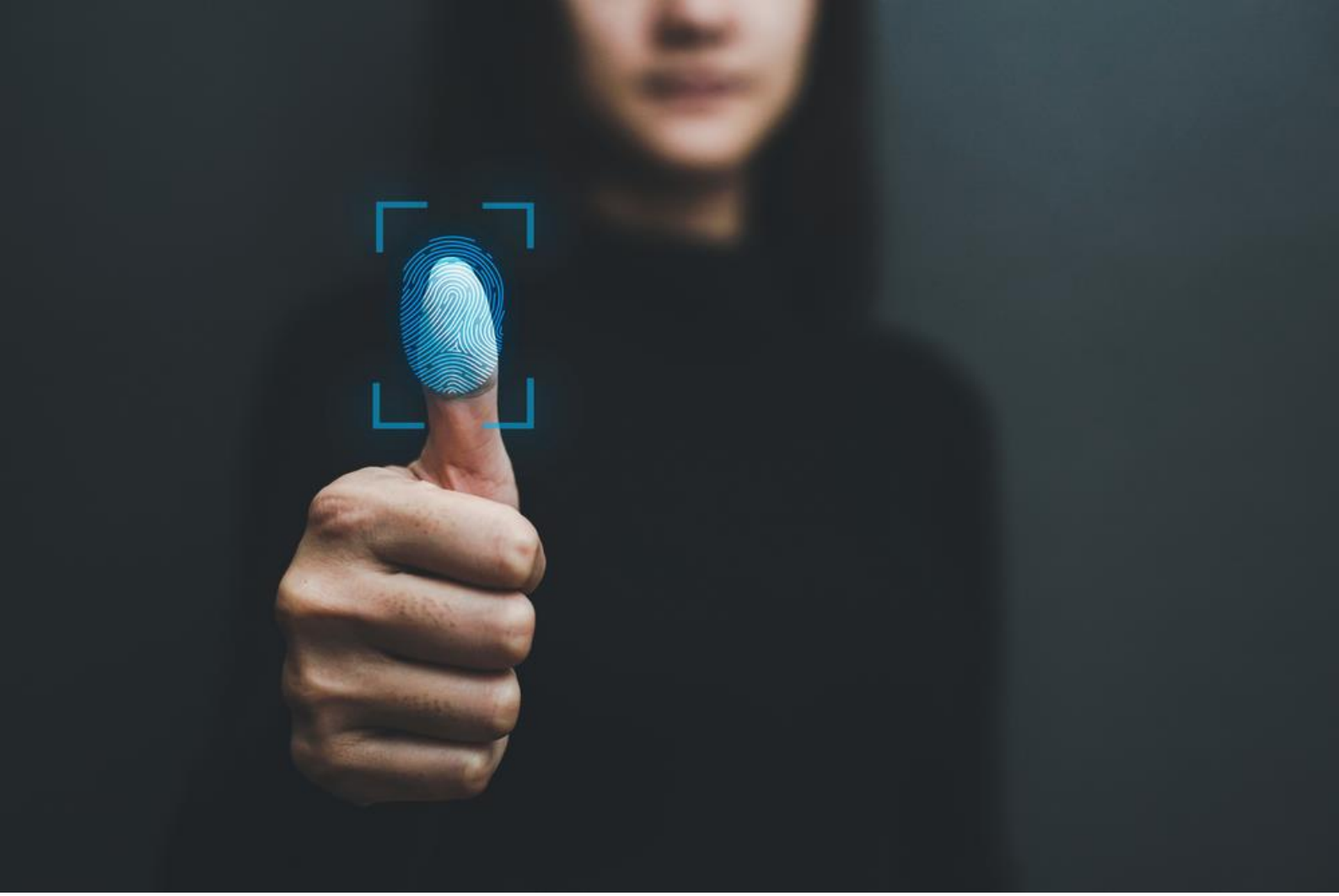


Digital Identity in APEC:

