# Digital identities

## Advancing digital societies in Asia Pacific

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

## GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

This report was authored by
**James Robinson,** Senior Analyst
**Barbara Arese Lucini,** Senior Analyst
**Jeanette Whyte,** Senior Policy Manager – APAC

TRPC is a research consultancy with over 25 years' experience in the telecommunications and information technology industries in the Asia-Pacific region. It offers specialised advisory, research and training services, with a focus on economics, regulatory and strategic business issues, and possesses an extensive network of industry experts and professionals throughout the region.

For more information, please visit www.trpc.biz

# Contents


# Foreword

This is the third report the GSMA has produced on Digital Societies in Asia Pacific and builds on the findings of previous studies.[1]

Digital identity is the cornerstone of a digital society – the capacity to prove you are who you say you are in a digital form is a fundamental component of economic, financial and social development. Mobile operators have a pivotal role to play: once an individual has been registered and issued with a digital identity, mobile phones and other connected devices can verify and authenticate that identity, and allow access to a variety of online transactions and services.

1 See Building digital societies in Asia: Making commerce smarter and Advancing Digital Societies in Asia

Digital identity is more than just a matter of policy and convenience; it provides the opportunity to interact with government securely, while also enabling governments to better respond to – and improve the lives of – citizens. Authentication of identity ensures that citizens and governments remain accountable for their actions, while enabling them to perform necessary actions, such as paying taxes or distributing social welfare. Digital identity connects people to electoral participation, educational opportunities, welfare payments, banking and economic development – all of which create a platform for the private sector to provide services and for the economy to flourish.

In Asia Pacific, digital identity is a priority in lower-income countries as a primary source of identification and as an opportunity to foster digital, financial and social inclusion. Such countries often lack robust systems for physical proof of identity and are building their identity systems on a digital basis, leapfrogging traditional paper-based systems. The scale of the identity problem in these countries is vast, with millions of people unregistered – a situation that not only causes problems in accessing e-government services, but also raises the most basic challenges such as buying a phone or applying for a bank account.

In higher-income countries, digital identity enables the transformation of traditional commerce and services into more efficient and convenient e-commerce and e-services. Canada, Belgium, France, Finland, Singapore and South Korea, among others, focus on creating digital identity ecosystems for successful delivery of digital public services. These countries emphasise digital identities to combat online fraud, ensure cybersecurity and enable digital, societal, trust-based transformation.

Properly designed safeguards of privacy and security engender citizens' trust in governments and companies, without impairing data flows within nations or across borders. Governments need to have modern frameworks in place for data protection and privacy, particularly in light of recent, high-profile data leaks such as a low-tech breach in India's Aadhaar national identity scheme.[2] Similarly, in light of well publicised hacking incidents such as the $81 million[3] cyber-attack on Bangladesh Bank in 2016, secure cyber protocols and platforms need to be in place to instil confidence in users and deter any would-be cyber criminals. Governments have a legitimate interest in enacting measures to ensure cybersecurity, but the measures should not impede the development of a digital society. A worrying trend in Asia Pacific is to legislate various requirements for data localisation – the storing of citizens' data within a country rather than outside, in the cloud, wherever it is most economical to do so. This will not only slow progress towards creating regional digital societies; it could also fail to address the aims of enhancing security, data privacy or consumer protection.[4]

This report focuses on the need for governments and businesses in Asia Pacific to partner in creating a digital identity programme that applies across national domains and disparate legal jurisdictions. With rapid adoption of new, mobile-based technologies and a broad array of states at different stages of development, Asia Pacific is ideally placed to provide the backdrop for uniting disparate stakeholders to promote the growth and expansion of digitisation.

As with many rapidly evolving aspects of the digital age, analysis of current issues of digital identity unveils still more questions. It is important to raise and clarify these questions so that we might begin to consider possible answers. Assisting in providing at least some of the answers is our ambition.

**Emanuela Lecchi**
GSMA
Acting Head of Asia Pacific
June 2018

2 "Data Breach: Aadhaar Details up for Grabs for Just Rs 500", thewire.in, January 2018
3 All references to $ are to US dollars.
4 For more detail, see Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia, Brookings, March 2018

# 1 Executive summary

In today's digital society, intelligently connected devices and interoperable services are revolutionising the way individuals and enterprises connect, communicate and navigate their surroundings. In Asia Pacific, where connectivity is primarily mobile-first and, in some emerging economies, mobile-only, mobile operators continue to play a critical role in the delivery of the digital services that enable and nurture the development of digital societies.

Connectivity is a recognised precondition for a digital society. The adoption of digital identities is another, leading to significant quantifiable economic benefits. One estimate, for example, quantifies the economic value of a system for establishing secure, nationwide digital identities in Australia alone at $8 billion per year.[5]

There is no single solution for providing digital identity across Asia Pacific. While governments are central in supporting the establishment of digital identity systems, the increasingly cross-border nature of digital activity and the need for added layers of authentication to ensure consumer trust have made it imperative for governments and the private sector to collaborate in developing and deploying solutions that protect users and keep personal information private and secure.

This report addresses these issues and sets out how digital identity systems can enable citizens to participate seamlessly and securely in our emerging digital societies. Achieving scale and effective registration of the population is crucial if governments are to achieve an inclusive digital society. Mobile operators can leverage unique resources to facilitate not only scale, but also a more secure and efficient registration process. We look at a host of country examples and use cases to show the diverse landscape of emerging, transition and advanced digital societies in Asia Pacific, along with recommendations for progressing from one stage to the next. These examples include payment systems that enhance trade via cross-border data transactions, initiatives that improve consumers' lives with digital services tied to a digital identity, and digital IDs for refugees to foster their financial and social inclusion in host countries.

5 "A frictionless future for identity management: A practical solution for Australia's digital identity challenge", Australia Post, December 2016

As activities and interactions become digitised, 'digital citizenry' – with individuals authenticating their identities in the digital space – becomes an important prerequisite for effective participation in society. The challenge ahead is to unlock the unrealised social and economic benefits of inclusion by developing robust, digital ID systems. Mobile operators are best placed to fulfil this need by offering a secure platform to seamlessly connect users with services and providers, while maintaining privacy and security.

Likely developments over the coming years include the following:

- A greater demand for **security and trust** by consumers before adopting services based on their digital identities. Properly designed privacy and security safeguards will help gain citizens' trust, while ensuring that the flow of data is not unduly impaired, whether at the national level or across borders.
- The application of **new technologies** such as distributed ledger technology (DLT), commonly known as blockchain. If structured with privacy by design and by default, DLT should address security concerns in complex, multi-party transactions via decentralised structures that better enable users to control what – if any – personal information they share with particular parties.
- More **collaboration and cooperation** between governments and the private sector to develop digital identity solutions that improve user experience through interoperability. An example of such partnering includes the work of the GSMA with mobile operators to develop Mobile Connect – a federated identity management system linking a person's electronic identity and attributes while providing simple, secure and convenient access to digital services.

Countries with robust national governance and centralised frameworks for development generally have a better chance of driving the necessary change. The same holds true for digital identities – a key pillar in developing a digital society. We therefore focus on tracking a number of national, digital identity programmes and digital economy plans. At the supranational level, only governments themselves can take the necessary steps to harmonise national rules on digital identities that will in turn improve global trade.

Since our previous Digital Societies report, all countries surveyed have increased their scores on our index of digital societies.[6] As we noted at the time, there is no single path to a digital society; rather, progress comes from a continuous process of integration and interconnection of processes and services to create new and more efficient ways of doing things. By bringing together government plans, use cases and best practices, we offer guidance for countries to consider when advancing their national digital agenda and ways to strengthen, where appropriate, each of the components of a digital society: connectivity, digital identity, digital citizenship, digital lifestyle and digital commerce.

## In short

- In emerging digital societies, digitisation is a tool to provide access to essential services such as healthcare, education, and financial services, which are otherwise not easily accessible due to cost of provision, lack of infrastructure and poor logistics.
- In transition digital societies, personalisation of services is greater than in emerging digital societies, leading to greater engagement between individuals and institutions.
- In advanced digital societies, the emphasis is on improving trust, efficiency, effectiveness and convenience by using smart technologies such as IoT, artificial intelligence (AI) and DLT.

6 To calculate the overall digital societies index and each of its components, we used a number of sources, including data from the UN, World Bank, WEF, IMF, GSMA Intelligence and the GSMA Mobile Connectivity Index. See Appendix B for a full methodology.

# 2 Introduction

In this report, we explore the role of government, mobile operators and the broader private sector in supporting digital identity in Asia Pacific. We focus on eight countries that showcase the variation in the region: Australia, Bangladesh, Indonesia, Japan, Malaysia, Pakistan, Singapore and Thailand. With the exception of Malaysia, we also examined these countries in the first GSMA Digital Societies report for Asia Pacific in 2016, and, as in the following year's report Advancing Digital Societies in Asia, we here re-examine the progress countries in Asia Pacific have made along their digital society path. Malaysia is a new addition to the list because of its emerging digital identity plans. The focus countries sit within our three broad categories of digital society – emerging, transition and advanced – based on the level of connectivity and the relative development of the various components of their digital societies.

Anyone who accesses services online acquires an online identity. However, an online identity is not the same as a digital identity. To deliver on objectives of inclusiveness, economic growth and digital citizenship, governments, the private sector, and mobile operators should support a framework of solutions for services that need a high degree of identity and security, i.e. for validation, verification and authentication, and are used across multiple platforms for different transactions.[7] This is particularly true in environments where many citizens lack awareness or experience in managing their own online identities and presence online.[8]

7 For example, in New South Wales, Australia, drivers will soon be able to have a 'digital' driving licence. This is akin to digitisation of a physical ID, more than what we refer to as a 'digital ID'. It is not clear how validated, verified and authenticated the driving licence will be. In addition, it seems that it will not support other uses, at least for the time being.

8 This is particularly pertinent in light of the recently reported breach of data from India's Aadhaar scheme.

The outline for this report is as follows:

- In Chapter 3, we consider a number of digital identity programmes in operation across our range of economies, from the developing Bangladesh[9] and Pakistan, to transition economies of Indonesia, Malaysia and Thailand, to the more advanced economies of Australia, Japan and Singapore. Of particular note are the initiatives undertaken by regional organisations such as ASEAN to ensure proper cross-border data flows.
- In Chapter 4, we provide an overview of the many, quantifiable benefits achieved and likely to be achieved for various countries' consumers, businesses, societies and economies.
- Chapter 5 looks at the need to foster trust in the digital economy, explains the difference between identity and authentication, and explores the role of appropriate privacy and security frameworks.
- Chapter 6 analyses the components of the digital economy index and compares scores across countries and progress since the 2016 GSMA Digital Societies report. We also plot each of the index's indicators against a new 'digital identity enabler score', to highlight the role that a focus on digital identity – and, in particular, the frictionless authentication of identity online and across networks – plays in progress to a fully realised digital society.
- Chapter 7 offers guidance on steps for the focus countries to improve their transformation to digital societies. These steps go beyond identity, but identity remains an underlying requirement, so we consider it separately in its own right.

## 2.1 Identity, digital identity and authentication

There are many definitions of what comprises a *digital* identity but at a basic level it is a function of three different concepts, namely validation, verification and authentication, and can be described as:

> a collection of electronically captured and stored identity attributes, including biographic data (e.g. name, age, gender and address) and biometric data (e.g. fingerprints, iris scans and facial photographs) that uniquely describe a person within a given context and are used for electronic transactions.[10]

An understanding of the way to prove identity in the physical, pre-digital world is essential to master the multiple facets of a digital identity. In the physical world, identity can be defined as *a collection of identity attributes such as biographic and number data that uniquely describe a person within a given context and are used for transactions*.

A primary ID provider (IDP) usually provides and collects identity attributes about a person. In the pre-digital world, different government agencies attach identity attributes to individuals, such as numbers for national IDs, passport documents and birth certificates. A system for the allocation of primary attributes allows other providers, known as secondary IDPs, to build on the primary attributes with attributes of their own. Whereas primary IDPs are almost invariably government agencies, secondary IDPs are usually not.

Banks can be effective secondary IDPs, as can mobile network operators. Secondary IDPs take the identity of a primary IDP such as a passport and use that as the basis for their customer identification. The secondary IDPs usually add other characteristics and their own reference numbers to protect personal information and other operational efficiencies. In the absence of efficient and cost-effective access to primary identity, secondary IDPs can fill the gap only up to a point by seeking identities from multiple sources to reduce the risk of fraudulent activity.

To do so, the IDP needs to carry out the following:

1. Identity validation: is the provided identity document or number genuine or valid?
2. Identity verification: does the provided data of the user match the identity on record of the digital identity?
3. Identification authentication: does the identity provided in fact belong to the user providing it?

9 Bangladesh has recently achieved the status of 'lower-middle-income' country and has set the goal of becoming a middle-income country by 2020.
10 Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, GSMA and World Bank, 2016

Many identification processes around the world fail on the first and second levels to validate and verify the identity, let alone check whether the identity provided is that of the user providing it. For example, before 2018, users could register SIM cards in Indonesia by completing a self-registration process when activating the SIM. The mobile operator's entity registering the SIM undertook no verification of the data entered. In this instance, the identity captured by the operators as the secondary IDP was open to falsification, so any subsequent authentication of the identity by customer care was neither efficient nor possible.

Ironically, in the physical world, the identity is rarely validated; for example, a bank takes a copy of a passport without validating whether the passport is fake and relies on the passport matching other forms of provided ID such as proof of address. In the online world, commercial service providers try to reduce the risk of fraudulent transactions or interacting with false identities by seeking multiple, credible sources to match identity data and/or add attributes to complement known data. For instance, when a person in Pakistan registers to be an Uber driver, Uber sends a person to the registered address to verify the data provided online and to check with neighbours that the person is who they say they are.

This process is both time consuming and costly and would be more efficient if other sources of data were used for verification. For example, a mobile operator could verify whether details provided by the driver's MSISDN (Mobile Station International Subscriber Directory Number)[11] matched those they provided to Uber. For online payment providers, mobile operators can enhance the verification process by providing contextual information available in its network to assess the level of fraud risk. For example, is the device, represented by the SIM, in its usual location? To check for abnormal behaviour, has the user frequently changed the SIM? And to enhance confidence, how long has the user been a customer of the mobile network?

Similar concepts exist in the digital world where mobile network operators use primary identity providers such as the Aadhaar system in India to register SIM cards and establish a secondary identity. In India, the mobile operators maintain a copy of the registered Aadhaar identity for each SIM card and have the ability to add attributes to that identity if they expose it to a third party.

In the digital world, for authentication, it is relatively easy to verify whether an identity is true. Verifying whether the identity provided belongs to the user providing it requires a secure and robust authentication mechanism that needs to be able to verify that the user is the owner of the identity.

## Defining level of assurance

Level of assurance describes the degree of confidence in the process of authentication. It provides assurance that the person claiming a particular identity is in fact the person to which the identity was assigned. The US National Institute of Science and Technology (NIST) has defined four levels of assurance.

