Cambodians (68% of population) have already been issued with a National Identity. This provides the foundation for the early stages of deployment of a digital identity and the development of a full digital infrastructure.

As next steps, Cambodia needs to establish an open and interoperable digital platform that allows wider participation. To build trust and promote public adoption, there needs to be in place appropriate legal, regulatory and governance structure and communication strategy on privacy and the functionalities of an established digital platform. It is also important to consider adopting regional and global standards to enable cross-border interoperability.

While there is good understanding of the qualitative benefits of a digital identity solution, a comprehensive cost-benefit analysis has not yet been undertaken and would be helpful to provide the priority funding and support to successfully deploy digital identity in Cambodia.

6.4 CASE STUDY - DIGITAL IDENTITY IN GHANA

1. What is the digital identity opportunity and objective?

One of the goals of the Ghanaian Government, as part of its digitisation agenda is to have a national identification system (National Identity Card) which uniquely identifies individuals using biometric features and can be used for verification and authentication purposes. The Ghana Card is issued to three (3) categories of persons: all Ghanaian citizens by birth, registration or naturalisation; all Ghanaians living abroad as well as foreign nationals legally or permanently resident in Ghana. As the foundation for creating a national identification, Ghana is introducing the Ghana Card, a national identity card which includes biometric attributes.

The primary drivers that underpin the efforts to develop a national identification are social, political and economic in nature. First and foremost, it would empower citizens and support social inclusivity and engagement. Ghana strives towards providing all citizens with a national identity, in line with the UN development goals. Second, it will provide citizens convenient and universal access to government services and it will underpin secure economic transactions in both consumer and business environments. Last, from a government and business perspective, it provides accurate population statistics, formalises the economy, drives down crime through better identification, drives up financial inclusion by providing a means to prove identity to financial service providers, and enables better cross-border cooperation.

In the longer term, Ghana envisions a full digital infrastructure with the Ghana Card as

GHANA STATISTICS

General:

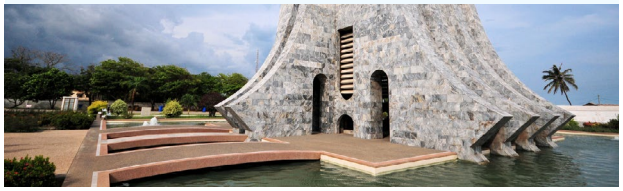
Population:	**30 million**
Population 16-65:	**82% population**
GDP:	**$67 billion**

Connectivity:

Smartphone:	**29% population**
Cellular network coverage:	**87% country**
Bank account:	**42% population**
Digital banking services:	**49% population**

Identity infrastructure:

Official ID documents:	✓ **National ID** ✓ **Passport** ✓ **Diver's license** ✓ **Voter's ID** ✓ **National Health ID**
eID present:	**Yes, Ghana Card**



the core national national identification. It will facilitate the delivery of digitised government services (including payments), alongside eKYC capabilities for banks and e-money issuers (EMIs). It also creates opportunities for further digitalisation including development of new use cases and innovation.

2. What is the local demand for national identification use cases?

Initial use cases for national identification are focused on the delivery of government services and providing citizens access to them. Already in place is the ability to apply for a passport without being physically present using the Ghana Card. Ghana wants to create a reliable system to reach all people for establishing social benefits, voting registrations and collecting taxes. Currently, services from the ministries and government agencies for Social Security, Foreign Affairs, and Health are being prioritised for implementation.

Specific sectors are also looking at how to leverage a national identification. The cocoa industry is using a digital platform to pay cocoa farmers through mobile money such that registered farmers who have wallets are paid through that channel but not through the Ghana Card. The banking sector, MNOs and local FinTechs are planning to use the Ghana Card to counter fraud and money laundering through eKYC and AML initiatives, facilitating digital payments services, and to improve account opening procedures. In future, they will also be able to adopt third party services that help with budgeting, financial planning and more, with less technical and financial know-how, helping to narrow the financial literacy gap. These services will be able to easily digest data and increase access to financial insights for consumers, while allowing them to conduct transactions in a more secure and user-friendly way.

Although the Data Protection Commission have established a regulatory framework, these providers can further improve consumer trust by ensuring that personal data is handled in an ethical and fair manner and by embedding security and privacy in their data practices Maintaining integrity, security and privacy of the data throughout the process is a matter of primary importance.