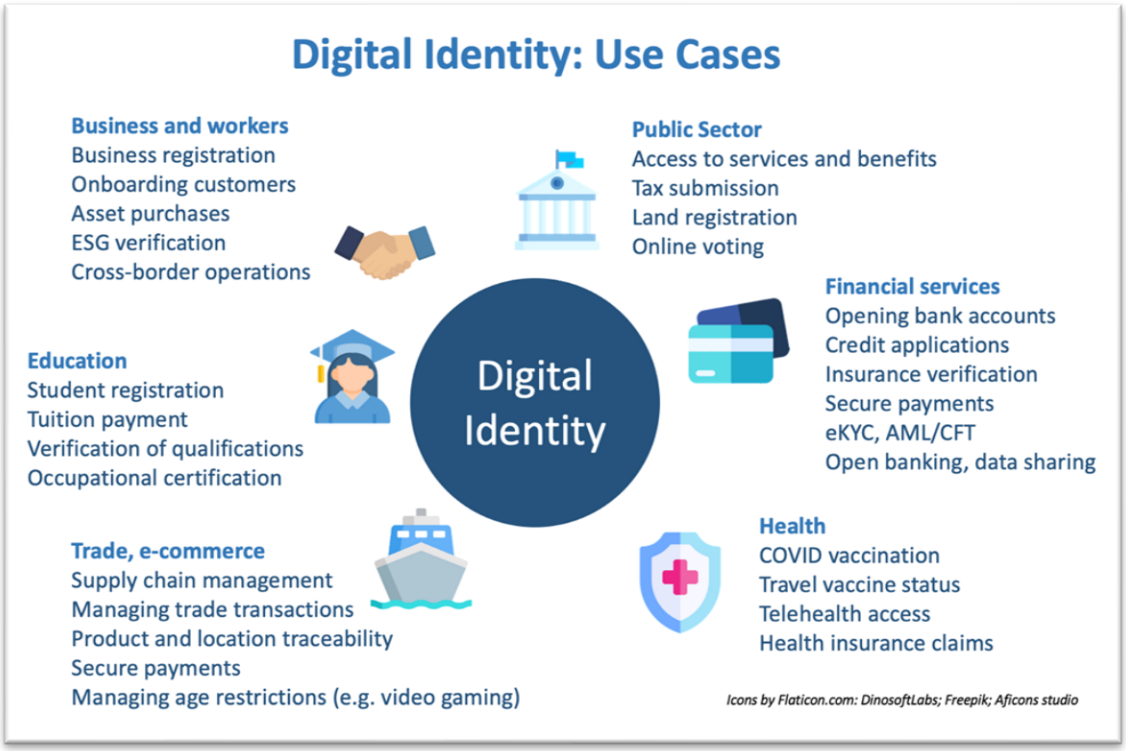
Deepening Trust, Inclusion and Interoperability in the Digital Economy

Report for the APEC Business Advisory Council
September 2022

Stephanie Honey
Honey Consulting Ltd

Deepening Trust, Inclusion and Interoperability in the Digital Economy

Good digital identity is a foundational building block in the digital economy, able to unlock value creation and inclusion for individuals, businesses and policymakers. Well-designed digital identity systems enable users to authenticate their identities online with confidence, enabling trusted, secure engagement across the economic, policy and social realms. At the economy level, good digital identity systems could boost GDP by the equivalent of between 3 to 13 percent in 2030 – up to $6.8 trillion in APEC economies, with more gains for emerging economies. Potential savings for public services could run to 110 billion hours saved; for businesses, payroll fraud savings alone could be up to $1.6 trillion. The box below sets out possible digital identity 'use cases'.



However, these benefits can only be realised if approaches within and across economies are coherent. The current digital identity landscape is fragmented: economies, businesses and individuals are using many different models, and sometimes no system at all. There are also some significant risks – around both misuse and exclusion – associated with badly-designed systems, necessitating the incorporation of robust safeguards for privacy, cybersecurity, and accessibility. APEC economies are well placed to work cooperatively to develop more coherent approaches, including giving thought to a set of principles for digital identity. The private sector also has an important role to play in helping shape and implement good digital identity ecosystems.

Recommendations

- Economies should design digital identity systems at the economy level that incorporate strong privacy and cybersecurity protections, are user-centric, are inclusive, sustainable and scalable, and integrate interoperability. This should be based on a set of coherent principles for good digital identity developed in APEC;
- Economies should engage closely with the private sector on the design and implementation of digital identity systems, and foster an enabling and competitive business environment and ecosystem;
- Economies should seek to boost uptake and foster cross-border interoperability, including by strengthening awareness and digital literacy, and pursuing interoperability mechanisms including mutual recognition and tailored approaches for specific use cases.