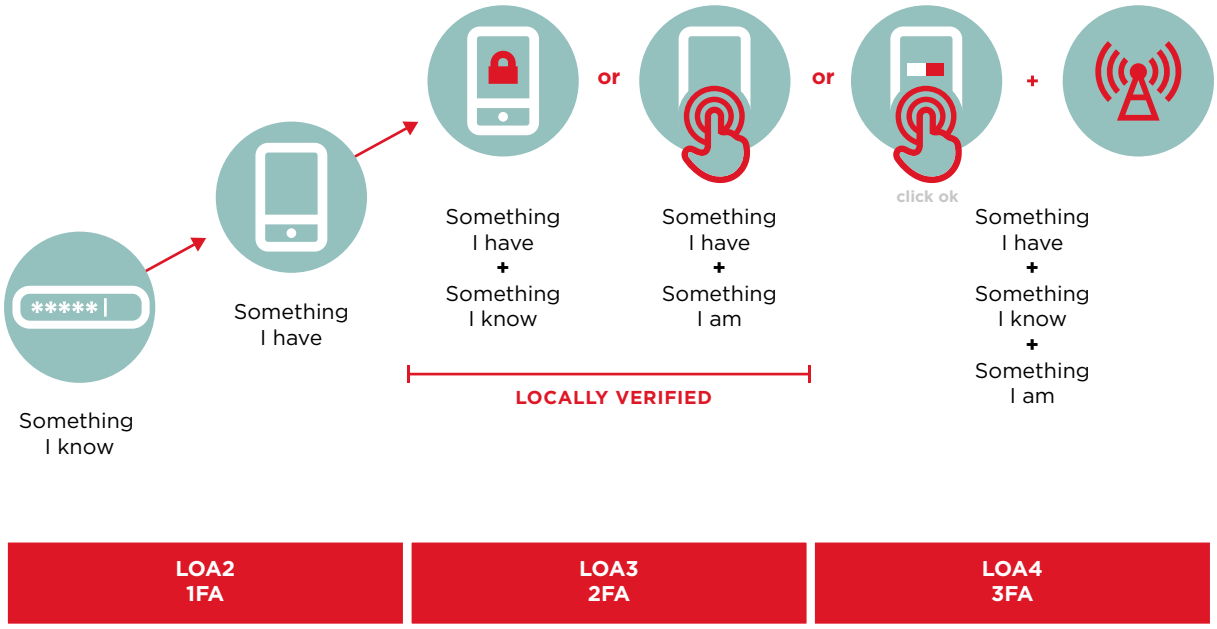
| Level of assurance | Level of confidence | Type of authentication | Example use case |
|---|---|---|---|
| **1** | Little/no confidence | No specific requirement for the authentication mechanism | Authentication for reading pages on a newspaper website |
| **2** | Some confidence | Single Factor – "Something I have" | Authentication for update of a record such as change of address on a website |
| **3** | High confidence | Two Factor – "Something I have" and "Something I know" or "Something I am " | Authentication for online access to a brokerage account |
| **4** | Very high confidence | Multifactor +PKI[12] – "Something I have" and "Something I know" and "Something I am " | For services where there is a potential for high risk of harm in the case of an authentication failure |

**Source:** NIST[13]

11 MSISDN is a number used to identify a mobile phone number internationally.
12 Public Key Infrastructure
13 Electronic Authentication Guideline, National Institute of Standards and Technology, US Department of Commerce, 2017

The increasing complexity of digital lives requires the development of ever more comprehensive and secure systems for authentication. The challenge is therefore to deliver the full spectrum of digital economy services and protect users' privacy and security online. Mobile Connect offers a valuable framework for achieving this goal. From the perspective of identity, governments regulate mobile operators as the providers responsible for registering SIMs against the government system for verifying primary identity. For authentication, even in the absence of national privacy laws, governments tend to regulate operators to protect the privacy of their customers. Together with Mobile Connect, operators work in a regulated framework for identity and authentication, with services delivered over a secure network. By contrast, governments do not regulate the identification practices of internet players such as Facebook and Google, which often have limited or no obligations for authenticating their users.

## The Mobile Connect Authentication Solution

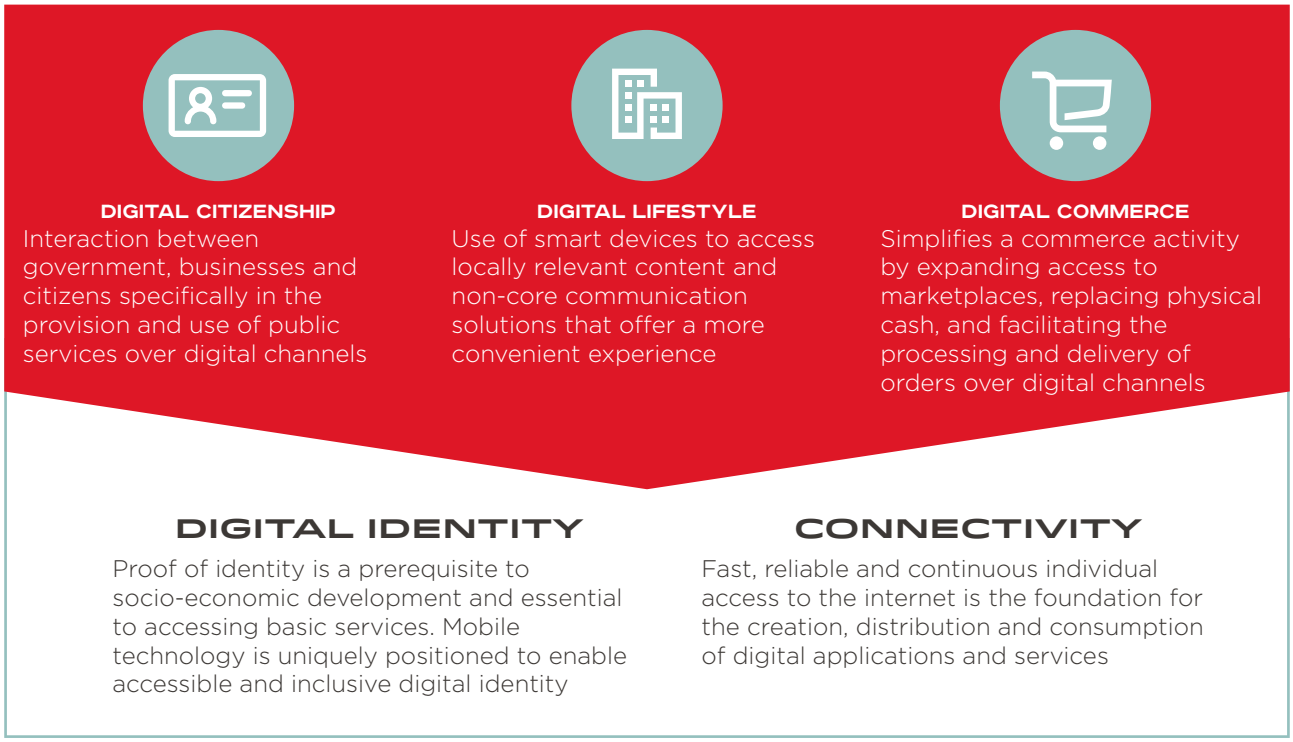


# 3 Digital societies landscape in Asia Pacific

Governments throughout Asia Pacific understand the importance of digital identity and are developing digital identity solutions, often in cooperation with the private sector. Cooperation is not without its challenges, but the principles for successful partnerships are increasingly well understood. Cross-border initiatives are also paving the way for effective digital trade in the region. Initiatives within ASEAN offer good examples of regional cooperation.

**Figure 1**

## Key components of a digital society




**Source:** GSMA Intelligence

Connectivity is one of two elements that constitute the foundation of a digital society, allowing companies to distribute, and users to consume, digital applications and services. In Asia, digital services function primarily through mobile, or "mobile-first" connectivity. This is particularly true of Asia's emerging economies, as well as remote areas in developed economies, where connectivity is often "mobile-only" more than "mobile first". Mobile operators are thus uniquely positioned to play a critical role in the delivery of digital services.

An equally fundamental component of a digital society is digital identity; without an identity, users cannot participate in the digital space and reap the benefits of a digital society. Once an individual has been registered and issued a digital identity, mobiles and other connected devices can be used to verify and authenticate that identity, and allow access to a variety of online transactions and services. Mobile operators and public sector players can achieve a lot in cooperation with each other.

For example, GSMA's Mobile Connect[14] is a global, open and common framework developed by the GSMA in cooperation with leading mobile operators. Through a single consistent interface, Mobile Connect supports authentication, authorisation, identity and attribute sharing or verification for service providers, while putting the user in control of their data. For end users, it combines the user's unique mobile number, and an optional PIN and/or other authentication factors for added security, to verify and authenticate the user. The combination of mobile device, mobile network and operators' business-process security enables secure and user-friendly services for a wide range of online use cases, including e-government services, e-commerce, e-health and payments. It is based on the principle of 'privacy by design'.

Mobile Connect enables the provision of an authentication experience on a par with best practice in the private sector, using mobile technology to leapfrog legacy infrastructure and economic barriers to delivering secure digital identity programmes. For governmental organisations, Mobile Connect can deliver flexibility, real-time access to information, assured interaction with citizens and multi-function digital identity, while reaching the required levels of security for robust mobile identity issuance and authentication. Mobile Connect is available to 470 million users in Asia Pacific across 31 operators.

## 3.1 National digital identity programmes in Asia Pacific

Government-backed or recognised identities (often a *physical* identity scheme) are the first step on the road to universal digital identity. Achieving scale and effective registration of the population is therefore important, as is the ability of the system to support multiple services without compromising the performance of the system. This is primarily a task for the public sector, but mobile operators can facilitate ID enrolment by leveraging mobile devices, agent networks and other assets, potentially including customer data (with explicit consent).

Countries from across the region recognise that a comprehensive and reliable national identity scheme is a precondition for effective public policy formulation; its absence can result in inefficiency, corruption and failure to deliver adequate social protection. Our focus countries also understand the need to scale enrolment in identity systems: as of 2017, for instance, the Thai government had registered about 97% of the country's population.

Nevertheless, the varying degrees of progress that the focus countries have made in the evolution of their national identity systems mean Asia Pacific is home to both pioneers and laggards. In digital identity, advanced economies are not always at the forefront. Citizens of some Commonwealth countries, including the UK, traditionally have been wary of how ID cards can give governments information and access to private records. For example, despite being an advanced nation, Australia has only recently announced the development of a federated digital identity system to simplify citizens' access to government services online, with information stored in a centralised database. In 1987, Australia abandoned its plans for its Australia Card, and in 2007, had to drop the notion of a more limited Access Card for Medicare and welfare payments due to citizens' concerns.

Other countries have had mixed results. The Malaysian Communications and Multimedia Commission (MCMC) announced plans to develop a secure digital identity platform for both the public and private sectors.

14 For more information on Mobile Connect, see https://mobileconnect.io/operators/

Singapore is further along in its digital identity scheme having overhauled its SingPass and CorpPass programmes to provide improved security and better integration with a range of existing and forthcoming services, including real-time payment authentication tied to a mobile number, and the use of shared services, such as bicycles, cars, lodging and drones.

Indonesia represents a progressive adopter of electronic identity credentials and technologies after launching its ambitious e-KTP (Kartu Tanda Penduduk elektronik, or Resident Identity Card) programme in 2011. The country rapidly scaled up enrolment in the programme to 100 million people during its first year and 140 million by 2012. However, difficulties in procurement and a corruption scandal have hampered e-KTP's national rollout, causing shortages and extended delays. In Japan, initial progress with the production and distribution of smart ID cards was slower than expected due to problems with systems integration.

A common aim of these national programmes is for a digital ID to reduce instances of forgery – particularly voter fraud – by relying on various biometric features. In Bangladesh, the Identification System for Enhancing Access to Services (IDEA) heralds the beginning of a change of culture towards efficient and effective delivery of public services, with the joint aim of removing instances of fraud, as exemplified by the discovery of 50,000 fake documents in 2014. The Indonesian government claims that e-KTP credentials are virtually impossible to forge and consequently should not be subject to misuse by criminals and terrorists, who have been known to evade capture by using multiple, counterfeit ID cards.

## National identity programmes

### Pakistan

Every citizen over the age of 18 is eligible for Pakistan's National Identity Card (NIC) issued by the National Database and Registration Authority (NADRA).[15] This unique 13-digit identification number is a mandatory requirement to obtain passports, bank accounts, licences and cellular connections, among other things. NADRA has also introduced SMS-based tracking for a number of its projects including its digital identity cards programme, enabling potential beneficiaries to check their eligibility via mobile.[16] With an aim to reduce the incidence of false identities, in 2016 NADRA launched a campaign to allow computerised NIC holders to re-verify the identity of their registered family members by sending an SMS via mobile.[17] This provided an opportunity to citizens to report to authorities any person registered illegally under the same family tree.

Through its NIC programme, Pakistan has been able to leverage its "citizen-centric data management" strategy to securely deliver a number of financial and government-to-person (G2P) services such as social grant programmes, financial inclusion programmes, smart national identity cards, and pension disbursement schemes.[18]

### Japan

Japan's National ID system, My Number, was introduced in 2015. It is a randomly generated 12-digit identification number issued to all citizens holding a residential record in the form of a digital ID smartcard, called the Individual Number Card. This contains digital certificates stored inside a chip for digital authentication. The owner's name, address, date of birth, sex, ID number and photograph are displayed on the card. In its initial phase, the card was for use in social security, tax returns and disaster-relief assistance. Applications for the ID card began in 2016, and signups were facilitated through mail and ID photo booths, as well as online.[19]

15 For more information, see https://www.nadra.gov.pk/identity/identity-cnic/
16 For more information, see https://www.nadra.gov.pk/local-projects/identity-management/sms-services-7000-8400-8300-8500/
17 "SMS NADRA to get your CNIC, family tree re-verified", The Express Tribune, June 2016
18 For more information, see https://www.nadra.gov.pk/solutions/e-governance/
19 For more information, see https://www.kojinbango-card.go.jp/en/kojinbango/index.html

### 3.1.1 Government inter-departmental interoperability

Establishing a single, all-encompassing e-government platform can improve inter-agency coordination and intra-agency efficiency, as well as delivering cost savings.[20]

Where the state recognises multiple IDs, interconnectivity and interoperability among the registries becomes a priority for seamless use of the identification and full coverage. Adopting a coordinated e-government strategy helps policymakers create a thriving and interoperable digital ecosystem at a national level, driving participation in relevant programmes.

## Government inter-departmental interoperability

### Bangladesh

In 2016, the Bangladesh government launched a mobile app, Alapon, to facilitate secure information exchange and communication between the country's 1.4 million government officials. Messaging, online voice and video calls, file and location sharing, and a mobile directory are among the app's features that help to connect government officials across agencies and departments via a single platform.[21] The government notes that better communication within the public sector is key to achieving higher standards of government services.

### Australia

Australia does not have a single national ID card; instead, it uses a variety of other digital documents for authentication. In May 2017, the federal Digital Transformation Agency (DTA) partnered with Australia Post to integrate their mobile Digital ID with the Commonwealth's Digital Identity Framework. By adopting nearfield communications (NFC), a smartphone can be used to scan information from a document, such as a passport or driver's licence, for Australia Post to perform a biometric comparison to the individual.[22]

### Japan

All government information systems in Japan use a cloud-based Public Certification Service platform for verification of identities to allow seamless access between systems, except for those information systems with special requirements. Public agencies at the national and local levels can track and share information, avoiding problems such as inaccurate payments or duplication of administrative processes, and breaking down vertical divisions within agencies. These efforts have also reduced operational costs to improve the security and disaster resilience of governmental and citizen data.

### Singapore

The Smart Nation and Digital Government Office (SNDGO) is currently developing its Moments of Life initiative, an intergovernmental framework that bundles government services and information. A project still in the making, it aims to use data to anticipate citizens' specific needs as they reach key life moments, such as marriage or the birth of a child. An initial version of the digital service is expected by the middle of 2018, with expansion in scope over the next two to five years.

20 For example, the UK government saved around £3.56 billion over the three years to 2015 from the digitisation of public services on the 'gov.uk' platform. See "How digital and technology transformation saved £1.7bn last year", Government Digital Service, October 2015

21 "Govt. unveils REVE developed Alapon app for employees", REVE Systems, September 2016

22 "Australia Post delivers on Digital iD", The Mandarin, July 2017

## 3.1.2 Public-private sector collaboration

Governments and private sector firms share a common interest in promoting robust digital identity systems for identification and authentication. Public and private stakeholders may rely on each other to build and manage identity systems: governments may outsource various aspects of their identity architecture to private firms (e.g. system development) and collaborate with the private sector to ensure interoperability of an official identity with private services such as metro passes. Similarly, private secondary IDPs often rely on official forms of identification such as birth certificates and national IDs to validate the identity of their users.[23]

Such partnerships face challenges. For example, in Bangladesh, the government scrapped a deal with a French company – Oberthur Technologies – for its failure to complete the production and supply of all ID cards on time. Successful collaboration between private companies and the state requires a sustained effort among actors, underpinned by common objectives and understanding. A joint report[24] co-authored by the GSMA, World Bank and Secure Identity Alliance identifies three areas to serve as the preliminary basis for cooperation:

- universal coverage
- appropriate and effective design
- the creation and maintenance of trust.

To create identity systems that meet these requirements, government and industry stakeholders must also develop a consensus regarding standards for: the legal and regulatory environment; technology; governance structures; public-private cooperation; stakeholder awareness; convenience; and facilitation of a competitive marketplace.

### Public-private sector collaboration

#### Pakistan

Pakistan was an early developer of a national ID card, operated by NADRA. A series of initiatives dating back to 2009 have emerged to link mobiles to digital identity, such as Telenor's EasyPaisa which uses the SIM to connect to, for example, the Bank of Punjab's branchless banking services through its Biometric Verification System (BVS). When integrated with the NADRA ID card, the service became a smartcard (from 2012 onwards) as part of the National Financial Inclusion Strategy.[25] Branchless banking is forecast to rise rapidly from 17 million accounts in 2016 to 20–30 million in a matter of years.[26]

An initial four-month pilot by Telenor in 2015 in collaboration with UNICEF, and supported by the GSMA, saw birth registration rates increase by an average of 200%. This included a 300% increase in Sindh province and 126% in Punjab. The current phase of the project seeks to register 700,000 children by the end of 2018. As of February 2018, the project had successfully reported 77,000 new births.