3. What and who needs to be supported with the national identification?

The Ghana Card can contribute to the creation of a national identification in Ghana. It currently provides a physical infrastructure with appropriate scanning equipment for biometric verification. Once a digital infrastructure with the right authentication means are in place, i.e. a card reader or a smartphone application, the Ghana Card can also be used as a national identification. Currently, Ghana focuses on provisioning a national identification to individuals in order to fulfil said use cases.

Ghana is also engaging with partner countries in the Economic Community of West-African States (ECOWAS) to ensure local identity standards are developed which would facilitate regional interoperability. As a start, a pilot is currently running enabling Gambians to use their card in Ghana.

4. What are local preconditions for national identification?

The ambition to create a unified national national identification is core to the Ghana Digital Roadmap. The NIA is working with a private sector technology partner to deliver the Ghana Card to ensure and oversee security, privacy and accuracy regarding data collection and deployed technologies. Much of the registration and roll-out processes have been

conducted in full compliance with the Data Protection Act, 2012 (Act 843) as amended. From an adoption perspective, there has been some evidence of public support for the Ghana Card, with queues forming at registration, and a sense of unity around the Ghana Card itself.

5. What is needed to facilitate trust in the national identification?

Security and transparency are at the heart of a sustainable national identification to ensure people trust the system and are protected from its misuse. Ensuring consumers have adequate information to understand how the national identification works, and how their information will be protected, is critical to engendering consumer trust and confidence. The Data Protection Commission exists to ensure consumer rights to data privacy, but stronger regulatory frameworks are needed to ensure strict adherence to privacy principles. Clear rules and standards will reduce organisational risk and enhance consumer trust and confidence. A national identification has the potential to usher in an era of improved customer experiences, open ecosystems and expanded value propositions but it's important that there are very clear customer communications to explain the benefits of the new services from those service providers.

6. What does Ghana's National identification roadmap look like?

Ghana's digital roadmap starts with full enrolment of all citizens into the national identity database as many Ghanaian citizens depend on the delivery of, and access to, critical government services. NIA was aiming for the registration of all citizens by 2020. It did not happen due to the pandemic, but as of now, 15 million people have been registered. In the next phase, the Ghana Card can be used to create a national identification. Some actions needed to achieve a national identification include:

- Greater collaboration across government and private sectors in developing strong citizen-centric services
- Defining and putting in place the appropriate governance structure and enhanced data privacy regulation
- Ongoing consultation with citizens and local populations on registration and uses of identity data, including monitoring uses of the Ghana Card in practice
- Sandboxing and testing of APIs for connected services
- Collaboration with the financial sector in order to counter fraud and money laundering
- Improving payment processes for government services

While much is still to be done and the complexities of identity may still provide some unexpected challenges, Ghana has come a long way in its effort to provide its population with a secure and strong national identity, which lays the foundation for a national identification in the future.

6.5 CASE STUDY - DIGITAL IDENTITY IN KENYA

1. What is the digital identity opportunity and objective?

Kenyans understand acutely both the need for strong, widely issued and widely recognized National Identity (ID) Card, as well as the potential abuses of identity systems. The current identity landscape in Kenya is seen as adequately covering the population, with a minority group subjected to delays in the acquisition of the ID card. This largely applies to communities living along the border whose application for ID documents requires additional scrutiny to ascertain their Kenyan nationality status. According to the Ministry of Interior and Co-ordination of National Government, the objective of introducing the new ID card system is to respond to emerging problems such as forgery, fraud, slow, manual and labour intensive processes in the issuance of the second generation identity cards.[8]

That said, various surveys have shown that:

- Only 9% of Kenyans lack a formal legal identity.
- 14% of Kenyans lack a formal account due to lack of an identity document.
- The gender gap between adult women and men without national identity has significantly reduced, with 11.2% of women and 6.7% of men lacking a national identity card.

With the introduction of the National Integrated Identity Management System (NIIMS) in 2019 (popularly referred to as the Huduma Namba), Kenya took concrete steps toward the creation of a master population database, which will

KENYA STATISTICS

General:

Population:	**47.6 million**
Population 16-65:	**55% population**
GDP:	**$96 billion**

Connectivity:

Smartphone:	**34% population**
Cellular network coverage:	**117%**
Bank account:	**30% population**
Digital banking services:	**79% population**

Identity infrastructure:

Official ID documents:	✓ **National ID** ✓ **Passport** ✓ **Driver's license** ✓ **Birth Certificate**
eID present:	**Yes, Huduma Namba**

8 https://www.immigration.go.ke/national-registration-bureau/

act as a single source of truth and contain information of all Kenyan citizens and foreign nationals residing in Kenya and will serve as a reference point for ease of service delivery to the people of Kenya.[9]

The focus is now on extending the array of public services available through this system supported by a legal framework and data protection for users. The eCitizen and e-Government platforms where Kenyans are able to access and pay for a variety of government services have been operating since 2014. The main issues going forward regarding improvements to the eCitizen portal include: expanding the array of public services available on the platform, enhancing the legal framework for oversight of the system, integrating data protection for users.