Executive Summary

The need for trusted, secure, and authenticated digital identities has never been greater. Individuals, businesses and policymakers are conducting more and more of their lives online, particularly as the disruptions of the COVID-19 pandemic continue to curb in-person interaction and prompt innovative models of engagement. Global internet users have climbed to 4.95 billion, with high levels of penetration in the APEC region, and more than two-thirds of the world now uses a mobile phone.[1] In this increasingly digitalized world, digital identity (digital ID) systems are foundational to engagement in the digital economy.

Currently, however, identifying yourself on the internet is a study in complexity – whether creating new passwords for dozens of different sites, or having to recall the answer to obscure security questions in order to complete online transactions. There is little consistency within or across economies, including in the APEC region. This means that the full economic potential of the digital economy cannot be realized – and it also exposes users to risks along with inefficiencies.

By contrast, "good" digital identity systems (that is, which are privacy-protecting, secure, trusted, sustainable, accessible and interoperable), are a cornerstone of economic and social engagement. This report looks at the current digital identity landscape in the APEC region; potential benefits to economies and explores how to enable wider adoption and interoperability.

In short:

Digital identity is one of the foundational building blocks of the digital economy

- Individuals, businesses and other legal entities, authorities, and even physical objects and locations, can all have a digital identity which enables them to assert and confirm unambiguously who they are in the digital realm.
- A digital ID is made up of "attributes" – biometric identifiers such as a fingerprint or facial scan, or other characteristics such as a name, date of birth or business registration that together make up a unique identity.

"Good" digital identity systems potentially unlock many benefits – for individuals…

- Well-designed digital ID can enable individuals to engage more efficiently, easily, confidently and securely online – for example, to access public or private services such as submitting taxes, receiving support payments, enrolling in a course, opening a bank account, or sharing health information such as vaccination status.
- There are particular benefits for underserved groups – especially in cases where individuals may not currently have a legal identity at all (around one billion people globally).

… for businesses…

- Well-designed digital ID can enable more seamless, trusted, secure, privacy-enhancing and efficient business and trade transactions, including leveraging the ability to identify physical objects and locations to streamline supply chains and increase trade efficiency.
- Digital ID can enable financial inclusion for individuals and businesses, especially micro, small and medium enterprises, and create more trusted and robust financial services engagement.

[1] WeAreSocial (2022), 'Digital 2022 Global Overview Report', https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/

…and for policymakers and economies

- At the economy level, McKinsey Global Institute has estimated that extending full digital ID coverage could generate the equivalent of 3 to 13 percent of additional GDP by 2030 – potentially unlocking up to $6.8 trillion for APEC economies, with the greater gains likely to accrue to emerging and developing economies.[2]
- Digital identity could save 110 billion hours of work for public services, reduce business onboarding costs by up to 90 percent and payroll fraud savings of up to $1.6 trillion annually.
- Over time, more benefits may be generated thanks to increasing uptake, evolving technologies, and innovation in ways to add value.

COVID has heightened the need for better, more secure online identification

- Since COVID-19, people and firms are conducting an increasing share of their activities online, and this has increased the need to identify oneself in the digital sphere: six months into the pandemic, for example, the average user had 25 percent more passwords than before.[3]
- Those who are not able to identify themselves effectively risk falling further behind in the digital divide; equally, good digital ID can be a powerful driver of economic inclusion.

The digital identity landscape is fragmented

- The policy, legislative, commercial, technical, technological solutions landscapes are fragmented across APEC economies, and globally.
- Some economies use a "centralized" approach (such as Singapore), others a "federated" network (Australia) or a "decentralized" ecosystem (some Canadian provinces), depending on government involvement and user control. Some economies set up a "trust framework" (such as that being developed by New Zealand).
- These models integrate the private sector in different ways (or not at all); the private sector has also developed its own systems, especially in the financial services and technology sectors.
- Differences in approach are not, *per se*, a problem – as long as there is overall coherence, and ideally, mechanisms to enable interoperability and accessibility for all.