#### Thailand

Thailand is undertaking several initiatives to become a digital and smart economy. In late 2017, the country announced plans to make the submission of biometric information mandatory for the registration of all new SIM cards.[27] Meanwhile, efforts to encourage cashless payments have increased. Mobile operators offer money transfer services, such as TrueMoney,[28] and in January 2017 the Bank of Bangkok launched PromptPay as part of Thailand's National e-Payment Initiative.[29] Through PromptPay, customers can transfer funds using a recipient's mobile number or national ID number without the need for bank account numbers.[30] A gap continues to exist between objectives and fulfilment, but as digital communications improve so will the quality and scope of services.

Moving towards a more digital economy and society, in February 2018, the Electronic Transactions Development Agency (ETDA) partnered with Omise,

23 Estonia, Finland and Moldova have all partnered with operators to deliver mobile authentication services to eID cardholders. In each case, the mobile companies issue users with a PKI-enabled SIM, and then charge a per-use fee when they use a digital signature to authenticate themselves for e-government and other online services.
24 Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, GSMA and World Bank, 2016
25 "Financial development and inclusion", Business Recorder, July 2017
26 "Pakistan on road towards digital economy", The Nation, January 2018
27 "Thailand to roll out biometric checks for SIM cards nationwide", Reuters, November 2017
28 Building Thailand's Digital Economy and Society, GSMA, 2015
29 "New mobile payment system launched in Thailand as part of National E-payment initiative", OpenGov, October 2017
30 "Thailand rolls out PromptPay money transfer service", Nikkei Asian Review, January 2017

Thailand continued

a Japanese blockchain-based start-up, to initiate the National Digital ID project. This aims to build a national eKYC (electronic Know Your Customer) portal to encourage online transactions for both private and public sectors with more standardised methods of verification and authentication.[31] Thailand is expecting to see more of these private partnerships in the near future and to encourage involvement from all sectors.

### Singapore

In 2017, Singapore announced the creation of a new Data Innovation Programme Office to develop a private sector data portal similar to data.gov.sg – the one-stop portal for free government datasets. The private sector data portal will provide a secure platform for companies to share data in a way that allows them to seize opportunities in the digital economy. Data such as goods delivery schedules and consumer traffic in malls could provide valuable input into data analytics to help companies detect trends and patterns that could in turn be used to develop innovative products and services.

## 3.2 Regional cooperation

Digital identity is an example of a common, accessible agenda that can readily turn into shared goals for Asia Pacific's countries.[32] For example, working together on harmonising regulatory frameworks or systems for digital ID can introduce hassle-free travel, provide convenience for consumers and businesses, and enhance trust in the system. This concerted action can help governments reap the benefits that stem from digital identity and address the challenges of increasing cross-border data flows and of cybersecurity that constrain digital commerce between countries and regional trade.

### Regional cooperation

#### Asian Development Bank (ADB)

In a 2016 report, ADB outlined the importance of digital IDs for development as the "rapid growth of new technologies such as mobile phones, social media and the internet allows for many services to be offered online, both by the government and the private sector."[33] ADB also recommended that governments take a harmonised approach to managing national IDs and creating digital identities.

In December 2017, an ADB report provided an assessment of the potential and limitations of distributed ledger technologies (DLTs), such as blockchain, in five use cases, of which digital identity was one.[34] The report said, "the creation of verifiable digital identities is a gateway issue for pretty much every possible DLT use case". It cautioned, however, that three requirements – security, controllability and portability – must be in place to realise the potential benefits, and digital identity efforts may still need to be part of a broader reform agenda.

31 "ETDA Thailand initiates National Digital ID project to promote online transactions", OpenGov, February 2018

32 International organisations such as the OECD, World Bank and World Trade Organization have supported several digital identity initiatives. For example in 2011, a $195 million concessional credit was approved for the Identification for Enhanced Access to Services (IDEAS) Project to help the government of Bangladesh in developing a reliable and accurate national identification system.

33 Identity for Development in Asia and the Pacific, ADB, 2016

34 Distributed Ledger Technologies for Developing Asia, ADB, 2017

## Association of Southeast Asian Nations (ASEAN)

In November 2017, payment systems operators from five ASEAN countries signed a memorandum of understanding to enable real-time cross-border payments. Singapore and Thailand are already discussing connecting their national digital payment systems.[35] This would bring together two platforms, Singapore's PayNow and Thailand's PromptPay, which allow peer-to-peer transfers via banks and enable payments to be made using recipients' mobile phone or national identity card numbers.

## Australia and Indonesia

Part of Australia's $296 million economic partnership with Indonesia includes working together to pilot the use of digital governance and collaboration in e-government, online service delivery platforms, analytics and digital identity. In February 2018 at the inaugural Indonesia-Australia Digital Forum, the discussion centred on digital opportunities between business, research institutions and government.[36]

## eIDAS and the EU

In July 2014, EU member states adopted regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS).[37] The regulation came into force in July 2016 and aims to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. The eIDAS regulation ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.

In February 2018 in partnership with the European Commission and more than 10 other organisations, the GSMA completed the second phase of a Mobile Connect and eIDAS pilot. Its primary goal was to determine how Mobile Connect, in combination with eIDAS, can verify individuals' identities and their entitlements for access to cross-border health services. The trial's jointly issued report[38] provides a number of insights into operating within the eIDAS framework and recommendations as to how Mobile Connect can facilitate new services.

The GSMA estimates that eIDAS will create an addressable market for authentication, authorisation and attribute services of about $2.5 billion by 2022.[39] The pilot highlighted how leveraging Mobile Connect and the eIDAS Regulation, together with European member states' investment plans for identity initiatives, could drive large-scale take-up of secure and reliable digital identity management solutions beyond username/password and smartcard-based approaches. The completion of the pilot is an important step towards developing a strategic action plan for mobile operators' assets to accelerate the development of a secure and trustworthy digital identity ecosystem, which in turn could allow the delivery of healthcare and other public sector services enabled by IoT.

35 "Singapore, Thailand Weigh E-Payment Alliance in Digital Push", Bloomberg, October 2017
36 "Indonesia and Australia: Partners for the Digital Age", Australian Embassy, Indonesia, February 2018
37 For more information, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
38 Mobile Connect for Cross-Border Digital Services: Lessons Learned from the eIDAS Pilot, GSMA, 2018
39 https://www.gsma.com/identity/eidas

# 4 Benefits of digital identity

The benefits of well-developed digital identity programmes to the economy as a whole, to consumers and society, and to governments are well documented. Even in an individual country such as Australia or Indonesia, studies show a digital identity programme potentially increases GDP and leads to savings of billions of dollars. Digital commerce is a major driver of economic benefit, leading to increased convenience for consumers and job creation. Consumers also benefit by participating in a full digital lifestyle, including through better education and training via digital platforms. Society as a whole benefits: better healthcare and improved financial inclusion are just two examples. In developing countries, a digital identity is a prerequisite for achieving the UN's Sustainable Development Goals (SDGs). Digital government is crucial to achieving these benefits.

## 4.1 The economy

A 2016 report by the Australia Post and the Boston Consulting Group considered the economic opportunities of the Australian digital identity ecosystem, calculating that the annual "economic value of an accepted digital identity" in the country was $8 billion[40] through the following:

- reduced customer service costs from efficient self-service of face-to-face/phone verification and authentication
- reduced cost of fraud and reduction in other serious and organised crime
- improved consumer experience by reduced friction from multiple identity steps at checkout and added payment security, which increases usage and lifts revenue
- savings in consumers' time, reducing the opportunity cost of verifying, authenticating and managing their identities and filling in forms to apply for service.

### Positive macroeconomic effects

#### Australia

The Department of Industry, Innovation and Science released a consultation paper *The Digital Economy: Opening Up the Conversation* in September 2017, which includes an estimate that the use of digital technologies will contribute to Australia's GDP between AUD140 billion ($81 billion) and AUD250 billion ($196 billion) to 2025.[41] The paper focuses on:

- enabling and supporting the digital economy, focusing on key mobile technologies such as IoT
- M2M and real-time data analytics
- raising Australia's digital business capabilities, driven by mobile access and participation
- empowering all Australians through inclusion.

In parallel with this conversation, the Digital Transformation Agency of Australia released the first component of its Trusted Digital Identity Framework, ensuring users are able to safely and securely connect with government services online.[42]

#### Indonesia

An estimate of the potential impact of digital technologies in Indonesia suggests an increase in the country's GDP of $150 billion by 2025 and 3.7 million additional jobs.[43] The manufacturing and retail sectors, characterised by low adoption of technology and a high reliance on labour, stand to benefit the most from digitisation. This is to be achieved through increasing standardisation of supply-chain management and logistics processes from Internet of Things (IoT) and identity and tracking systems, on the one hand, and through increased digital payments, powered by mobile access and enabled by digital identity and transaction solutions, on the other hand.

For companies, consumers with digital identities can:

- increase efficiency through greater participation options in everything from integrated payroll and benefits to collaborative online workflow
- help focus marketing efforts
- become targets for highly personalised products.

A well-developed digital identity programme means that such benefits are not confined to any one specific vertical sector but occur across industries.

40 A frictionless future for identity management: A practical solution for Australia's digital identity challenge, Australia Post, 2016
41 Digital Australia: Seizing Opportunity from the Fourth Industrial Revolution, McKinsey & Company, 2017
42 https://www.dta.gov.au/what-we-do/policies-and-programs/identity
43 Unlocking Indonesia's digital opportunity, McKinsey, 2016

## 4.1.1 Digital commerce

CapGemini's World Payments Report 2017 estimates that *global* non-cash volumes of payment transactions will record a compound annual growth rate (CAGR) of 11% between 2015 and 2020, underlining the significance of digital commerce in society.[44] Much of that growth is driven by mobile commerce,[45] with consumers increasingly using contactless payment technologies, such as NFC, and businesses in many sectors enhancing the user experience of their digital services on mobile platforms.

According to the World Bank's Findex, the proportion of the adult population *in Asia* that made a digital payment increased from 35% in 2014 to 50% in 2017.

Research by Bain & Company discusses the considerable growth in number of digital consumers in the Southeast Asian countries of Singapore, Malaysia, Thailand, Indonesia, Philippines and Vietnam, bringing the value of this region's online economy to $50 billion in 2017.[46] The report estimates that the region now has 230 million "online engaged customers", i.e. users who have researched products and services online. This total is set to continue growing over the coming years. Google estimates that the total e-commerce market in Southeast Asia will reach $88 billion by 2025 (a CAGR of 32%) with the potential to climb to $120 billion over that time frame.[47] According to the Bank of Thailand, the value of e-payments via mobile phones surged from $765 million in Q3 2010 to $76.5 billion in Q3 2017.[48]

This promise of further rapid expansion presents attractive growth opportunities to those who can play a role in meeting the needs of online customers in the region. For these reasons, Singapore's central bank is encouraging commercial banks to switch to all-digital payments.[49] A cashless society will help restrict the shadow economy, increasing tax revenues and curtailing criminal activity. The Reserve Bank of Australia (RBA) plans to make Australia a largely cashless society by 2020, relying on the use of mobile platforms for digital commerce. The New Payments Platform (NPP),[50] supported by the RBA and 12 founding financial institutions, enables cheap, secure, 24×7 instantaneous payments. It works by establishing a PayID, which could be a mobile phone number, email address or business registration number, and linking that to the user's bank account so that payments can go through existing online and mobile banking apps, or through other new apps that will take advantage of the platform. In many ways PayID acts as the logical extension of an economy that already relies heavily on mobile payments – from tap-and-go, to BPAY, to Apple Pay.

Multilateral trade agreements can further accelerate the development of such initiatives by facilitating interoperability between national systems and aligning, or harmonising, regulatory requirements. The benefits that could emerge from interoperability across data flows, financial transactions, identity and commerce have been recognised in the recently concluded Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Of the eight countries under review, four – Australia, Japan, Malaysia and Singapore – are signatories.

### CPTPP

Among the CPTPP's objectives lies a core purpose to develop the seamless flows of goods, services and investment regionally, with a particular focus on data and electronic commerce. This means methods by which to move people, products, services and money must accelerate among the CPTPP's 11 signatory countries of Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam. For example, according to Viet Capital Securities research, Vietnam's domestic and foreign-invested firms are expecting an increase in exports from the CPTPP.[51] Research shows that there is a high compliance cost to non-tariff barriers – the time and money to process border clearance. A trusted identity system that works across the CPTPP member countries will alleviate much of the bottleneck.

44 https://www.worldpaymentsreport.com/#non-cash-payments-content
45 I.e. electronic transactions performed on mobile phones.
46 "Digital economy takes off in Southeast Asia as the number of connected consumers surges 50 percent in the last year to 200 million", Bain & Company, May 2017
47 "e-conomy SEA: Unlocking the $200B Digital Opportunity", Google and Temasek, May 2016
48 See PS PT 012: https://www.bot.or.th/English/Statistics/PaymentSystems/Pages/StatPaymentTransactions.aspx
49 "Singapore wants to be Asia's Sweden in push for cashless payment", Bloomberg, August 2016
50 "Real time payments system delayed to 2017", The Australian Financial Review, December 2014
51 "World Bank assesses impacts of CPTPP on Vietnam's economy", VietCapital Securities, March 2018

In addition, enabling interoperability of the identity and payment trust systems of, for example, Singapore's PayNow system and Australia's similar mobile number payment system would expedite peer-to-peer transactions and reduce the time it takes for businesses to get paid, including across borders.[52]

## Enabling commerce and payments with mobile identity solutions

### Pakistan

In 2015, Easypaisa, the mobile money joint venture between Telenor and Tameer Microfinance, launched its online payment gateway, allowing e-commerce platforms to accept digital payments and integrate through a set of APIs and plugins.[53] In addition to allowing the use of credit and debit cards, e-commerce platforms that integrate the use of Easypaisa allow buyers one of three options to settle their online purchase: virtual or physical prepaid companion cards issued against the mobile wallet account balance; the Easypaisa mobile wallet account; or cash at an Easypaisa agent.

Due to a lack of secure digital supply-chain records, Pakistan has a high fraud rate for 'cash on delivery' transactions as there is no way to know where a product went missing nor any way to receive confirmation of delivery. Mobile-identity authorisation could be used for cash on delivery: a SIM registered against a government ID could authorise receipt of goods along the supply chain. In this way, mobile identity solutions provide assurance to the e-commerce retailer and to the consumer that the transaction has been completed.

In January 2017, MasterCard and Pakistan's NADRA announced a partnership to allow citizens to use national identity cards to conduct financial transactions, to receive government payments, and to send and receive domestic and international remittances.[54] Although the two parties suspended this partnership for security reasons and lack of proper authorisation, talks in October 2017 suggest that they may revive it.[55]

### Malaysia

Malaysia's MyKad identity card can be used as a driving licence, ATM card, e-wallet and loyalty card. The e-wallet service allows users to top up their MyKad to make purchases of up to $500 (MYR2,000), or for Touch 'n' Go services to pay for road tolls and public transport.[56] Users who register their MyKad with MyKad Smart Shopper can enjoy Cash Points and Reward Points when they shop at any of MSS's participating merchant outlets by verifying their registered MyKad during payment. Participating merchants include Hotel Seri Malaysia and online merchants including Lazada, hotels.com, airasiago.com and Zalora.

52 "Australians to transfer money using only mobile number or email in 2017: RBA", ZDNet, September 2016
53 Unlocking the digital potential of Pakistan's e-commerce industry, GSMA, 2018
54 "Mastercard helps expand financial inclusion in Pakistan by optimizing National ID cards with e-payment functionality", Mastercard, January 2017
55 "NADRA Likely To Revive Money Transfer Accord With MasterCard", ProPakistani, October 2017
56 "5 Things You Didn't Know You Can Use Your MyKad For", Lite

## 4.2 Consumers

The combination of smartphone technology and digital identity enables people to transform the way they work, communicate and play, participating in a full digital lifestyle. According to GSMA research, mobile phone ownership, supplemented with internet access, is associated with an improvement in peoples' lives, as shown by increases in average life evaluations and net positive emotions.[57]

The smartphone is still the hub of an individual's digital experience,[58] and is the one device that people have with them at all times. Its increasing functionality, such as embedded sensors for biometric identification, and the expanding apps ecosystem make it a suitable medium for interacting with a variety of services and processes with real-time verification.

Trust is cited as a key barrier to adoption of e-commerce. For consumers, trust relates to a number of aspects of being online; security of a personal identity or fear of identity theft are major factors. Service providers fear the risk of fraudulent transactions: this barrier can be addressed by increasing trust in the robustness of the consumer identity provided.