The Huduma Namba allows for more effective allocation of resources, streamlines government service delivery and business processes, and enables citizens to use a single ID in multiple different contexts, saving on the costly and difficult process of obtaining reliable and unique identifiers to access sometimes vital services. Access to private sector services such as banking and mobile telecommunications services could also be made much easier and faster as the Huduma Namba gains critical mass, and user traction. In fact, a broader, fully digitised Huduma Namba, is seen as a key component in the wider digitisation of the government and the Kenyan economy.

2. What is the local demand for digital identity use cases?

Aside from a need to access government services and payments, demand for digital identity is rising in Kenya's financial sector with a key need to support the growing demand for digital financial services. The financial sector continues to enhance its interoperability, which greatly benefits from a robust digital identity system for bank customers and payments users. The ability to safely layer additional services or products also depends on a robust and secure digital infrastructure, all of which boost safe innovation in the industry.

Digital identity supporting financial services is seen as a key focus of the digitisation of Kenya's economy as outlined in the 2019 blueprint for a digital economy. This blueprint mainly addresses the issue of financial inclusion but also focuses on enhancing trust in Kenya's financial system by improving Anti Money Laundering and Combating the Financing of Terrorism (AML/CFT) processes and being able to better understand the informal economy. For consumers, it will mean access to a wider range of financial services more quickly and should accelerate the number of new entrants into the financial services space, enabling wider consumer choice. Building consumer trust in this new ecosystem will require cross-industry coordination and investment, not just in education and awareness campaigns around how consumers can enjoy the benefits of new services, but also through initiatives to provide reassurance around data usage and data rights. Ultimately though, for consumers the focus is not on digital identity itself, but on the new services it can enable, the problems that are solved and the new value that is created, and that is what will determine whether these initiatives are a success.

3. What and who needs to be supported with the digital identity?

The Huduma Namba project will consolidate existing, siloed databases (currently accessed through the Integrated Population Registration

9 https://www.hudumanamba.go.ke/background/

System IPRS - when identification services are required). It will require intra- governmental co-operation, as well as trust from citizens. Businesses may already be ahead of the curve in Kenya in terms of how they can take advantage of digital identities, and consumers may already be familiar with digital identity driving the services they use due to widespread use of digital payments and banking services. Huduma Namba is yet to be fully rolled out and the level of uptake among Kenyans is yet to be formally assessed.However, there may be a need to provide reassurance to citizens and help them understand the ways in which they can both use and take control of the data they share, and for government regulators to understand the long-term risks around personal data and the potential regulatory and oversight measures that will need to be in place.

4. What are local preconditions for digital identity?

Kenya has several characteristics in its favour when it comes to digital identity. The current identity landscape, strong culture of digital entrepreneurship, and foreign investment means Kenya is set to be a hub for digital identity innovation. Existing examples include apps which provide digital identity services directly, but also digital services that rely on or are strengthened by digital identification. Widespread use of mobile banking and payments products (M-Pesa, which is the largest, but others such as Airtel Money and T-Kash) have played a role in preparing the population for the kinds of digital services that are enabled by digital identity. To some extent, the providers offering these mobile money products illustrate how identity-driven services can build trust. In general, inclusion is a big theme in Kenya, but equally important from a regulatory perspective are financial stability, market integrity and bolstering safety and soundness in the market. Beyond financial inclusion, Kenya's focus in 2020 has shifted to quality, usage, cost effectiveness and market conduct issues.