There are potential risks from digital identity systems, as well as benefits

- Well-designed digital identity systems within economies, and greater interoperability across them, can help reduce costs, create efficiencies and enhance the integrity of transactions.
- But "good" digital ID systems must take account of a number of critical design considerations:
  ⇒ Robust privacy and cybersecurity protections(recognizing that data could be misused)
  ⇒ inclusion (ensuring that no individual or group is systemically excluded);
  ⇒ sustainability and scalability (the system must not be costly or complex to maintain);
  ⇒ interoperability (to reduce complexity and costs for users).

More work is needed within and across economies to develop good systems

- Concerted action from policymakers, working in partnership with business, is needed across many layers of the digital identity ecosystem, including:
  ⇒ definitions and technical standards;

---

[2] McKinsey Global Institute (2019), *Digital Identification: A key to inclusive growth*. "Full" digital identity coverage in this context means establishing basic digital identity systems, to enable verification and authentication, but also advanced identity applications, that can store or link additional information about individual ID owners and can thus facilitate advanced data sharing with informed user consent – see Section 5 of the MGI publication.

[3] Spadafora, A., 'Struggling with password overload? You're not alone', TechRadar, 21 October 2020. https://www.techradar.com/news/most-people-have-25-more-passwords-than-at-the-start-of-the-pandemic

⇒ regulatory settings and policy approaches;
⇒ user uptake, including building digital literacy, awareness and trust.

The private sector can and should play a central role

- There is a strong case to integrate business into digital ID design and implementation – but also good reasons not to leave this foundational infrastructure *solely* in the hands of the private sector
- A competitive digital identity services sector will boost innovation and productivity – so this should also be factored into the design and implementation of the digital identity ecosystem.

A 'one-size-fits-all' approach is not needed – but coherence and interoperability are

- The breadth of cross-border business, trade and people movement in APEC means that digital ID "silos" do not make sense: a one-size-fits-all approach is not needed, but greater coherence is.
- Individual APEC economies are starting to think about how to achieve greater cross-border interoperability, for example through recent digital economy agreements such as the Digital Economy Partnership Agreement
- Some regulators are exploring mutual recognition of digital ID for business, payments and other use cases, and policymakers in the World Bank, OECD and Digital Government Exchange are talking about principles for policy design.
- Private sector initiatives are also helping to drive cross-cutting models, especially in the financial services sector.

APEC is well-placed to lead these efforts, in partnership with business

- APEC is an ideal forum to work on digital ID. APEC has a long history of developing principles-based approaches to important digital economy issues such as privacy, and practical tools such as the digital APEC Business Travel Card.
- Sharing best practices and developing a set of "APEC digital identity principles", would be consistent with many of the priorities in the APEC Internet and Digital Economy Roadmap, including developing digital infrastructure, the promotion of interoperability, the development of holistic policy frameworks, the promotion of coherence and cooperation in regulatory approaches, the adoption of enabling technologies, enhancing trust and security, enhancing inclusion and facilitating e-commerce and digital trade.

So, what's needed?

- APEC economies should design and enable digital identity systems at the economy level that incorporate strong privacy and cybersecurity protections, are user-centric, and that integrate inclusion and accessibility, sustainability and interoperability.
- Developing a set of coherent 'digital identity principles' in APEC would be a valuable first step.
- Economies should also engage closely with business on the design and implementation of digital identity systems, and foster an enabling and competitive business environment and ecosystem.
- Work is also needed to boost uptake and accessibility, and foster cross-border interoperability. This calls for strengthening awareness and digital literacy, and for pursuing interoperability mechanisms including mutual recognition and in specific use cases.
-

Acknowledgements

This report was commissioned by the APEC Business Advisory Council (ABAC). It was prepared by Stephanie Honey of Honey Consulting Ltd.

The report would not have been possible without the support of ABAC members. Particular thanks for their thought-leadership go to Anna Curzon, Chief Product Officer of Xero, Co-Chair of the ABAC Digital Working Group leading ABAC's workstream on digital identities, and ABAC New Zealand member; to Janet De Silva, Chair of the Toronto Regional Board of Trade, Chair of ABAC's Digital Working Group and ABAC Canada member, to Ige Egal of ABAC Canada, Lead Staffer for the Digital Working Group, and to JC Parreñas of ABAC Japan and the Asia Pacific Financial Forum, and Senior Advisor at the Daiwa Institute of Research Ltd.