### Enriching lives and lifestyles with digital services enabled by a digital identity

#### Bangladesh

Mobile operator Banglalink provides education services via Education Portal, MegaMind and MEDU to subscribers. The mobile phone number functions as the unique identity for users to subscribe to the services. Education Portal provides access to information on SSC, HSC, university admission, test preparation and exam queries, with a subscription fee of $0.0024 (BDT0.20) per day. MegaMind is an m-learning platform using SMS and IVR for knowledge sharing. MEDU provides general knowledge, exam tips and career counselling via SMS, IVR and WAP.[59]

#### Indonesia

Jakarta is notorious for its heavily congested streets where commuters typically spend 3–4 hours per day in traffic jams. Looking to address this challenge, the Jakarta city administration, since 2014, has worked with various mobile app providers, including Google Waze, to provide real-time information and updates to commuters on public projects, ongoing construction and planned events including road closures and repairs.[60] Waze is a community-based crowdsourcing traffic and navigation app where registered users can share and submit information on traffic with one another through a live map, and share local events, street fairs or real-time fuel prices. Using crowdsourced data from users, Waze communicates the information to the city administration to then take the necessary steps to alleviate congestion.[61] Waze is able to provide accurate and constantly updated traffic information for drivers to best plan their travel. A recent addition is identifying navigation routes based on Indonesia's odd/even licence-plate policy, enabled by entering the last two digits of a vehicle's number plate.[62]

#### Malaysia

Malaysian telco Digi's Video Freedom offers customers the option of purchasing hourly or daily passes to stream video content on their device for less than MYR5 without it counting towards their internet allowance. Digi works with both international and local partners including YouTube, iflix, Viu, Astro Go, Netflix and Twitch.

57 GSMA-commissioned survey in 142 countries: The Impact of Mobile on People's Happiness and Well-Being, GSMA, 2018

58 The range of mobile devices has surged over the last decade on exponential growth of apps and cloud-based services and includes mobile phones, tablets and wearables (e.g. smart watches).

59 Unlocking the digital potential of Pakistan's e-commerce industry, GSMA, 2018

60 "Jakarta Joins Forces With Waze on Traffic Updates", JakartaGlobe, November 2014

61 "Indonesia: Jakarta city authorities to work with Waze", Telematics News, November 2014

62 "Waze to adapt navigation to Jakarta's odd-even license plate policy", The Jakarta Post, August 2017

## 4.3 Society

The social benefits from digital identification of individuals are extensive and include wider access to healthcare, education and financial services.

### 4.3.1 Achieving universal healthcare

Identification is necessary for a medical practitioner to administer the appropriate medication and level of care based on a patient's health records and medical history, while an individual's access to state subsidies also hinges on the ability of healthcare providers to verify eligibility. The digital aspect of identification is necessary to improve the quality of healthcare by allowing such information to be shared across public and private institutions via electronic health records, and will be a crucial building block in any country that wants to implement a universal healthcare scheme.

Digital healthcare is also receiving urgent attention from Asian governments for its potential to fill chronic shortages of hospital beds and healthcare professionals. Indonesia, for example, had just 0.2 physicians and 0.9 hospital beds per 1,000 people in 2012.[63] The World Health Organization (WHO) predicts that by 2030, there will be a global shortage of 18 million healthcare professionals.[64] Remote monitoring and real-time video or voice conferencing are examples of how digital healthcare can maximise the effectiveness of the healthcare system without demanding further labour resources from medical practitioners; digital identification is central to the provision of digital healthcare services. At the same time, however, sharing medical records heightens privacy concerns, which we consider in Chapter 5.

### Singapore

The Ministry of Health's HealthHub is a one-stop online portal for Singapore citizens and permanent residents who can log in to check their latest health records, make appointments at public healthcare facilities, and access personalised information "to lead a healthier lifestyle". HealthHub is available via web and mobile app, and can be accessed by logging on to the national digital authentication system, SingPass. The Integrated Health Information Systems (IHiS), a subsidiary of the Ministry of Health, is in charge of developing and implementing innovative technologies in the healthcare sector. Key initiatives include: 1 Queue 1 Payment (1Q1P), an integrated queue and payment system that optimises patients' appointments and payments. The Outpatient Pharmacy Automation System enables pharmacies to handle high prescription loads safely and efficiently, and the Smart Health Video Consultation system, which leverages video conferencing technology, enables remote consultations.[65]

63 https://data.worldbank.org/indicator/SH.MED.BEDS.ZS?locations=ID
64 Global strategy on human resources for health: Workforce 2030, WHO, 2016
65 See IHiS: www.ihis.com.sg/Project_Showcase/Healthcare_Systems

## 4.3.2 Delivering greater financial inclusion

Combining digital identity with mobile technology can change the landscape of financial inclusion. According to the World Bank's Global Findex, in 2017, 1.7 billion adults globally were unbanked.[66] In Southeast Asia, the proportion of the adult population with an account at a financial institution or a mobile money account increased from 60% to 71% between 2014 and 2017. However, more than 850 million adults are still financially excluded. By contrast, more than 83% of the world's population have access to 3G mobile connectivity, and two thirds have access to 4G.[67]

Non-banks, such as mobile operators, are playing a key role in Asia, facilitating digital payments and user authentication, and accelerating the digital commerce ecosystem through partnerships with service providers and financial investments. For example, there are now more than 235 million registered mobile money accounts in South Asia, representing a third of registered mobile money accounts globally.[68]

### Financial inclusion

#### Bangladesh

In June 2015, Bangladesh announced it had joined the Better Than Cash Alliance to accelerate its transition from cash to digital payments.[69] In addition to driving e-commerce, this will support greater financial inclusion by digitising social welfare payments to citizens, fees that citizens make to the government for services, and domestic and international remittances. The agency in charge of this, Access to Information (a2i), is using mobile phones to connect unbanked citizens to financial services. For example, a2i has partnered with bKash, a mobile financial service provider, to allow rural customers to deposit cash or send money using text messages.[70]

#### Pakistan

In Pakistan, mobile money providers (or 'branchless banking' service providers) are extending the reach of mobile financial services to people outside the traditional banking system. By the end of 2014, 9 million people, representing 7% of Pakistan's adult population, had used peer-to-peer (P2P) transfers or bill payment services offered by branchless banking operators at least once. As well as P2P transfers, the industry has delivered various government-to-person (G2P) campaigns such as the Benazir Income Support Programme and Internally Displaced Persons payments, with the total value of transactions equivalent to 3.5% of the country's GDP.[71]

66 http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf#page=3
67 The Mobile Economy 2018, GSMA, 2018
68 2017 State of the Industry Report on Mobile Money, GSMA, 2018
69 "Making Digital Bangladesh Vision 2021 a reality, Government joins the Better Than Cash Alliance", Better Than Cash Alliance, June 2015
70 "Seriously, Bangladesh is the country to beat on e-payments", GovInsider, May 2017
71 Building digital societies in Asia: Making commerce smarter, GSMA Intelligence, 2015

## 4.3.3 Providing identities for refugees

The United Nations High Commissioner for Refugees (UNHCR) estimates that there are more than 65 million forcibly displaced persons (FDPs) worldwide.[72] FDPs are less likely than other migrants and foreign nationals to possess proof of identity, which may have been forgotten, lost, destroyed, stolen in transit, or purposefully left behind.[73] FDPs face identity-related barriers that contribute to instances of exclusion and limit their access to mobile connectivity, financial services, education, healthcare and employment.

Mobile providers can leverage unique resources to make registration processes more secure and efficient, improve cross-organisational data sharing, and establish digital identities for verification anytime, anywhere. This presents new opportunities to work with humanitarian agencies to better understand the needs and potential of refugee populations and the obstacles they face in using mobile services. Such partnerships can also lead to positive outcomes for host governments and local communities due to reduced reliance on state resources, reduced risks of financial exclusion, strengthened financial integrity, and increased economic activity in local host communities.[74]

### Proving identities for refugees

#### UNHCR

Collaboration between the UNHCR and other humanitarian organisations has led to the development of the KoBo Toolbox, a free, open-source tool for mobile data collection that allows organisations to collect refugee data in the field using mobile phones or tablets.

#### Malaysia

In Malaysia, the UNHCR has begun issuing photo ID cards for scanning and verification using a free mobile app called UNHCR VERIFY-MY. The app allows law enforcement officials and other authorities engaged in UNHCR's protection work to scan a Quick Response (QR) code on the back of the ID and visually verify the cardholder against the personal details and photograph displayed on the mobile device's screen.

An immediate application of this solution became apparent in 2016 during the onset of the Rohingya refugee crisis. With increasing numbers of Rohingya seeking sanctuary in Malaysia, UNHCR issued the new biometric identification cards to combat identity fraud and the use of counterfeit documentation.

72 http://www.unhcr.org/uk/figures-at-a-glance.html
73 Refugees and Identity: Considerations for mobile-enabled registration and aid delivery, GSMA, 2017
74 Ibid.

### 4.3.4 Supporting the UN's Sustainable Development Goals (SDGs)

The GSMA and mobile operators are united in support of achieving the UN's 17 SDGs in Asia Pacific where 850 million people (or 20% of the population) are estimated to be unregistered, including 65 million children under the age of five.[75] Given its high levels of global penetration and high population coverage, mobile technology has the potential to act as a conduit for trusted and robust digital identity solutions for the underserved, contributing to the delivery of SDG 16 (Peace, justice and strong institutions).

#### Supporting the SDGs – legal identities for all

**Pakistan**

Telenor Pakistan, in partnership with UNICEF, has developed a mobile solution to digitally register births. Birth registration details are reported through authorised community members such as health workers and marriage registrars, or through Telenor Pakistan's agent network using an Android app. The collected data automatically populates a web-based dashboard, providing government ministries with real-time information on reported and registered births and up-to-date information on the status of each application.[76]

**Indonesia**

Since 2015, child development organisation Plan International has been working with the Ministry of Home Affairs (MoHA) to identify ways to increase the coverage of birth certificates in Indonesia.[77] As part of the Medium Term Development Plan 2015-19, Indonesia's president has set a target of 85% of children to have a birth certificate by the end of the period. One social protection programme is therefore using a mobile app to complete birth registration and marriage certification. SIAK, MoHA's population database, validates the application using the unique ID numbers of the parents, which then triggers the creation of an identity card number as well as a birth certificate for the child.

## 4.4 Government

As government activities become more digitised, digital citizenry – including the need for individuals to prove their identities digitally – increasingly becomes a prerequisite for effective societal participation. Government actions determine the benefits of digital inclusion and the adverse consequences of digital exclusion.[78]

Digital identities can create an opportunity for the state to broaden the revenue base – a critical need in many developing countries – by bringing previously undocumented citizens and informal businesses into the 'tax net', and by increasing trust in public services administration among citizens through improved transparency, accountability and communication of government activities and expenditure. In the formal sector, digitising linked invoices for sales taxes such as VAT and GST via, for example, blockchain technologies has the potential to eliminate missing trader fraud – one of the world's largest sources of tax fraud and one of the biggest causes of lost government revenue.[79]

From an individual's perspective, a digital identity acts as a gateway to enable faster and easier interaction with the state, which, when underpinned by the existence of a secure legal framework incorporating appropriate checks and balances, also helps address concerns over privacy when accessing sensitive material, such as medical or tax records.

75 World Bank ID4D
76 Innovations in mobile birth registration: Insights from Tigo Tanzania and Telenor Pakistan, GSMA, 2017
77 Birth registration for all in Indonesia: A Roadmap for Cooperation, Plan International, 2016
78 Governments also need to address the potential side effects of exclusion. As more services become available online, there is a need to support digital literacy, including for senior citizens in developed countries. Singapore, for example, has recognised this need as one of the pillars of its Smart Nation programme.
79 See, for example, A VATCoin Solution to MTIC Fraud: Past Efforts, Present Technology, and the EU's 2017 Proposal, Boston School of Law, 2018

## E-government services

### Bangladesh

Bangladesh is connecting 18,500 government offices and creating a mobile-optimised, integrated service delivery platform, supported by Access 2 Information (a2i). An example of this programme is the Department of Environment's Environmental Clearance Certificate Application System, which anyone can access anywhere at any time. The entire processing system can be tracked, and when the certificate is ready, a notification SMS and email are sent with the address of the office for collection. As a result, 200% more applications were submitted within seven months of launch. Alongside this is a Digitizing Implementation Monitoring and Public Procurement project to place government procurement online.[80] As part of its 7th Five Year Plan (2016–2020), the government set a target of increasing public institution usage of e-procurement from zero in 2014 to 100% by 2020.[81] Such an increase would enable the government to realise cost savings of up to 13.5% in public good provision.[82]

### Indonesia

Since 2014, citizens in Jakarta have used the Qlue app to provide feedback to the city government.[83] Through their mobile phones, citizens can take pictures, upload photos and report a problem to the government, which in turn forwards the case to the relevant local authorities to follow up. Users can monitor the progress and status of their report, while officials also upload a photo of the reported location once they complete their response.[84] The service has now expanded to six other cities in Indonesia.

### Malaysia

Public sector transformation using ICT is laid out in the Public-Sector ICT Strategic Plan (2016-2020), which targets the transformation of public service delivery by 2020. Spearheaded by the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), the plan outlines key goals on digital, data, cloud and cyber security. Certain government services will be offered only digitally, with the expectation that the vast majority of access will occur via mobile, from citizens with IDs able to access the services. The government also intends to enable and promote online payments, with 19 agencies to offer mobile payments by 2020. MAMPU will look to encourage broader use of data in government, with analytics to improve digital delivery, and a dedicated platform built for government agencies to share data and internal service access with each other.[85]

### Singapore

In Singapore, the Digital Readiness Programme Office is helping citizens access various government services digitally. Online services include a revamped SingPass, which uses two-factor authentication via mobile phone to authenticate access, a digital vault MyInfo for storage of personal details so users need not repeatedly provide and verify their personal information when transacting online,[86] and the eCitizen portal for access to all e-government services and transactions in a secure manner.[87] To date, 1,600 government services have been made available digitally.

80 "Big bucks for ICT to boost Digital Bangladesh plan", theindependentbd.com, June 2017
81 Seventh Five Year Plan, FY2016 – FY2020, General Economics Division (GED), Planning Commission, Government of the People's Republic of Bangladesh, 2015
82 Birth registration for all in Indonesia: A Roadmap for Cooperation, Plan International, 2016
83 "Open Data Brings Change to Indonesia", World Bank, January 2017
84 "Monitoring app Qlue helps Jakarta improve services, efficiency", The Jakarta Post, May 2016
85 The Malaysian Public Sector ICT Strategic Plan 2016-2020, Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)
86 "All SingPass users to be auto enrolled in digital data vault MyInfo by year end", The Straits Times, February 2018
87 For more information, see www.tech.gov.sg/-/media/GovTech/Media-Room/Media-Releases/2014/11/SingPass--Factsheetpdf.pdf

# 5 Building individuals' trust in the digital world

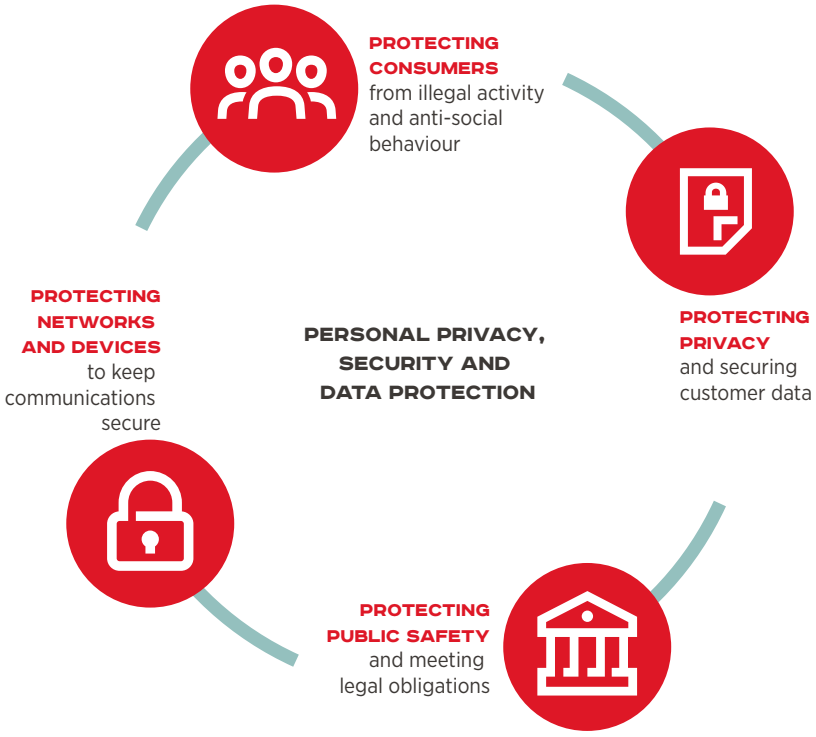
Trust is crucial if citizens are to adopt digital identity services. Privacy, security and data protection are essential to maintain and ensure citizens' trust, but it is important to balance the protection of personal and sensitive data with the free flow of information that a digital economy demands. Equally, cybersecurity is essential but policymakers must ensure that the adopted measures have the least impact on the digital economy necessary to achieve their intended results.  Failure to do so risks impairing the achievement of the benefits quantified earlier.