5. What is needed to facilitate trust in the digital identity?

The primary concern during the launch of Huduma Namba was the lack of an appropriate and comprehensive regulatory framework on the implementation of NIIMS. However, Kenya enacted the Data Protection Act on November 8, 2019. The purpose of the Act is to inter alia regulate the collection and processing of data in Kenya. This Act established the Data Protection Commission and since then, consent mechanisms have been the preferred way of establishing trust around data collection and use. The Act, therefore, addressed previous concerns over the handling of personal data owing to lack of a formal data protection law.[10]

37 million Kenyans have been registered to Huduma Namba using biometric data. The Huduma Namba system will contribute to the Kenya's Big 4 Agenda, Kenya's development blueprint, which looks to enhance Food Security; Affordable Housing; Manufacturing and Affordable Healthcare for all. The Government's efforts to establish a National Master Database through Huduma Namba addresses Kenyan citizens' constitutional rights to access public information. At the same time, it will enhance efforts to meet the goals of the Big 4 Agenda by creating a national persons' identification database that will be a reference point for key national development initiatives.[11]

10 http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
11 https://www.hudumanamba.go.ke/the-big-4/

6. What does Kenya's Digital Identity roadmap look like?

The 2019 Digital Economy Blueprint produced by the Ministry of Information Communications and Technology (MoICT), explicitly calls for every Kenyan to have a digital identity. Currently, the intention is to connect all databases in the IPRS (Integrated Population Registration Services) and collect associated biometric data into a single source of truth, the Huduma Namba. This is still work in progress. The increasingly active involvement of citizens in the ongoing national identity project, and the collaborative approaches being taken by entities such as the central bank and private sector digital financial service providers, means that there is a clear ambition for digital identity. Whilst there is a definite need for collaboration, it would be prudent for targeted goals within sectors to enable buy in. An active Data Protection Commission and participants in the private sector already leveraging identities suggest that Kenya's route to full realization of its digital identity vision is at prime stage for enhanced collaborations across both public and private sector.

The need has been identified and the journey started with goals set to help deliver the vision for Kenya.

PUBLIC-PRIVATE PARTNERSHIPS IN DRIVING ADOPTION

07

COVID-19 has severely disrupted trade, travel and lives. In 2020, the airline industry lost approximately US$118.5 billion[12], with estimated losses to the wider international tourism industry in excess of US$2 trillion[13]. Even as the global situation stabilises, countries are cautious of reopening of borders to international travellers for fear of triggering a domestic outbreak. Destination countries require passengers to reliably prove that they are not carriers of the virus, and governments are developing digital solutions to provide this assurance.

An example is HealthCert, which is a set of digital standards and schema for issuing digital COVID-19 test results certificates that are in line with international standards and the Singapore Government's requirements. HealthCert was developed in collaboration with Singapore's Government Technology Agency (GovTech) and the Ministry of Health (MOH), and enables healthcare providers to issue digitally verifiable health credentials.

Partnerships were formed with private sector technology companies to bring HealthCert to market quickly. As partners came on board and enabled HealthCerts issuance capabilities, healthcare providers performing pre-departure testing for travellers were soon mandated to issue these digital certificates. Through this public-private partnership, Singapore became the first country in the world to have digitally verifiable health credentials issued to all travellers from more than 300 clinics across the nation.

During this time, the Safe Travel Plan workgroup (a cross-ministerial workgroup focused on the safe reopening of borders, which involves private sector partners such as investment company Temasek) identified the proliferation of digitally verifiable health credential solutions to combat fake COVID-19 test certificates as an operational challenge.

Through open engagement with the private sector, a partnership was formed with Affinidi, a Temasek-founded company, which has a universal verifier solution. The solution is able to verify credentials based on a range of different standards. By working together to refine and deploy Affinidi's verifier solution at immigration counters at Changi Airport in less than 6 months, Singapore also became the first country in the world to be able to recognise digitally verifiable health credentials based on multiple standards, allowing it to tap on global private and public initiatives to safely reopen its borders.

These public-private partnerships have demonstrated that by supporting and tapping on each other's capabilities, the pace of innovation and execution can be accelerated substantially and achieve outcomes that may not have been possible otherwise.

7.1 SINGAPORE CASE STUDY: DIGITALLY VERIFIABLE HEALTH CREDENTIALS

While many countries agree on the pressing need to open up international travel while containing the spread of COVID-19, there are difficulties in achieving this quickly. Previously, credentials for international travel were transmitted in two formats: physical documents (e.g. visas, passports) or centralized databases containing data about travellers (e.g. INTERPOL). Both approaches have significant drawbacks that make them unviable for this situation. Physical pre-departure tests (PDTs) and vaccination certificates carry a significant

12 https://www.iata.org/en/pressroom/pr/2020-11-24-01/
13 https://www.unwto.org/impact-assessment-of-the-covid-19-outbreak-on-international-tourism

risk of fraud.[14,15,16] Building a centralized database might have been a solution but the security and privacy concerns along with the time required to align on standards and policies, and connect over 150,000 hospitals and clinics worldwide[17] makes it impractical. In addition to that, the fragmented and constantly changing nature of cross border travel requirements calls for a modern digital solution which is trustworthy, yet decentralized in its nature.