In addition, we warmly thank others from around the APEC region who have generously contributed their experiences, expertise and insights in discussion with the author. Unless specified in the text, no particular comment or conclusion should be taken as reflecting the views of, or attributed to, any individual or organization. Any errors remain the full responsibility of the author.

In particular, sincere thanks to the following:

Joni Brennan (President, Digital Identity Council of Canada); Richard Lomas (Senior Vice President, Government Affairs Asia Pacific, Citi); Patrik Jonasson (Senior Director Public Policy Asia-Pacific, GS1); Jaco Voorspuij (Senior Manager, Transport, Logistics & Customs, GS1); Douglas Arner (Holdings Professor in Law, Hong Kong University, Hong Kong, China); Kukita Shinya (ABAC Japan and NEC Corporation); Toshiya Matsuki (Executive Vice President, NEC Corporation; and ABAC Japan); Tak Tada (Director for Planning at Institute for International Socio-Economic Studies; and Executive Professional (Government Relations) at NEC Corporation); George Awap (Assistant Governor, Bank of Papua New Guinea); Saliya J. Ranasinghe, Centre for Excellence in Financial Inclusion, PNG); Noah Talo (General Manager, YuTru); James Gore (Managing Partner, Gore Consulting, and ABAC Papua New Guinea); Jessica Ortíz Morales (Director, Asia-Pacific Section, COMCE, and ABAC Mexico); Cecily Lin (Department for Internal Affairs of New Zealand); James Bergin (Executive General Manager, Architecture & Integration, Xero); Claire Barber (CEO, MATTR); James Brown (Director Global Partnerships, AplyID); Colin Wallis, Executive Director, Digital Identity New Zealand; Jason Lee (Director, International Policy and Engagement, Singapore Business Federation and ABAC Singapore); Clement Chow (Singapore Business Federation); and Nicole Vukonich (Policy Manager, National Center for APEC, and ABAC United States).

Introduction

Asserting and proving your identity is relatively simple in the offline, physical world: we can present a passport, a driver's licence or a letter from a utility company, to show who we are, how old we are, where we live and other important identity attributes. This enables individuals to undertake all kinds of activities such as accessing government services, enrolling to study, opening a bank account, or even just having a glass of wine at a bar.

In the online world, however, proving identity is not so straightforward: it involves many repetitive and confusing processes, with differences across platforms and sectors, and creates potential vulnerabilities for user data as a result.

This matters: being able to prove who you are online is an increasingly important element of engaging not just in the digital economy, but in the wider business and societal context too.

The current operational, regulatory and policy landscape for digital identities is fragmented, with many different models in use in the public and private sectors.

Failure to address this foundational element of the digital economy in a robust and coherent way across the APEC region represents an important missed opportunity.

This report provides an overview of digital identity and the different models in use around the region. It examines possible areas for future work to support the development of better, more user-centric and trusted digital identity systems within and across economies. It builds on extensive work undertaken by the Asia Pacific Financial Forum over many years on the use of digital identities in the financial services sector, as well as other recent reports prepared for ABAC, including on e-signatures, digital trade and data sharing.

The report is structured as follows:

Section 1 provides an overview of the key concepts of digital identity

Section 2 outlines some of the models that have been developed and their potential benefits and drawbacks.

Section 3 gives a snapshot of current digital identity frameworks across a selection of APEC economies. It outlines a number of examples and use-cases in the region.

Section 4 looks at the case for interoperability, and some of the approaches that are being developed to enhance the portability and interoperability of digital identities.

Section 5 examines the way that trade agreements are seeking to deepen regulatory coherence on digital identities in the region.

Section 6 examines considerations for ABAC and APEC economies. The report makes three key recommendations on digital identities.

Contents

Section 1: Overview of key concepts

The what, who, why and how of digital identities

Digital identity systems establish frameworks for the creation of unique identities for users, asserted and verified unambiguously through electronic means. [4]

In the offline world, the credentials that can be used to establish a person's identity are familiar and widely trusted: for example, a passport or physical identity document such as an ID card or a driver's licence.

By contrast, in the online world, a range of possible ways to assert and prove identity have evolved over time, ranging from simple self-selected usernames verified with passwords, to more complex forms of digital identity such as a scan of a fingerprint, or an electronic credential from a "digital wallet", that are governed by a formal system.