## 5.1 Privacy, security and data protection

Increasingly, the reasons cited by citizens for inactivity online include security and privacy concerns. Properly designed privacy and security safeguards will help gain citizens' trust, while ensuring that the flow of data is sustained, whether at the national level or across borders. Privacy, security and data protection interact, as shown below.[88]

**Figure 2**

### The interaction of privacy, security and data protection




**Source:** GSMA

### 5.1.1 Privacy

When Cambridge Analytica allegedly accessed personal data from millions of Facebook users to target them for political campaigns, the need to act to protect privacy of data became front-page news.[89] The personal attributes collected in identity registration processes, or used in identity authentication processes, represent the type of information that data protection and privacy policies, laws and regulatory agencies need to protect – and which citizens expect they will protect.

In Asia Pacific, of the 50 countries that mandate SIM registration, only 22 have a data protection and/or privacy framework; 22 do not have a framework; and six are considering implementing one.[90] Of the eight countries under review in this report, Bangladesh does not have a data protection/privacy framework, and Indonesia and Thailand are considering implementing data privacy frameworks.

It is important that privacy and data protection rules strike the right balance between protecting consumers and encouraging the development of a digital society. Privacy and data regulations can be considered in line with best practice when they adhere to the following:[91]

88 Safety, privacy and security across the mobile ecosystem: Key issues and policy implications, GSMA, 2017
89 It is claimed that Cambridge Analytica, a UK-based consultancy, acquired data on millions of Facebook users and their friends, which was utilised in targeted political ads in the UK's EU referendum campaign, as well as by President Trump's team in the 2016 US election campaign.
90 Access to Mobile Services and Proof-of-Identity: Global policy trends, dependencies and risks, GSMA, 2018
91 Mobile Privacy Principles: Promoting consumer privacy in the mobile ecosystem, GSMA, 2016

- Based on principles which provide openness and transparency, offer user choice and control, guarantee data minimisation and retention, respect user rights, adopt appropriate security measures, and protect children and vulnerable individuals.
- Based on the risk of harm to consumers – ensuring the data is used only for its original purpose, implementing security measures such as pseudonymisation[92] and encryption.
- Sector and technology neutral – the same data privacy rules should apply to the same service whether provided by a mobile operator or an OTT player. IoT services should be covered by general data privacy laws.
- Innovation and investment friendly without being too prescriptive.

## 5.1.2 Cross-border data flows

Cross-border data flows have grown 45 times in volume since 2005.[93] Privacy regulation should therefore be light on restrictions of such flows as these benefit consumers, the economy and society. However, some countries such as Indonesia and Vietnam have set cross-border restrictions on data delivery, storage and processing, which prevents firms moving their citizens' data to a jurisdiction the government interprets to be less strict regarding privacy and security. Countries often impose these rules on the belief that supervisory authorities can more easily scrutinise data that is stored locally, or that the privacy and security standards of a country can only be enforced if the data stays in that country.

Data localisation and data sovereignty requirements have the potential to negatively impact growth, foreign direct investment, social development and economic productivity.[94] A way forward is for privacy and data protection frameworks to be based on internationally recognised principles, as this can mitigate risks without restricting data flows and the benefits they bring. Such high-level alignment increases trust between countries and allows a coordinated approach. In Asia, there are two main privacy frameworks: the ASEAN Privacy Framework and the APEC Privacy Framework and its accompanying systems. While these two frameworks already share many of the same principles, further formal integration and harmonisation of their respective approaches could help countries in Asia Pacific more fully and broadly bridge data protection gaps and reduce inconsistencies across privacy regimes. The GSMA has commissioned a study to consider these privacy frameworks – at both the regional and national levels – with the objective to identify specific steps that can be taken to support the evolution and convergence of privacy frameworks in Asia. The findings from this study will be published in September 2018.

## 5.1.3 Cybersecurity

In light of high-profile cyber security incidents (such as the $81 million Bangladesh Bank cyber-attack in 2016), a cybersecurity framework is required to instil trust among users and deter cyber criminals. While governments have a legitimate interest in ensuring cybersecurity, it is important that cybersecurity does not become an impediment to the development of a digital society.

92 Pseudonymisation is a procedure for replacing personally identifiable information with one or more artificial identifiers or pseudonyms
93 Digital Globalization: The New Era of Global Flows, McKinsey Global Institute, 2016
94 Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?, ITIF, 2017

## 5.2 New technologies for privacy and security

New technologies such as distributed ledger technology (DLT), commonly known as blockchain, may help to allay security concerns via their decentralised structures that are difficult to hack or alter.[95] In contrast to attacks on centralised corporate or government systems, which go undetected for an average period of seven months,[96] Keyless Signature Infrastructure (KSI) and similar DLTs provide instantaneous alerts of any breach.

Thailand is planning to implement a KSI technology in its digital ID programme. Similarly, the Financial Services Agency of Japan and three major banks are developing a shared identification system based on blockchain technologies where customers will only need to register once and have their personal data stored and administered on blockchain. They can also use the same account across all participating banks and financial institutions.[97] Likewise, the Philippines has several proofs of concept to use blockchain to streamline the handling and issuance of local business permits[98] – a government priority to reduce red tape in, for example, rolling out rural telecommunications infrastructure. From a small base, the blockchain industry is growing rapidly, with projections of an 80% CAGR over the next four years to $8 billion in size, with Asia Pacific showing the fastest regional growth in blockchain use.[99]

Digital economies increasingly rely on artificial intelligence (AI) and machine learning to deliver value by analysing huge amounts of data from online transactions. To target advertising, AI algorithms of companies such as Facebook and Google rely on individuals' private data that, when compiled and tracked over time, can constitute part of an individual's digital identity or help identify an individual through their digital footprints. Thanks to vast stores of data and relatively few constraints on the collection and use of private or personal information, China has become the clear leader in Asia Pacific for AI applications. Apart from compiling a nationwide database of individual credit scores based on personal data from firms required to share it, the Chinese government even allows the monitoring of workers' thoughts: government-backed projects are using brain-reading technology to monitor changes in emotional states of soldiers, employees on production lines and drivers of high-speed trains.[100]

95 Because it is not possible to delete data from a blockchain, to conform with the EU citizens' "right to be forgotten", personal data may need to be stored via links, off chain, or via other technical means.

96 Estonian blockchain technology: FAQs

97 "Japan developing shared ID system for banks", Nikkei Asian Review, September 2017

98 "Digitalization of government", Business World, February 2018

99 "Blockchain Market by Provider, Application (Payments, Exchanges, Smart Contracts, Documentation, Digital Identity, Supply Chain Management, and GRC Management), Organization Size, Industry Vertical, and Region - Global Forecast to 2022": Research and Markets, 2017

100 See, for example, 'Forget the Facebook leak': China is mining data directly from workers' brains on an industrial scale, South China Morning Post, May 2018.


# 6 Countries in Asia Pacific on the digital society path

Digital identity is the cornerstone of a digital economy: analysing digital identity in detail only makes sense in the context of an assessment of the progress made by the countries identified towards a digital society. Countries with a strong digital identity enabler score perform better on the digital society path, but generally all countries surveyed have improved their scores compared to the 2016 GSMA Digital Societies Report.

For each of the eight focus countries, we have updated the index from the previous report[101] to look at the progress they have made along the digital society path. The digital society index has four components:

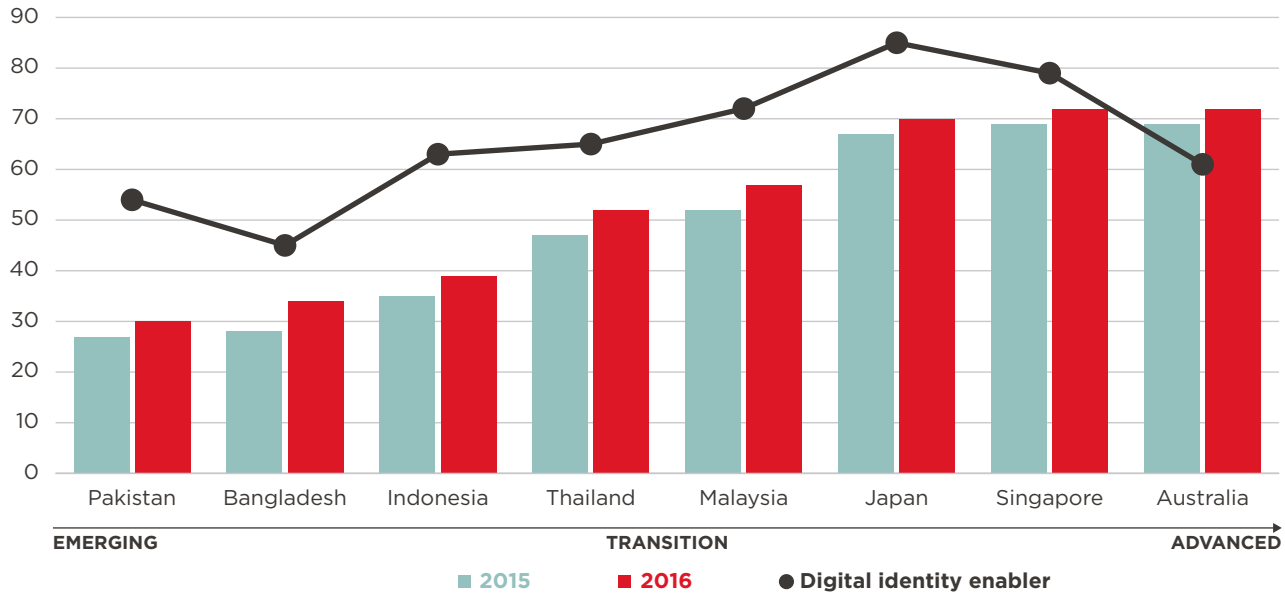
- connectivity
- digital citizenship
- digital lifestyle
- digital commerce.

In light of the focus of this report, we plot the "digital identity enabler" score, which is a measure of the availability and usage of identity and digital identity,[102] against connectivity and each of digital lifestyle, digital citizenship and digital commerce. As can be seen from Figure 3, aside from Australia, which is in the process of developing a digital identity system, the countries with the highest digital-identity enabler scores are performing better along the digital societies path.

Looking at the overall digital societies score,[103] in general, all countries have increased their scores between 2015 and 2016. Bangladesh and Pakistan increased their scores the most, with 21% and 13% improvements, respectively. Bangladesh had the second highest increase in digital identity, after Thailand.

**Figure 3**

## Digital society: country index scores




**Source:** GSMA Intelligence

The provision of digital identity is causal in promoting digital activity. Governments that have focused on either provisioning digital identity as a means of driving digital economy development (Indonesia, Thailand) or uniting various identity-enabled programmes (Japan, Singapore) have witnessed corresponding increases in their digital society scores. The increase in digital society scores reflects the increasing ubiquity of access that interoperable national ID has enabled.

By contrast, Australia and Pakistan provide evidence of a lag in uptake that can result from the lack of a well-deployed national digital ID system. As well as they have performed in developing their overall digital society environments, we find both empirical and anecdotal evidence of how much better those results could have been through a more widely available or coherent national ID programme.

101 Advancing Digital Societies in Asia, GSMA Intelligence, 2016

102 Digital identity enabler score is measured in terms of whether there is a national identity system in the country and how many people are actually registered. Additionally, it looks at digital identity, in particular if people use it to access online services and if there is a data protection and/or privacy framework in place.

103 Different sources have been used to calculate the overall digital societies index and each of its components. These include data from the UN, World Bank, WEF, IMF, GSMA Intelligence and GSMA Mobile Connectivity Index. See Appendix B for a full methodology and sources used.

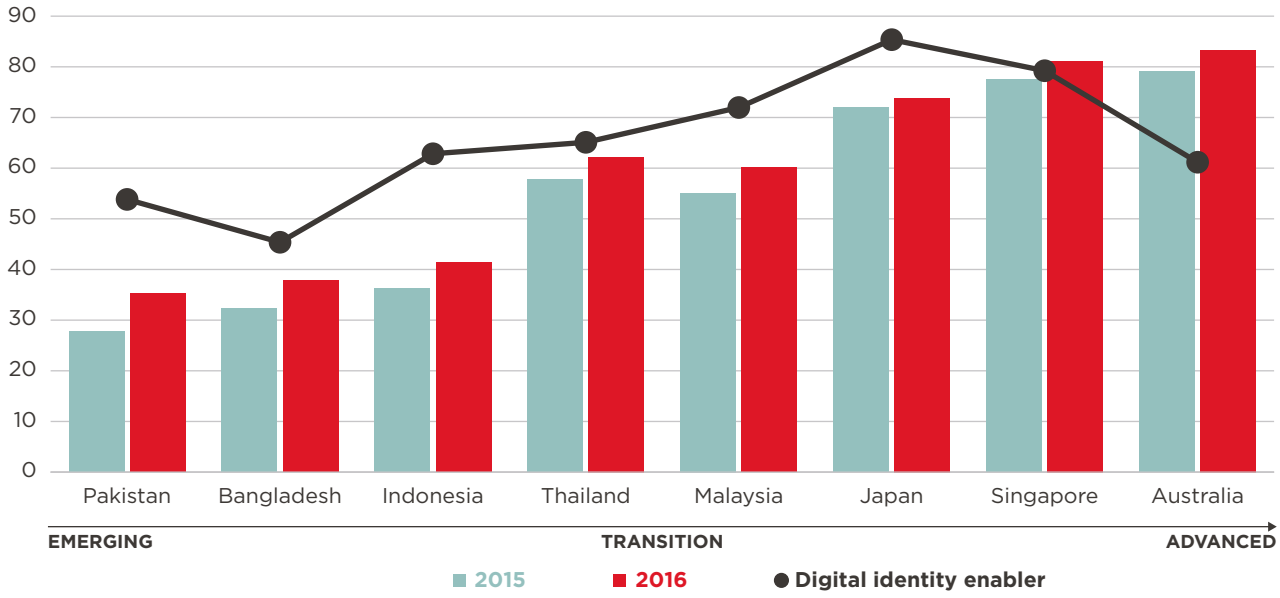
## 6.1 Connectivity

In most Asian countries, mobile is the main technology used to access the internet. The availability of high-speed network coverage is fundamental to developing a digital society and is therefore reflected in the connectivity component of the index. Pakistan has had the highest score increase, at 27%. This has been driven by improved network quality – particularly lower latency and greater coverage.

Countries towards the left-hand side of the digital society chart tend to have limited availability of spectrum, and limited population coverage, particularly 4G, resulting in slower download/upload speeds. These are fundamental issues to address when trying to move towards an advanced digital society.

Figure 4

### Connectivity: country index scores



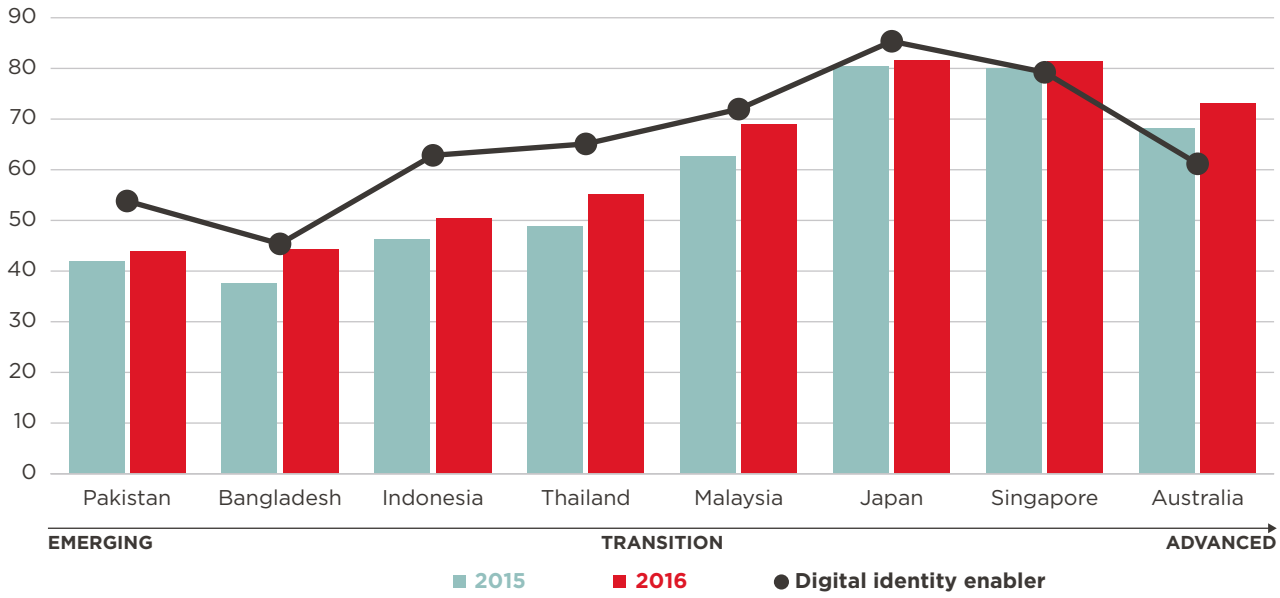

**Source:** GSMA Intelligence

## 6.2 Digital citizenship

Citizens need to have an identity to be able to access and fully utilise government services. Digital identification is therefore a prerequisite of digital citizenship. The digital citizenship component measures both the state of the identity system and the availability, richness and pervasiveness of e-government services.