Open, interoperable standards like Open Attestations or Verifiable Credentials enables global interoperability of data that was traditionally stored within physical documents, by making the exchange of data with digital systems virtually costless and cryptographically secure.

Participants across the ecosystem benefit from switching to an interoperable digital system for verifying data validity. For medical labs and clinics, this is easy to set up without disruption to their existing process. They do not have to invest in costly integration with international or national systems that store healthcare records. For travelers, such a solution provides an intuitive and familiar experience since the credentials can be used both in a mobile app and in a form of a printed QR code. And, most importantly, verifying parties, such as immigration authorities and airlines, benefit from increased transparency and level of assurance in the authenticity of the documents. In addition, it provides improvements in operational efficiency: Airlines have estimated that it takes up to five minutes for check-in agents to verify a passenger's paper-based PDT, whereas with the new digital solution, the verification takes less than two seconds per passenger, with the possibility for further automation and integration into existing processes to make the travel process even more seamless. Solutions which may be used in advance of the airport venue as a signal into airline boarding pass processes are most desirable – to eliminate any changes to passenger behavior at the airport.

These standards are most beneficial when they are universally accepted and implemented by technology implementers in the ecosystem.

The need for common standards

All around the world, private and public sector players have launched initiatives to create digital health credentials for COVID-19 test and vaccination certificates. Inevitably, this has led to a fragmented ecosystem, where many solutions are vying to be the leading global or regional end-to-end solution, and many governments are creating unique national digital credential standards. With this fragmentation came a new set of challenges:

1. **No common standard:** Each private or government solution created its own standard and/or implementation method, making it difficult for verifying institutions (such as workplaces, airlines, immigration authorities, etc.) to easily and securely authenticate the credential. Not having a common standard also makes it complicated for healthcare institutions to adopt digital credentials in a quick and seamless way.

2. **Fragmented verification methods:** With each digital health credential issuer, there is a native verification process for only that credential, meaning there is no quick or easy way to verify other various credentials in the industry.

14 https://www.bbc.co.uk/bbcthree/article/ee6ed923-e00e-445b-8a98-7b9917178e30
15 https://www.europol.europa.eu/newsroom/news/europol-warning-illicit-sale-of-false-negative-covid-19-test-certificates
16 https://www.cnbc.com/2021/02/01/fake-covid-tests-criminals-try-to-profit-from-travel-restrictions.html
17 https://en.wikipedia.org/wiki/Lists_of_hospitals

3. **No interoperability between the various standards and implementations:** Most existing solutions require end-to-end adoption (issuance, storage, presentation and verification), and most do not integrate with other solutions.

However, towards the end of 2020, there was a shift in the digital credentials landscape, as private and public sector players recognized that it is unlikely for a single solution to be implemented universally or even across the entire travel industry. As such, there are now several unifying initiatives and products that prioritise open collaboration, cross-industry innovation and interoperable solutions to safeguard public health, in an effort to re-open borders and economies. Some examples of these efforts by inter-governmental and other international organisations include:

- World Health Organization created the Smart Vaccination Certificate Working Group to establish key specifications, standards and a trust framework for a digital vaccination certificate to facilitate implementation of effective and interoperable digital solutions that support COVID-19 vaccine delivery and monitoring, with intended applicability to other vaccines.

- World Economic Forum created a coalition, COVID Action Platform, to galvanize the global business community for collective action, protect people's livelihoods and facilitate business continuity, and mobilize cooperation and business support for the COVID-19 response.

- Common Trust Network was launched by The Commons Project Foundation and the World Economic Forum, to empower individuals with digital access to their health information so they can demonstrate their health status while protecting their data privacy, provide governments a trustworthy model for verification and acceptance of foreign lab tests and vaccination records, whether digital or paper-based, support airlines, airports, cruises, hotels, employers and venues to rely on a trusted health certificate without having to verify it themselves or hold any data, and enable a clearer understanding of health entry requirements for destinations for all stakeholders involved.

- Good Health Pass Collaborative, which is an open, inclusive, cross-sector initiative, bringing together leading companies and organizations from the technology, health, and travel sectors, to create an end to end blueprint for interoperable digital health pass systems and building a safe path to restore international travel and restart the global economy.

- IATA has developed the Travel Pass service for their airline members, which is based upon a decentralized data exchange model.

The private sector is also playing a role in developing and deploying solutions to simplify verification processes. Examples include:

- Affinidi developed a universal verifier that allows verifying institutions to easily recognize and authenticate any digital credential standard and/or implementation. This is made possible through interoperability with different credential issuers and digital health passports solutions. Verifying officers at airline check-in or immigration could use Affinidi's universal verifier to verify different credentials without switching technologies or changing the verification method.

7.2 CAMBODIA CASE STUDY: NEXT GENERATION PAYMENT SYSTEM

With the promoting of a safe and efficient payment system being one of the National Bank of Cambodia ("NBC") 's key priorities, several development initiatives had been undertaken over the past decades to uplift payment system capabilities, ranging from the National Clearing System ("NCS"), FAST system ("FAST") and Cambodian Shared Switch ("CSS"). The latest addition to the payments landscape is Project Bakong - a project that explores the use of an alternative technology platform to further enhance payment system in Cambodia.

This Project was explored as part of effort to address the lack of interconnectivity and interoperability, and attain efficiencies (reduced cost, increased speed, and enhanced security) within the current payment system. It also aims to promote financial inclusion and ease Cambodian Riel ("KHR") cash payment.

As such, in 2016, NBC established a working group to explore the use of blockchain and distributed ledger technology ("DLT") in payment systems. By early 2017, the group had developed use-cases under the auspices of Project Bakong. The name Bakong comes from a prominent Khmer temple from 9th century whose architecture was replicated to build Cambodian Independent Monument in 1958. The logo of Bakong project is the outline of the temple's structure.

Within the same year, prototypes were developed during the second half of the year. In early 2018, the group evaluated the results of the prototype tests and continued to fine-tune business processes, system processes, and internal system integration. By mid-2018, a call for express of interest from the banking and financial institutions to participate in the project was announced for the first time. Several financial institutions participated in the demonstration and discussion of the project.

Given the technological considerations along with the multitude of operational/stress tests that went into the development of Bakong, NBC is positive that this new generation payment system using the blockchain/ DLT technology is feasible. Without hampering the existing payment system and substantial investment by existing participants, an upgraded version of FAST with key design features proves sufficient to further explore the Project Bakong prior to introducing it to the general public.

With regards to the caveats discussed above, the NBC acknowledges that there is a need to mitigate risks, while constantly evaluating the effectiveness and efficiency of the project. The NBC in collaboration with interested participants will strive to bring the effective and cyber-resilient payment system out of this project. As a next step, the NBC has started a pilot test with a first batch of 8 participating institutions and will continue to analyze the technology and business model of the Project Bakong. The pilot test has been completed by the second quarter 2019. Where appropriate, all participants have taken part in the second round of testing in the third quarter of 2019. Bakong went live for the public in early 2020 and a follow-up report on the outcome of the pilot test will be prepared and circulated among stakeholders of the project.

JOURNEY TO ADOPTION

08

Policy makers should act now to reap the benefits of a common digital infrastructure with digital identity at its core in order to accelerate exponential growth of digital transactions. By developing this, policy makers support their citizens from a health, wealth, social and economic perspective. In addition, threats from isolated solutions are avoided, leading to cost-reduction in the long-run.

Across the globe, countries are developing their digital identity model and solution design. Local characteristics such as culture, level of maturity and starting point determine the optimal model and solution design. Hence, no silver bullet exists in shaping a digital identity solution that is fit for purpose.

The considerations for arriving at an optimal national digital infrastructure solution depend on local prerequisites, needs, and available design choices. Once these are identified, it is essential to clearly define a go-to-market strategy as adoption of the four pillars determines its success.

Key factors for successful adoption include:

1. **Alignment of common strategic understanding:** Increase the common strategic understanding of how a full digital infrastructure, with digital identity at its core, creates local benefits for society. Taking a holistic approach will help in seamless integration of digital identity with the other components of the digital infrastructure. Considering the approach of other countries, the interoperability of digital identity components will also contribute to cross-border use.

2. **Development of regulatory enablers:** Create a trusted environment regarding cybersecurity, data privacy and data protection. Technical requirements and implementation are often the first thing to be reviewed. However, the development of related regulation is just as important. Regulation contributes to the reduction of identity fraud and associated losses and increases trust in the digital infrastructure and digital identity.