**Figure 5**

### Digital citizenship: country index scores




**Source:** GSMA Intelligence

Of our eight focus countries, Pakistan and Bangladesh have the lowest digital citizenship scores. Among the focus countries, Pakistan has the lowest share of population registered and has seen one of the lowest increases in the digital identity enabler between 2015 and 2016. Bangladesh, by contrast, has seen the strongest growth in digital citizenship. The increase was mainly driven by the importance the government associated with increasing e-government services: Bangladeshis are today receiving more than 200 services from more than 4,500 Union Digital Centres. Also of note is the increased focus on the provision of digital identity and the delivery of services using identity. Even with a lower absolute digital identity enabler, Bangladesh has surpassed Pakistan in terms of digital citizenship. Bangladesh's score is still comparatively low because of the limited use of e-government services and, most importantly, the lack of a data protection and privacy framework.

Aside from Australia, which is in the process of developing a digital identity system for rollout in 2018,[104] all countries have some form of national identification system. As of 2017, however, there were still more than 170 million unregistered people in the eight focus countries – the majority in Pakistan, Bangladesh and Indonesia.[105] Some systems provide greater sophistication, allowing access to multiple e-services and digital signature, such as in Japan and Malaysia, while some are relatively less advanced but still allow access to certain e-services, as is the case in Indonesia and Pakistan. To move along the digital society path, it is important not only to make e-government services available, but also to ensure that citizens have the necessary level of digital literacy to use and access these services.

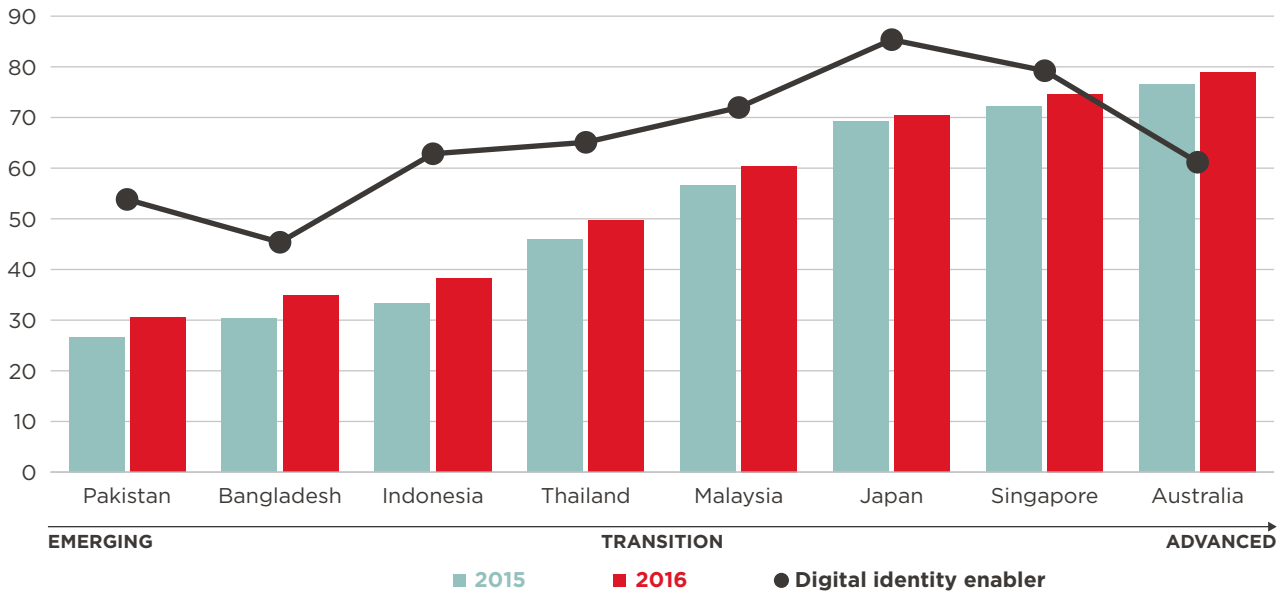
104 For more information, see ttps://www.dta.gov.au/what-we-do/policies-and-programs/identity/
105 World Bank ID4D Database

## 6.3 Digital lifestyle

The digital lifestyle index component looks at access to and use of smart devices together with the advancement of IoT and availability of local content. IoT has taken off in advanced countries, and we see it gaining momentum in emerging and transition countries too. In fact, GSMA Intelligence forecasts that the total number of IoT connections (cellular and non-cellular) globally will reach 25.2 billion in 2025, with Asia Pacific accounting for 44% of connections. The global IoT market will be worth $1.1 trillion in revenue by 2025, with Asia Pacific generating 35% of this.[106] For this economic value to be captured, and for the possibilities of data analytics to be fully enabled, frictionless identification across networks becomes an imperative, both for governments and industry.

Figure 6

### Digital lifestyle: country index scores




**Source:** GSMA Intelligence

Bangladesh and Indonesia have seen the highest score increases, followed by Pakistan. This has been driven by an increase in adoption of smartphones and other connected devices. However, all three countries are still in the high growth phase for smartphone adoption, and are relatively nascent in terms of availability of IoT compared to other countries.

Availability of local content is another important aspect for countries to move along the digital society path. If users have the means to access different solutions, but the content is limited or not relevant to them, adoption and the use of more advanced services will lag. For example, in emerging and transition countries, the number of apps developed per internet user is low compared to more advanced countries. Even if apps are available, they are not always in the most commonly spoken language, making it more difficult for people to access them. Basic literacy, and digital literacy in particular, is low in South Asia.

106 IoT: the $1 trillion revenue opportunity, GSMA Intelligence, 2018

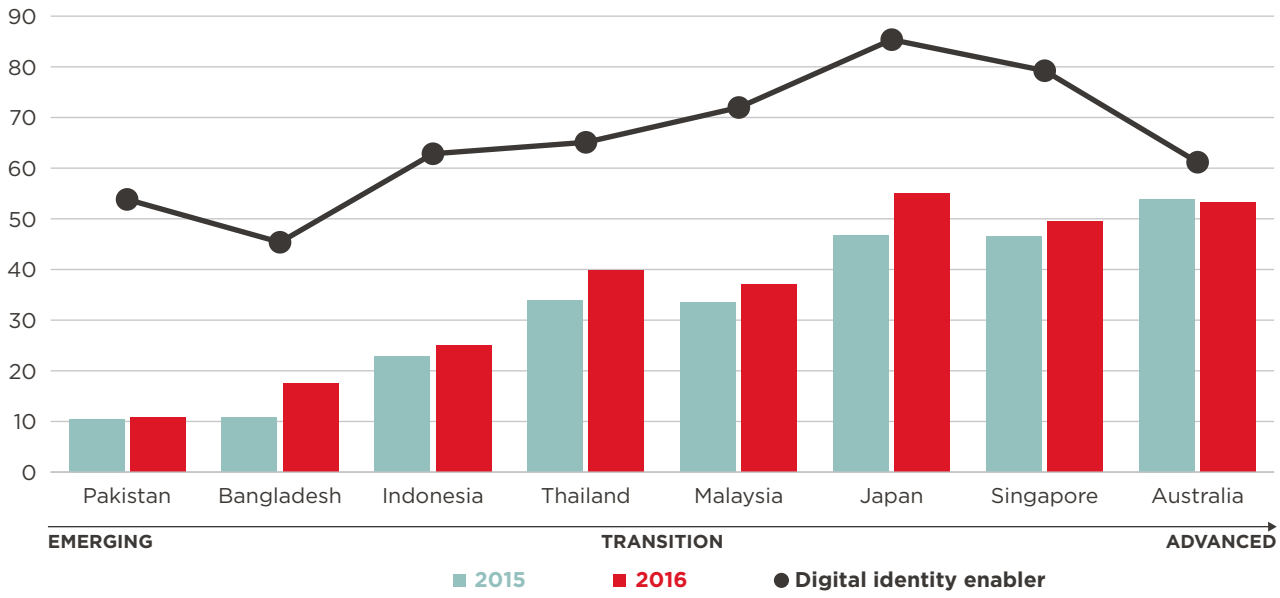
## 6.4 Digital commerce

Digital commerce (access to marketplaces, services and payments replacing physical cash) is an essential element of a digital society. In most emerging markets, cash remains the predominant payment method. Only in a handful of countries, such as Sweden,[107] is a cashless society in sight. In Australia, the share of consumer payments made in cash fell from 70% in 2007 to 37% in 2016.[108] For China, it has been estimated that by 2020 the use of cash will fall to 30%, down from 61% in 2010.[109] The total cost of cash usage on societies can be as high as 1.5% of GDP.[110]

The digital commerce component of the index looks at the advancement in financial inclusion and the level of development of the e-commerce ecosystem.

Figure 7

### Digital commerce: country index scores




**Source:** GSMA Intelligence

The score for digital commerce in Bangladesh increased by more than 60% between 2015 and 2016, and has been driven by an increase in financial inclusion, both through traditional financial institutions as well as mobile money services. All developing countries among our focus countries have seen a significant increase in both financial inclusion and online commerce between 2015 and 2016. According to a GSMA report,[111] in 2017 South Asia was the fastest growing region for mobile money, with active[112] mobile money accounts growing by more than 50% to 86 million. Other drivers of digital commerce include the increase in mobile internet penetration and smartphone adoption, increased border trade, and the growth in trusted payment systems such as debit and credit cards, quick response (QR) codes and mobile wallets.

107 In Sweden, the proportion of cash payments in the retail sector has fallen from close to 40% in 2010 to about 15% in 2016. See The Riksbank's e-krona project Report 1, Sveriges Riksbank, 2017.
108 Payments System Board Annual Report, Reserve Bank of Australia, 2017
109 Social Networks, e-Commerce Platforms, and the Growth of Digital Payment Ecosystems in China: What It Means for Other Countries, Better Than Cash Alliance, 2017
110 Mastercard
111 2017 State of the Industry Report on Mobile Money, GSMA, 2018
112 On a 90-day basis.

# 7 Moving up the digital society value chain

Each of the eight countries has digital society plans, but they vary considerably. Some plans are comprehensive; others tend to focus on specific, strategically important sectors of the economy. In terms of outlook, some plans set out long-term goals, while others are devoted to short-run aims. A brief description of the plans can be found in Appendix A. In this section, we provide guidance, based on their current plans, for governments and policymakers to consider when building their national digital agenda and how to strengthen, where appropriate, each of the components of a digital society: connectivity, digital identity, digital citizenship, digital lifestyle and digital commerce.

Developing and transition economies need to ensure interoperability across different government platforms and need to better leverage existing digital identity systems to provide government services while mapping a path to develop the role of the private sector. Where countries lack safeguards for data protection, they need to implement the right frameworks or 'smart policies' for privacy and security. Advanced economies are further ahead in their pursuit of a trusted environment for their digital citizenry, and in these economies, the focus shifts to promoting frictionless ways of identifying users online and across different networks. Needing to build and ensure trust in such environments will increase as IoT and analysing data from thousands, if not millions, of connected devices, becomes the norm.

# 7.1 Pakistan, Bangladesh

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Pakistan** | Vision 2025 is Pakistan's plan to become a prosperous country, leveraging digital technologies to achieve significant growth and productivity gains in all sectors.[113]<br><br>Pakistan has made good progress in areas such as mobile money account registrations and mobile connectivity. These early wins should be coordinated with applications and programmes that drive usage.<br><br>Digitisation is still in nascent stages, and will require significant focus, not just on ICT policies – which is where the focus is now – but on a holistic and coordinated approach to both industrial and economic development and social enablement. | Mobile broadband (3G and above) coverage has increased significantly since 2014, but uptake has remained low.[114] As of June 2016, only 10% of Pakistanis subscribed to mobile broadband services.<br><br>Pakistan's mobile sector has significant scope for development and can support digital advancement by connecting people in underserved rural areas and providing a platform to increase financial inclusion.<br><br>Pakistan's National Telecom Policy seeks to modernise the regulatory framework. It should introduce clearer licensing and competition rules, as lack of clarity in competition policy regulation can create uncertainty for mobile operators. Competition between operators can encourage investment and lead to innovation in the telecoms market. | Updating e-government websites and services will enable the government to offer more comprehensive and easy-to-access services, such as interoperable e-government services linked to the CNIC, e.g. paying taxes online.<br><br>Work with private sector organisations to further enable the use of the CNIC to provide digital services for individuals.<br><br>Empower women by fostering the use of digital IDs to give women access to direct cash transfers. | Empower more women through digital literacy programmes.<br><br>Support local language apps and platform development with government-funded incubation programmes.<br><br>Work with industry to develop local accelerator and incubation programmes, as well as learning opportunities for developers to travel and learn from other countries. | Create a local ecosystem for the development and commercialisation of homegrown apps and solutions.<br><br>Continue to encourage entrepreneurship: the growth of tech hubs in Pakistan has boosted entrepreneurship in the country. Pakistan has more than 25 tech hubs and Plan9, the largest tech hub, has already incubated 118 start-ups.[115] | Increase financial access by developing money programmes for rural and remote populations by leveraging mobile technologies to access banking services.<br><br>Support SMEs: these constitute almost 90% of Pakistan enterprises. Work with SMEDA[116] and the Ministry of Industries & Production to<br>– Create conducive and enabling regulatory environment<br>– Develop industrial clusters<br>– Provide business development services to SMEs in all areas of business management.<br><br>Encourage cross-border trade – crucial for development of SMEs. |

113 Pakistan 2025, One Nation – One Vision, Government of Pakistan
114 Country Overview: Pakistan, A digital future, GSMA, 2016
115 Ibid.
116 Small and Medium Enterprises Development Authority.

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Bangladesh** | To successfully promote its national digital agenda, Bangladesh should take into consideration a range of key supporting factors such as the level of technology enhancement and upgrade required, ensuring foreign assistance with development priorities and foreign direct investment, diversifying its export market, human resource training and skill development, and improving resource allocation.<br><br>The government has undertaken key initiatives such as aligning national development plans with the SDGs, and developing the National ICT Policy and the Perspective Plan of Bangladesh 2010–21. | Rationalise the licensing regime to improve investment climate, and support quality of service for the consumer.<br><br>Create a predictable roadmap for future assignments of spectrum (e.g. 700 MHz), in consultation with industry players.<br><br>Reform mobile sector-specific taxation towards a more balanced and efficient structure to increase affordability of mobile products and services.<br><br>Include private civil society sectors in connectivity projects in rural areas.<br><br>Upgrade existing spectrum licences to technology-neutral, to facilitate faster deployment.<br><br>Ensure timely and affordable release of spectrum to facilitate better quality and more affordable services. | Promote robust identification-validation processes while adopting consistent data protection and privacy frameworks. Regulations and related laws defining the parameters of digital ID implementations also need to be in place.<br><br>Consider adopting flexible and proportionate approaches towards proof-of-identity requirements for forcibly displaced persons to be able to access mobile services, particularly in emergency contexts.<br><br>Explore the use of new digital identity technologies such as blockchain. | Adopt whole-of-government approach, combined with open data policy, so that organisations – both government and non-government – can make use of data to add value to products and services.<br><br>Launch big data initiatives to deliver scalable response (e.g. disaster response, m-health, connected living and others).<br><br>Open policy development process to citizen input and consultation so that policies can be demand driven and limited resources allocated to immediate challenges.<br><br>Utilise mobile (and other) platforms for digital awareness and literacy programmes; bring ICT into the school curriculum and partner with trusted NGOs to deliver hands-on training in digital literacy. | Develop digital solutions for patient data collection, reporting and telemedicine to improve quality of records and support remote monitoring and diagnostics.<br><br>Digitise hospitals and clinics to allow the use of solutions for remote patient monitoring, remote diagnostics, health data management, data security and imaging.<br><br>Initiate digital education programmes for all and bring ICT into the school curriculum and educational establishments to guarantee that citizens of tomorrow receive skills necessary for the modern economy.<br><br>Promote IoT technology to enable smart cities and smart mobility that can reduce congestion and collisions, contributing to improved safety. | Focus on devising solutions for rural e-commerce and low-cost online transactions.<br><br>Enable mobile money providers to provide cross-border and international remittance services to customers.<br><br>Increase uptake and use of mobile money services by digitising more payment streams – for example, wage payments in Bangladesh's garment factories.<br><br>Work together with the mobile and internet ecosystem to ensure that innovation can flourish by encouraging development of incubators and opening up APIs to start-ups. |

## 7.2 Indonesia, Thailand, Malaysia

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Indonesia** | Digitally restrictive policies such as the government's data sovereignty law, and sector-specific rules that require data centres and disaster recovery centres to be located in Indonesia are an impediment to cross-border data flows, and will undermine the digital economy agenda as well as the government's goal of becoming the largest digital economy in Southeast Asia. | Working towards completion of the Palapa ring network to provide fibre-optic high-speed broadband nationwide by 2019 is essential.<br><br>The government needs to continue to explore the means of expanding rural and remote access through the use of wireless technologies, as well as ensure clarity over spectrum allocation policies (such as the release of the 700 MHz for mobile broadband) to promote growth of the digital economy and interoperable digital applications and solutions.<br><br>Greater connectivity of and between government agencies will facilitate improved coordination as well as better communication between government and citizens, thus increasing public access to government information – e.g. via government websites. | Addressing data consistency and corruption issues is the first necessary step to imbuing trust in Indonesia's digital ID programme, and a crucial step in encouraging citizens to enrol with the e-KTP card programme.<br><br>Develop a general data protection policy to ensure the protection of personal privacy while ensuring cross-border data flows are not restricted.<br><br>Develop a roadmap for e-government services leveraging the use of digital IDs to provide more efficient and transparent government services. | Tailor digital literacy programmes for diverse groups, including women, rural communities, the youth (particularly in terms of online work and talent platforms, and training), and other marginalised communities.<br><br>Develop educational and awareness campaigns on fostering good online behaviour, as well as tolerance, especially among the youth. | Publishing government data and statistics on an open government data website will improve transparency and government reporting, and will focus government agencies to identify performance indicators for digital reporting.<br><br>The availability of data will also allow users to develop innovative and relevant solutions for a variety of demographics and constituencies across the country. Currently digital applications and solutions are disproportionately focused on social media and entertainment, rather than broader lifestyle or development options. | Only 20% of offline small businesses export, compared to almost 100% of small businesses with a website and access to a digital platform. Encouraging small businesses to use internet platforms is therefore fundamental to growth.<br><br>Encourage the use of digital payments by offering incentives for users who pay for public services through digital means. |

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Thailand** | Building trust into the foundational policies and programmes of the digital economy is fundamental.<br><br>Thailand's digital laws, including the Cyber Security Bill,[117] have been criticised as being political tools to limit freedom of speech. Intertwining a political agenda into the framework of the digital economy will undermine development. | Basic connectivity is still a challenge in many rural parts of the country. A lack of spectrum availability has been cited by mobile operators as a key challenge requiring operators to invest more into their networks and raising connectivity costs.[118]<br><br>The sustainability of the government's Net Pracharat project should be considered, and a suitable plan drafted. The project aims to provide free fibre broadband access to 40,432 remote villages by the end of 2018. | Implementation and uptake of the new national digital ID project should be accelerated by creating standardised and interoperable data formats so government entities can seamlessly connect, exchange and share data.<br><br>Develop a roadmap for private sector services that can leverage the use of the new national digital ID such as in healthcare and payments. | The MDES' big data, data centre and cloud computing committee's role should be enhanced to enable partnerships with the private sector to explore the use of government data. This resource sharing could give rise to innovative solutions that may help to solve complex social issues.[119] | The NBTC's plan to regulate OTT services should take into consideration the possibility of adverse impact on digital lifestyle opportunities. Regulation on OTTs should not stymie innovation or prevent both individuals and businesses from accessing innovative digital products and services.<br><br>The enforcement of laws such as the Computer Crime Act, which have been used as a tool to prosecute political dissidents, interfere with internet freedom and may result in distrust in the security and privacy of digital assets. | To promote and accelerate digital commerce opportunities, the EDTA should pursue further discussions with regional markets (besides Singapore) to link Thailand's interbank m-payment system PromptPay to other national systems, and to ease cross-border transactions. |

117 "Thai junta gives green light to bill on mass surveillance", prachatai.com, January 2015
118 Spectrum Auction Risks Leaving Thailand Stranded in a Mobile Data Slow Lane, NERA Economic Consulting, 2017
119 "Big data panel to direct country's digital transition", Bangkok Post, March 2018

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Malaysia** | Malaysia's comparatively smaller market means that it has to maintain an open economy if it is to attract foreign investment and foreign participation. This is particularly true in promoting the digital society agenda. The DFTZ[120] provides a strong story but needs to remain open to all players if Malaysia is to promote an inclusive developmental agenda. | Malaysia's mobile broadband environment (speed/cost) has recently fallen behind Thailand and, at one point, Vietnam, due to poor speed and comparatively high cost. Correcting this and meeting the PM's call for "double the speed at half the price" requires a more robust fibre backbone and greater competition at both the wholesale and retail levels.<br><br>The initial ASO, planned for June 2018, has been pushed back to enable a smooth transmission to DSO.[121] No new date has yet been announced. | Monitor and promote the Public-Sector ICT Strategic Plan (2016-2020) which aims to transform public service delivery based on digital technologies, open data, use of cloud and cybersecurity.<br><br>Ensure robust security and privacy foundations around the government's mobile digital identity solution, 'MyIdentity', to provide convenient digital service delivery, with security, privacy and efficiency.[122] | By 2020, Malaysia's Vision is to achieve a 100% literacy rate. While the focus of earlier plans was on connecting schools and equipping them with computers, smart devices are now the communications tool of choice.<br><br>Malaysia can take a leaf out of the book of digital natives in the US where websites and mobile apps are widely available to spread digital literacy and to aid both teachers and students. | The digital economy can help Malaysian start-ups to raise funds through crowdsourcing and P2P lending, as detailed in Digital Malaysia which targets the B40 (Below 40) group of households.[123] | The establishment of the DFTZ will improve e-commerce in the country and potentially establish Malaysia as a regional hub for SME trade. However, the platform will need to remain open to all players, and the zone will need to stay competitive with emerging challenges from Thailand and Vietnam.<br><br>The assistance of mobile apps that provide financial templates and calculations are a digital tool to help overcome the main challenges facing Malaysia's venture-capital market, e.g. limited funding, risk aversion, cyclical nature of the industry and difficulty to exit.[124] |

120 Digital Free Trade Zone.
121 "Analogue TV switch-off date deferred for smooth transition to digital TV", Borneo Post, March 2018
122 Developing Digital ID to support the Digital Economy in Malaysia, Malaysian Communications and Multimedia Commission
123 "Crowdsourcing off to good start in Malaysia, challenges remain", Digital News Asia, June 2017
124 Venture Capitalists in Malaysia: Challenges and Future Directions, Eliza Nor, School of Management, Universiti Sains Malaysia

# 7.3 Australia, Singapore, Japan

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Australia** | Finalise and release the digital economy roadmap with clear targets and opportunity for industry to work together.<br><br>Establish a coordinating agency or mechanism to help coordinate across relevant government departments. | Ongoing delays, inadequate delivery and technology choices for the National Broadband Network (NBN) need to be addressed.[125]<br><br>Recommendations of the 2015 Spectrum Review Report should be implemented.[126] | Implementation of the Digital Transformation Agency (DTA) of Australia's Trusted Digital Identity Framework will ensure users are able to safely and securely connect with government services online.[127]<br><br>The development of the digital economy roadmap should incorporate components of the Trusted Digital Identity Framework to enable citizens to connect to both public and private services. | Continue to provide funding to support science, technology, engineering and mathematics (STEM) skill development, with a focus on improving digital literacy, from early learning to higher education, and for older Australians.<br><br>Develop platforms and competitions to encourage local app development and build an ecosystem for local content apps. | Government should provide a supportive environment to leverage benefits of technology and plan for disruption of technology across all sectors. | Requirements for the regulatory fintech sandbox[128] should be relaxed to ensure flexibility and participation of larger institutional financial institutions as well as unregulated fintech players.<br><br>Australia needs to finalise participation in the APEC CBPR system.[129] |

125 "Australia struggles to deliver national broadband plan", Financial Times, September 2017
126 Spectrum pricing – review, Australian Government Department of Communications and the Arts, 2018
127 "Digital ID another step closer", Australian Government Digital Transformation Agency, February 2018
128 See Australian Securities and Investment Commission: http://asic.gov.au/for-business/your-business/innovation-hub/regulatory-sandbox/
129 APEC Cross Border Privacy Rules public consultation – Australia's participation, Australian Government Attorney-General's Department, 2017

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Singapore** | Given the size of its market and regional competition and challenges, Singapore needs to look beyond the Hub strategy that has worked in the past, and position itself as an 'economic influencer'.<br><br>This will require changing its top-down approach and adopting a more encompassing policy agenda and more responsive and nimble regulatory regime.<br><br>This means encouraging the free flow of data, information and ideas, as well as accepting that risk and failure are inherent parts of the digital economy. | While Singapore's connectivity is ahead of its regional counterparts, 5G will be a key turning point, and Singapore will need to align spectrum and regulatory frameworks if it is to continue to be successful. | Singapore has a number of e-Identity frameworks in place. A major challenge in this area is ensuring that private and sensitive identity data is secure.<br><br>The government needs to develop a holistic approach to using digital identity to interact with the Smart Nation initiatives.<br><br>Many cybersecurity initiatives have taken shape these past few years, but Singapore continues to be the target of increasingly sophisticated attacks, many of which have focused on theft or sabotage of identity. There needs to be greater focus on adequate cybersecurity protection for digital identity frameworks to ensure protection of sensitive data and interlinked data from identity. | In moving from coordination to consultation, a digitally empowered Singapore needs digitally empowered Singaporeans.<br><br>Singapore's population is relatively well-versed in all things digital. But efforts must be made to strengthen the inclusiveness of digital innovation.<br><br>As a rapidly ageing society, Singapore must ensure the elderly are not left behind or forgotten in the digital economy. This includes digital literacy initiatives that help the elderly avoid common hacking and phishing scams via digital portals. | Singapore has successfully digitised major portions of its economy and society. This is partly thanks to strong regulatory frameworks that attract entrepreneurs and reassure investors.<br><br>But as the digital economy becomes less about technologies and more about applications, creative thinkers will need space to do what they do. Singapore must enable the conditions for innovators to be innovators, and creators to be creators. | Singapore's digital commerce ecosystem is one of the region's most mature. yet paradoxically it is also one where consumers' interests rarely come into play. Whether it is in regulating competition in the sharing economy, or a confusing laissez-faire approach to digital services (the multiplicity of digital payment offers), Singapore needs to take decisive and consistent stands on consumer interests and commercial surety. |

| | National digital agenda | Connectivity | Digital identity | Digital citizenship | Digital lifestyle | Digital commerce |
|---|---|---|---|---|---|---|
| **Japan** | While Japan has ambitious digitisation plans, the country lacks a culture of aggressive entrepreneurship, with most innovations developed by large organisations rather than start-ups.<br><br>While Japan continues to develop its digital economy, it should also look to develop an independent start-up culture supported by government grants and incubators. | While adopting an industry-led approach to developing 5G, Japan should ensure that interoperability and harmonisation are at the forefront of the various 5G technologies, through the hosting of forums for 5G stakeholders to discuss and share standards. | Japan needs to accelerate implementation plans for rolling out digital IDs, learning from the difficulties faced when implementing the MyNumber system.<br><br>Secure and distributed ledger technologies would potentially enable a reliable and robust permanent public record of all transactions and allow access to banking services across participating banks through a common ID-verification service, providing increased convenience to consumers. | Digital literacy programmes should focus on the aging population, as well as on reducing dependency on cash.<br><br>Digitisation of the healthcare industry will also improve and ensure the sustainability of the public health insurance scheme. | Japan can encourage citizens to adopt an entrepreneurial mindset through social safety nets, encouraging innovation and calculated risks rather than following the societal pressure of securing a career in a big-name company.<br><br>Amend the Personal Information Protection Act (PIPA) to allow the transfer of personal information outside Japan. | Considering the aging population of Japan leading to labour shortages among Japan's SMEs, further development and promotion of ICT, automation and robotics can work hand-in-hand with the use of teleworking capabilities – for example, hiring people from remote locations or overseas.[130] |

130 "Japan Turns To Telework To Expand A Diminished Workforce", Forbes, July 2016

# Appendix A
# National digital development plans

## Pakistan

In 2017, Pakistan's Ministry of Information and Telecommunications published its *Digital Pakistan Policy 2017*, with ICT as an enabler of every aspect of socioeconomic development. It encompasses four areas of implementation: sector digitisation, cross-sector collaboration, IT-sector sustainability, and entrepreneurship and innovation, along with 13 policy goals, but no specific targets or timelines.[131]

The Pakistan government is focused on improving the extent, reliability and affordability of broadband connectivity across the country, especially in remote areas. Its Universal Service Fund (USF) operates a number of "special projects", including providing ICT training for girls and enabling people with disabilities to use telecoms services.[132]

In recent years, Pakistan and China developed a *Long Term Plan for the China-Pakistan Economic Corridor (CPEC)* from 2016 to 2030 to create, *inter alia*, smart and safe cities across Pakistan, including Islamabad and Lahore in 2016. Each project has a smart platform linked to the country's National Data Centre, and the aim is to train 2,000 professionals, mainly at Chinese training centres in Pakistan.[133]

## Bangladesh

The Bangladeshi government's Vision 2021 sees Bangladesh becoming a middle-income country, with poverty eliminated. by 2021 – the 50th anniversary of Bangladesh's independence from Pakistan. Vision 2021 relies on a Digital Bangladesh strategy to bring socioeconomic transformation through ICT and has the following priorities:

- develop digitally literate human resources
- connect citizens
- take government services to citizens' homes
- make the private sector more productive and competitive.

The strategy has made progress in all four priorities, and particularly in making government services more accessible via, for example, the launch of a national digital identity system. However, the ID system has raised concerns about the amount and security of the collected data in the absence of a robust framework for data protection. In April 2016, hackers stole $81 million from Bangladesh's central bank.[134]

Bangladesh's Access to Information (a2i) programme aims to improve information quality, widen access and decentralise delivery of public services. A2i has trained more than 200,000 civil servants and thousands of Digital Centre Entrepreneurs to implement e-services at 4,500 Union Digital Centres across the country.

As part of the Vision 2021 strategy, an Office for Public-Private Partnership (PPP) facilitates the development of public infrastructure with the aim of increasing infrastructural investment from 2% to 6% of GDP.

A lack of fixed-line infrastructure for backhaul and long-distance transmission hinders the rollout of mobile broadband, as do low rates of digital literacy, restrictive policies and high prices, including local taxes, which can account for 30% of basic data

131 "MoIT Releases Digital Pakistan Policy 2017", ProPakistani, August 2017
132 See USF: https://usf.org.pk/
133 "Exclusive: The CPEC plan for Pakistan's digital future", Dawn.com, October 2017
134 "Bangladesh Introduces 'Smart' National Identity Cards", advox.globalvoices.org, October 2016

packages.[135] The country auctioned 4G only in 2018 and restricts 3G services to the 2100 MHz band. Until recently, it prohibited the sharing of mobile base stations, towers and backhaul facilities.

To boost connectivity, in 2017 Bangladesh began extending a fibre-optic ICT Network to Remote Areas to connect 25–30% of the population.[136] The arrival of the SEA-ME-WE 5 submarine cable has also doubled international bandwidth capacity.[137] Bangladesh's 2017 budget provides for 12 IT parks and seven IT training centres across the country.[138]

## Indonesia

In August 2017, Indonesia launched a *Roadmap for the National Electronic Commerce System for 2017–2019* to grow e-commerce[139] to $130 billion (IDR180 trillion) by 2020, making the country the largest digital economy in the region.[140] The roadmap has 31 initiatives across seven sectors: education and human resources, funding, tax, consumer protection, cybersecurity, communication infrastructure, and logistics. A decentralised political system often results in local governments driving such developments without the benefit of central coordination. In April 2018, Indonesia's Ministry of Industry released the *Making Indonesia 4.0* roadmap, prioritising five sectors: food and beverage, textile and apparel, automotive, electronics, and chemical, with 10 cross-sectoral initiatives.

Indonesia's *1000 Start-Up Digital National Movement Program* aims to foster 1,000 digital start-ups worth $10 billion (IDR136 trillion) by 2020.[141] In early 2018, new regulation cut in half a 1% tax on SMEs with annual turnover below IDR4.8 billion ($360,000).[142]

Indonesia's *National Broadband Plan 2014–2019* aims to increase broadband and mobile connectivity to all parts of the country's archipelago.[143] To address the problem of last mile coverage, and extend 4G services to remote island areas, the government in late 2017 assigned the 2.1 GHz and 2.3 GHz bands to mobile operators.[144]

Indonesia needs to refocus on its electronic identity card (e-KTP) project and accelerate registration and issuance to equip all citizens with a digital ID for passports, driving licences, SIM card registration, taxpayer identification numbers, insurance policies, land ownership certificates and other identity documents.