3. **Leveraging of adoption accelerators:** The right level of collaboration from the private sector can help increase the pace of adoption of digital identity. Collaboration is important to ensure that interoperability and trust are safeguarded as the foundation of the digital infrastructure and digital identity. Involvement from the private sector can also help accelerate the implementation of digital identity due to the variety of use cases. For many markets, resources and motivation to develop a suitable digital identity solution should be provided by the private sector in consultation with the right public sector partnership and governance.

4. **Conducting of ongoing dialog with stakeholders:** Liaise with all involved public and private sector stakeholders to ensure the digital identity model and solution design is fit-for-purpose.

For end-users, a clear communication strategy helps to create awareness as people often need more information on the advantages of 'going digital' and interacting and transacting online. Reaching the most skeptical people is key to encouraging identity and financial inclusion. On the relying-party side, it is important to have the right build and engagement environment for service providers. Great communications and tools will help to get the right level of community support. This will result in rapid go-to-market and deployment of applications where end-users can really reap the benefits of and be in control of their data and financial assets.

8.1 NEXT STEPS FOR FURTHER RESEARCH

1. **Expansion of the research for authorisation & consent, payments interoperability and data exchange:** To follow and complement the in-depth analysis of digital identity. This will also help inform policymakers what local preconditions already exist, which existing regulations help define the digital infrastructure environment and which may need alignment.

2. **Analysis of digital identity progress in other countries:** Additional countries from other regions in the world could be involved in the research to demonstrate that the issues raised in this document are not unique to Asia and Africa. Examining other countries in Europe, Latin America and North America is still under discussion and are a consideration for future research.

3. **Cross-border use of digital identity:** Countries are at various stages of implementing a digital identity solution as part of the delivery roadmap to arrive at a digital infrastructure. The digital identity model and solution design applied by countries is fit for purpose and addresses the domestic use cases critical to their economy. Future research should seek to look into the possibilities of supporting cross-border use cases for digital identity and will consider the following areas:

   a. Open source solutions that may help countries deploy cost effective solutions where they have yet to deploy a digital identity solution in country to avoid issues that other countries have faced

   b. An interoperability layer based on open source solutions that could provide interoperability across digital identity solutions and across borders to support the aspirations for a truly global digital economy. To this end, MAS plans to collaborate with the BIS Innovation Hub in Singapore to explore the opportunities to improve cross-border payments by connecting payment systems to digital identities across borders.

The insights from future research should contribute to enhancing common understanding on digital identity as foundation for a digital infrastructure enabling and accelerating the next evolution in the digital economy.

4. **Building a consortium of countries to explore interoperable frameworks:** The next phase of the initiative will focus on engagement, dialogue and consensus with central banks and regulators to drive collaboration and explore common frameworks for foundational digital infrastructure.

GLOSSARY

08

Authentication	Process of someone proofing that it is actually this person that is performing an interaction
Attribute sharing	Process of end-user sharing a single or set of attributes pertaining to their digital identity with relying parties. Attributes could include name, phone number, email address, residential address, income, and age required to fulfil a specific need in a use case
Authentication assurance	Level of certainty that the claimant of the identity controls the authenticator. Authentication assurance is lower for a username and passport as someone can easily falsely claiming the identity, and higher for a biometric fingerprint or multiple factors such as a mobile token in combination with a fingerprint
Authorisation (or consent)	The process of initiating a digital (payment or data) transaction by making evident that someone is who he/she claims to be and have the authority to do the transaction
Application Programming Interface (API)	Specifies how some software components should interact with each other
Anti-Money Laundering (AML) requirements	Legal controls that require financial institutions and other regulated entities to prevent, detect and report money-laundering activities
Consent (and authorisation mechanism)	Enables end-users to control their data and money when they digitally interact and transact with their service providers of choice
Data exchange	Enables end-users to make their data available and accessible to any service provider of their choice for a set period of time
Digital Identity	Enables individuals, businesses, and public institutions to represent themselves and others in the digital economy
Digital Infrastructure	Layer built on top of the internet, accelerating innovation in how end-users and their service providers interact and transact in the digital economy
Federated identity	Ability of relying parties to rely on one digital identity created by a trusted party. The end-user can use a federated digital identity at multiple places
Financial Inclusion	Availability and equality of opportunities for end-users to access financial services in order to participate in the (digital) economy

Identity assurance	Level of certainty that the credentials being present during identity proofing can be trusted to be the proxy for the individual to whom the credentials had been issued, and not someone else. The level of identity assurance is lower for a self-asserted digital identity, for example a social media profile, than for an identity verified by a trusted source, for example a passport verified by the government.
Identity provider	Role in the identity ecosystem which creates, maintains, and manages identity information for end-users while providing identity services for relying parties
Identity verification provider	Role in the identity ecosystem that verifies user identity data, such as a government (for passport), mobile network operator (for phone location), postal service (for address), financial institution (for core identity data from KYC actions).
Identity proofing (also referred to as verification)	Process of confirming an end-user is who they claim to be. Relying parties use identity proofing during the digital sign up of an end-user
Interoperability	A situation in which local (payments or data) instruments belonging to a given scheme or platform may be used in platforms developed by other parties, cross-sector, cross-border. Interoperability requires technical, legal, and business compatibility between systems
Know Your Customer (KYC)	Process for banks or others to verify identity of customers, typically tied to regulatory or other business policy requirements. eKYC is referred to the digital process of Know Your Customer
Level of Assurance (LoA)	Ability to determine, with some level of certainty that a claim of a particular identity made by a person or entity can be trusted to actually be the real identity. LoA plays a central role in creating trust in the identity and transaction online.
Mandates	Process of enabling people to act on someone' else behalf. If end-users may be allowed to act behalf of someone else, either be it an individual or an entity, then the mandate functionality comes into play

Mobile Network Operator (MNO)	Provider of wireless communications services that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure, back haul infrastructure, billing, customer care, provisioning computer systems and marketing and repair organisations.
Payments	Ensures end-users can control and exchange their financial assets
Personal Identifiable Information (PII)	Any data that could potentially be used to identify a particular person. Examples include a full name, passport number, and email address
Platform	Single party model established to connect two-sides of the market (e.g. end-users and relying party). In identity platform models offer a federated identity which end-users can use at multiple relying parties
Relying Party (RP)	Used to describe the organisation that provides services to end-users, in underlying transactions relies on the digital identity of that end-user
Trust Framework	Multiple party model established for a common purpose (such as setting up a digital identity solution) consisting of a legally enforceable set of legal, business and technical agreements and standards

REFERENCES

09

1 World Bank (2016), "Digital identity: towards shared principles for public and private sector cooperation", http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf

2 World Economic Forum (2019), "Platform for good digital identity", https://www.weforum.org/projects/digital-identity

3 Source: "A Blueprint for Digital Identity", World Economic Forum 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

4 Mastercard (2019), "The Global Data Responsibility Imperative". Retrieved from https://www.mastercard.us/content/dam/mccom/en-us/documents/global-data-responsibility-whitepaper-customer-10232019.pdf

5 McKinsey (2019), "Digital Identification, a key to inclusive growth". Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

6 World Bank (2019), "Digital ID a critical enabler for financial inclusion". Retrieved from https://blogs.worldbank.org/psd/digital-id-critical-enabler-financial-inclusion

7 Open Identity Exchange (2018), "Digital Identity in the UK, the costs of doing nothing". Retrieved from https://openidentityexchange.org/blog/2018/04/26/digital-identity-in-the-uk-the-cost-of-doing-nothing/

8 National Institute of Standards and Technologies (2020). Retrieved from https://www.nist.gov

- Aadhaar (2019), "About your Aadhaar". Retrieved from https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html
- BankID (2019), "This is BankID". Retrieved from https://www.bankid.com/en/om-bankid/detta-ar-bankid
- Brunei: Key stakeholders from the Central Bank and government agencies
- Cambodia: Key stakeholders from the Central Bank and government agencies
- CamDX (2020), "Cambodia Data Exchange Platform". Retrieved from https://www.camdx.gov.kh
- e-Estonia (2019), "About e-Estonia". Retrieved from https://e-estonia.com/about-us/
- Ghana: Key stakeholders from the Central Bank and government agencies
- Kenya: Key stakeholders from the Central Bank and government agencies

- MyInfo (2019), "About us". Retrieved from https://www.singpass.gov.sg/myinfo/common/aboutus
- National Identification Authority (2020) "Ghana Card". Retrieved from https://nia.gov.gh
- SingPass (2020), "About SingPass". Retrieved from https://www.singpass.gov.sg/singpass/common/aboutus
- World Bank ID4D Survey, 2018 – noting that this figure may be overstated as the legal age in Kenya is 18 years not 15 years.
- World Bank Global Findex Survey, 2017.

DOCUMENT AUTHORS

This document has been produced as a collaboration between: The Monetary Authority of Singapore; The Central Banks and government agencies of Brunei, Cambodia, Ghana and Kenya; Mastercard.