A variety of regulations could limit cross-border data flows and hamper the development of Indonesia's digital economy. Requirements on data "residency" such as Reg. No. 82/2012 on electronic system and transaction operation (GR82), and Reg.No. 20 of 2016 on Personal Data Protection in Electronic Systems, along with proposed requirements to store all data in the country, will limit local SMEs in particular in terms of undertaking overseas expansion, investment and the interoperable transactions needed by global identity networks.

## Thailand

Thailand's *Digital Government Development Plan 2017–2021* plans to digitise all sectors, with a focus on agriculture, tourism, education and public administration.[145] The *Thailand 4.0 Policy* focuses on strengthening digital infrastructure and promoting robotics, aviation and logistics, and the digital industry. A 20-year *National Strategy* to 2036, known as the "6-6-4" plan, presents six key areas, six primary strategies and four supporting strategies for sustainable development via improved human capital, green growth and more science and technology. Moreover, a 12th *National Economic and Social Development Plan (2017–2021)*[146] has 10 national strategies for strengthening cooperation between public and private sectors in R&D investment and increasing access to and use of technology among farmers, community enterprises and SMEs.

For improved broadband connectivity, in 2016, the National Broadcasting and Telecommunications Commission (NBTC) drafted a five-year master plan on the use of new technologies such as 5G and to encourage sharing of telecoms infrastructure.[147] To increase rural connectivity, the government plans

135 Bangladesh: Driving mobile-enabled digital transformation, GSMA, 2017
136 "Bangladesh government kicks off rural fibre project", TeleGeography, May 2017
137 "Bangladesh connected with second undersea cable", Daily Star, February 2017
138 "Big Bucks for ICT to boost Digital Bangladesh Plan", theIndependentbd.com, June 2017
139 "Government Releases E-Commerce Roadmap", Amcham Indonesia, August 2017
140 Digital Economy of Indonesia, Kominfo, 2016
141 "KOMINFO Indonesia working on number of initiatives to boost digital start-up ecosystem and support SMEs", OpenGov, October 2017
142 "Govt finalizes regulation on e-commerce", Republika.co.id, February 2018
143 Indonesia Broadband Plan: Lessons Learned, ITU, September 2015
144 "Commencement of Radio Frequency 2.1 GHz Rearrangement for Mobile Mobile Networking Implementation", Kominfo, November 2017
145 "Govt announces five-year digital integration strategy", The Nation, March 2017
146 National Economic and Social Development Plan, The Government Public Relations Department, September 2016
147 "NBTC drafts five-year master plan for Thai telecoms industry", Capacity Media, September 2016

to provide low-cost broadband access to Thailand's 70,000 villages by the end of 2018.[148]

Thailand still lacks clear data frameworks for privacy and cybersecurity, although a long-delayed data protection bill would define and safeguard standards without impeding necessary internal and cross-border data transfers. The country also lacks a strong pool of digital talent. Just over 1% of Thai students showed "superior problem-solving and analytical skills", compared to an average figure of 15% for OECD countries,[149] and Thailand ranks 10th out of 11 Asia Pacific countries for digital skills.[150]

## Malaysia

Malaysia's *Economic Transformation Plan* (ETP) of 2010 aims to elevate the country to a per-capita Gross National Income of $15,000 by 2020,[151] by which time the digital economy is targeted to contribute 20% to GDP.[152] Intervening five-year plans set strategies and targets based on 12 National Key Economic Areas and six Strategic Reform Initiatives. The *National eCommerce Strategic Roadmap* of Malaysia's National eCommerce Council also aims to double the annual rate of e-commerce growth to more than 20% by 2020.

The Malaysia Digital Economy Corporation (MDEC) steers foreign digital investments into data centres and cloud computing with the intent of making Malaysia an e-commerce hub for ASEAN.[153] Similarly, the country's Digital Free-Trade Zone, launched in November 2017, facilitates cross-border trade in support of local e-commerce businesses.[154] In October 2017, MDEC launched a 'Cloud First' strategy to accelerate the adoption of digital technologies in Malaysia. The strategy will begin by improving public services, although the government will then look to encourage the private sector's adoption of cloud technologies.[155] Also in 2017, the Ministry of Health launched the Malaysian Health Data Warehouse as a central system to house citizens' health data,[156] and Bank Negara proposed a regulatory sandbox to promote fintech services.

## Australia

In September 2017, Australia's Department of Industry, Innovation and Science issued *The Digital Economy: Opening Up the Conversation*[157] as a roadmap with three focus areas:

- enabling a digital economy through infrastructure, standards and regulations that enhance trust, confidence and security
- raising Australia's productivity, competitiveness and digital business capabilities
- empowering citizens with inclusive measures to foster resourcefulness, adaptability and digital skills.

By 2025, the country targets digital technologies to contribute AUD140–250 billion ($81–196 billion) to Australia's annual GDP[158] or up to around one sixth of the country's annual GDP of $1.2 trillion for 2016.

By 2020, Australia's controversial and expensive nationwide, broadband fixed-line network, first proposed before 3G in 2007, should connect 8 million people or about a third of the population. However, by 2016, 4G mobile services already covered 98% of the population, making the need for such a network obsolete. Instead, 765 new mobile base stations should complete coverage of regional and remote areas under the country's Mobile Black Spot Program.[159] Australia plans to deploy 5G from 2020.

## Singapore

Launched in 2014, Singapore's Smart Nation programme has made Singapore an integrated, hyper-connected nation. From government services to business productivity, the programme has encouraged public and private organisations to use smart technologies to enhance work and lives.[160] A National Digital Identity (NDI) system, to start in the second half of 2018, will build on an existing SingPass system for government services to become a central authentication system for securing individuals' and businesses' private sector transactions.

148 "Thailand targets broadband in all villages by end-2018", Mobile World Live, May 2017
149 "Education gap too wide for leap to Thailand 4.0", The Nation, January 2017
150 "Thailand ranks 10th for digital skills in Asia-Pacific", CIPD, August 2017
151 Overview of ETP, Performance Management and Delivery Unit, Pemandu
152 "Digital economy growth to contribute significantly to Malaysia's GDP", New Straits Times, October 2017
153 National Ecommerce Strategic Roadmap, Malaysia Digital Economy Corporation (MDEC), 2016
154 "DFTZ Goes Live", DFTZ
155 "Plans for cloud-first strategy and national AI framework revealed at 29th MSC Malaysia Implementation Council Meeting", OpenGov, October 2017
156 For more information, see http://www.moh.gov.my/english.php/pages/view/129
157 The Digital Economy: opening up the conversation, Industry Australia, 2017
158 Digital Australia: Seizing Opportunity from the Fourth Industrial Revolution, McKinsey & Company, 2017
159 "Mobile Black Spot Program hits new milestone", Ministers for the Department of Communications and the Arts, January 2018
160 For more information, see https://www.smartnation.sg/about/Smart-Nation

A 10-year roadmap of the Infocomm Media 2025 plan promotes the use of data, advanced communications, and computational technologies to create an ecosystem for continuous experimentation.[161] Examples include the Smart Nation Sensor Platform, a nationwide network of sensors, which will enable connectivity, data and video analytics, and data-sharing across government agencies.[162] As part of the plan, Singapore's National Research Foundation is pledging up to SGD150 million ($108 million) over five years to boost Singapore's artificial intelligence capabilities.[163]

Singapore's Info-communications Media Development Authority of Singapore (IMDA), its Smart Nation and Digital Government Group, Government Technology (GovTech) Agency, SPRING Singapore, and 'SMEs Go Digital Programme' all help SMEs harness data-driven technologies to improve productivity.[164] Similarly, Singapore's Committee of the Future Economy supports start-ups in the fast-growing fintech, regtech and healthtech sectors, and in November 2016, the Monetary Authority of Singapore introduced a fintech sandbox to let companies experiment with innovative products and services without excessive regulatory intrusion.[165]

In January 2018, Singapore's parliament introduced a cybersecurity bill to empower a Cyber Security Agency to better manage and respond to cybersecurity threats.[166] The parliament is also looking at ways to tackle fake news.[167]

## Japan

The 2020 Olympics in Japan's capital, Tokyo, will showcase the country's advanced technologies – from autonomous vehicles and 5G networks to digital payments and robotics. The Japanese Cabinet's current, fifth Science and Technology Basic Plan to 2021 goes beyond the economy's digitisation to a digital transformation of Japanese society itself. From healthcare for ageing populations to responses for natural disasters, the Society 5.0 concept covers a wide range of socio-economic challenges that new, AI-based technologies can help address.

Japan's Ministry of Economy, Trade and Industry (METI) recently published guidelines on regulating the sharing economy, characterised by firms such as Airbnb and Uber. The guidelines create a conducive legal environment to protect both operators and consumers.[168] In January 2018, the government also said it would incorporate aspects of the sharing economy into its measurement of consumption and GDP.[169]

Japan has only one "unicorn" start-up firm, Mercari – an online marketplace, compared to the US with 112 and China with 59, each valued at over $1 billion.[170] A lack of investment, a domestic-focused start-up market, and a lack of entrepreneurial risk-taking account for Japan's struggle to create digital giants. A similar hesitancy to go digital meant that, in 2016, cash still accounted for 62% of Japanese consumer transactions by value, versus just 10% in South Korea and 22% in the UK.[171] Nevertheless, Japan's government encourages mobile wallets and mobile IDs, through Osaifu-Keitai services, supported by all mobile operators via the *de facto* Japanese standard, Sony's mobile FeliCa ICs. In October 2017, Japan's Financial Services Agency established a FinTech Proof of Concept Hub to allow fintech start-ups to experiment without regulatory constraints.[172] Japan is also the only country to recognise the use of altcoins as legal currency.

161 For more information, see https://www.mci.gov.sg/portfolios/infocomm-media/infocomm-media-2025
162 For more information, see https://www.tech.gov.sg/-/media/GovTech/Media-Room/Speeches/2017/5/Factsheet-Smart-Nation-Sensor-Platform.pdf
163 "Singapore's artificial intelligence capabilities to get S$150m boost", Channel News Asia, May 2017
164 "SMEs go Digital", Prime Minister's Office and Infocomm Media Development Authority, February 2018
165 FinTech Regulatory Sandbox Guidelines, Monetary Authority of Singapore, 2016
166 For more information see https://www.csa.gov.sg/-/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en
167 "Select Committee to examine fake news threat in Singapore", Straits Times, January 2018
168 "Japan begins licensing the sharing economy", Nikkei Asian Review, June 2017
169 "Japan to revamp GDP data to reflect sharing economy", Reuters, January, 2018
170 "Gen Isayama: It's time for Japan to nurture its own 'unicorn' startups", Nikkei Asian Review, January 2018
171 Financial Cards and Payments, Euromonitor International, November 2017
172 Japan Legal Update, Jones Day, October 2017

# Appendix B
# Index methodology

## Digital society metrics

There are four main components of a digital society, digital citizenship, digital lifestyle, digital commerce and connectivity. An index has been built for these components to show the advancement of a country along its digital society path.

The digital society metrics use a number of indicators across the four components. The overall index gives equal weight to each of the four components. Each is made up of the following dimensions, number of indicators and corresponding weighting of indicators:

- **Digital citizenship**
  - Availability and usage of identity and digital identity: 4 indicators – 50% weighting
  - Provision of public services through digital channels: 5 indicators – 50% weighting
- **Digital lifestyle**
  - Access and use of smart devices: 2 indicators – 25% weighting
  - Solutions beyond core communications into consumer IoT: 5 indicators – 25% weighting
  - Solutions beyond core communications into enterprise IoT: 7 indicators – 25% weighting
  - Locally relevant content online: 8 indicators – 25% weighting
- **Digital commerce**
  - Traditional banking: 4 indicators – 25% weighting
  - Financial inclusion: 3 indicators – 25% weighting
  - Transactions: 5 indicators: 25% weighting
  - Online commerce: 5 indicators – 25% weighting
- **Connectivity**
  - Mobile infrastructure: 4 indicators
  - Network performance: 3 indicators
  - Spectrum: 3 indicators
  - Other enabling infrastructure: 4 indicators

**Digital citizenship** is measured along two dimensions:

- **The existence of formal identity systems and digital identities:** whether there is a national identity system in the country and how many people are actually registered. Additionally, this looks at digital identity – in particular, if people use it to access online services and if there is a data protection and/or privacy framework in place.
- **The provision of public services through digital channels:** the availability and quality of online and e-government services and the extent to which citizens use them.

**Digital lifestyle** is measured across four dimensions:

- **Access and use of smart devices:** the smartphone adoption rate and share of licensed cellular IoT connections, as a percentage of total connections.
- **Solutions beyond core communications into consumer IoT:** IoT connections per capita (or per vehicle/household where relevant) in the following categories: consumer electronics (smart TV, home entertainment, personal entertainment, set-top box), smart home (home appliances, home infrastructure, home security and energy monitoring), wearables (fitness trackers and smart watches), smart vehicles (connected car, connected bike, insurance telematics) and others (trackers for children, the elderly and pets; drones; robots).
- **Solutions beyond core communications into enterprise IoT:** IoT connections per capita in the following categories: smart city (public transport, surveillance, electric vehicle charging, street lighting, parking, waste management), smart utilities (energy, water and gas smart metering, smart grid), smart retail (points of sale, digital signage, vending machines, ATMs), smart inventory (inventory tracking, monitoring and diagnostics, warehouse management), smart buildings (heating and air con, security, lighting, hot desks, office equipment), health (remote monitoring of medical devices, emergency vehicle infrastructure) and other (fleet management, applications in agriculture, oil, mining, construction).
- **Locally relevant content:** local relevance and content availability. Local relevance captures the proportion of the population that are active social media users, apps developed per internet user, Online Service Index score and the number of generic top-level domains per capita. Availability of content captures accessibility of top Apple Store and Google Play mobile apps, number of apps available in the first language of a country and the proportion of population with accessible apps in their first language.

**Digital commerce** is measured across four dimensions:

- **Traditional banking:** the number of commercial bank branches and ATMs per capita, and credit card and debit card ownership.
- **Financial inclusion:** the percentage of adults that have an account (at a financial institution or a mobile money account) and the percentage of population using online banking.
- **Transactions:** the share of the adult population that has sent or received domestic remittances, paid for utility bills, received wages, received government transfers and received payments for agricultural products.
- **Online commerce:** the percentage of the population that has made or received digital payments, the share of adults that have ordered or purchased goods online and the share of online shoppers. Additionally, it measures the availability of electronic content in a country.

**Connectivity** is measured across four dimensions:

- **Mobile infrastructure:** 2G, 3G and 4G network coverage, and the number of years since 3G networks launched.
- **Network performance:** average mobile upload/download speeds and latency.
- **Spectrum:** Digital Dividend, sub-1 GHz and above-1 GHZ spectrum used for mobile services per operator.
- **Other enabling infrastructure:** access to electricity, international bandwidth per internet user, the number of secure internet servers per capita, and internet exchange points per 10 million people.

# Building the index

The process consisted of determining the relevant data for the four components, identifying the indicators, normalising the data, addressing missing data, and finally calculating the composite index. For all the indicators, the latest data available at the time of research was used, and the values for each indicator were taken from the same year.

To build the index we needed a complete dataset, so to impute variables we used a 'hot-deck' imputation method. This imputes a value for a country by taking the value of another country that is similar. Hot-deck imputation works by taking the country with a missing metric – country A – and finding the country with the closest value for a similar metric – country B – and then using that country's missing metric score as our estimate for country A.

As the indicators had different units and scales, any indicator that did not use a 100-point scale had to be normalised to make the indicator values comparable, as well as to construct aggregate scores for each country. For indicator values that required normalisation, minimum and maximum values were set in order to transform the indicators expressed in different units into indices between 0 and 100 using the following formula:

$$\text{Normalised value} = ((\text{actual value} - \text{minimum value}) / (\text{maximum value} - \text{minimum value})) \times 100$$

Once all the necessary values had been normalised, the index was constructed as a composite index of the four components on a 100-point scale according to the weightages described in the indicator table above – 1 represents the worst situation and 100 the best. This allows us to compare the countries' scores for each category. To calculate the overall score, the sum of the indicators within each component was used, taking into consideration the weightage of each indicator.

The data was drawn from a variety of sources, such as World Bank, United Nations, World Economic Forum, Economist Intelligence Unit, UNCTAD, IMF Financial Access Survey, We are Social, OICA and GSMA Intelligence. The majority of the datasets comprise hard, factual data such as smartphone adoption rates and some data sources rely on more subjective inputs, such as the UN eGov Index, which assesses different aspects of e-government services.

gsma.com

**GSMA Head Office**
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601