These methods all entail an electronic representation of the subject being identified, based on digitally-captured information about a set of "attributes". Attributes can include biometric data, such as a fingerprint or facial features; or biographical information, such as a name, date of birth or business registration number. Attributes can be supplied and verified by governments, by institutions (including authoritative sources such as banks) or by other private-sector providers.

This system – of the assertion and verification of attributes – enables the user to prove that they are who they claim to be, and thereby to gain access to services or networks without further manual or in-person intervention.

Digital identity systems may include databases, processes, technology, infrastructure, credentials, and legal frameworks for the capture, management and use of personal data to identify and verify people and things.

They can be set up through government action such as legislation, or in a purely private framework (for example, in a system set up by a technology company or mobile operator).

They can be "foundational" (based on economy-level identity systems or registries), or "functional" or "transactional" (such as drivers' licences or health insurance member registries – intended for specific transactions). Often functional systems rely on foundational systems for core information; in other cases, especially if there is no foundational system, the identities from functional systems can be used in a range of different settings.[5]

Digital identity processes

Key processes in digital identity systems include authentication ("Who are you?"), authorisation ("What are you allowed to do?") and assurances ("This person is who they claim to be" – a positive declaration intended to give confidence in the authenticity of an identity). The strength of these processes can vary, including in relation to the level of risk involved. For example, in the financial services sector, a high level of authentication and assurance may be required to comply with anti-money laundering requirements. In other situations, such as purchasing a bottle of wine in a supermarket, a lower level of assurance may be acceptable. Depending on the design

[4] UNCTAD (2022), *Why robust digital identity systems are essential in fostering trade and development*, Policy Brief No. 96

[5] World Bank (2019), ID4D Practitioner's Guide, World Bank Working Paper number 137292, 11 June 2019

of the digital identity system, the identity provider may be able to indicate to the person relying on the assurance how much confidence is warranted.

There is a lack of agreed definitions for digital identities. Without greater consistency, it can be challenging for policymakers and businesses to develop coherent approaches.

Whose digital identity?

A major focus of the development of systems for digital identities is on the identity of natural persons or *individuals*.

However, *corporate* digital identity (or the related digital identity of *legal entities*) can also be established, and can faciliate business and trade processes. There are some useful parallels between individual and corporate digital identity structures, but also some important differences in the way that relevant systems should be designed – these are discussed later in the paper.

Digital identities can also be established for physical and digital *objects*, and even for physical *locations*. Examples of these approaches are given below.

Good digital identity systems have many benefits for all participants:

For ***individuals***, as many as 1 billion people globally lack a legal identity and 3 billion face considerable limits online, exacerbating economic and social exclusion, which may worse as economies become more digitalized.[6] Digital ID can enable more trusted access to government services, banking, education, healthcare and commerce, and can help to share travel and vaccination status securely. [7] Depending on design, digital identities can provide individuals with "ownership" over their own data, by requiring explicit consent before data is shared or used by others. This has promise for marginalized or underserved groups, for example for Indigenous communities to manage their own unique genealogical and other identity information – although this may involve complex policy, design, and technical challenges.

For ***workers***, being able to prove that they have professional or occupational qualifications (such as health and safety certification, or ongoing professional development qualifications or certification), to record professional micro-credentials and retain control over important elements of HR records

For ***businesses***, trusted transactions are at the heart of robust, efficient and innovative business operations. Digital identities can be used for business registration, onboarding customers, e-contracts, data sharing, compliance with regulatory requirements, social and environmental compliance, e-commerce, supply chains and Customs clearance. Trusted interactions are also an important way to mitigate the risks of cybercrime, which is forecast to cost organizations $5.2 trillion globally in the five years from 2020 to 2025.[8]

For ***regulators and policymakers***, digital identities can enable streamlining of administrative processes and the more efficient provision of services to communities, such as enhanced compliance with tax and other regulatory requirements, efficient delivery of services including education and healthcare, land registration or voting.

[6] World Bank, *ID4D 2020 Annual Report*

[7] McKinsey Global Institute (2019), *Digital Identification: A key to inclusive growth*; and WEF/WTO (2022), *The Promise of TradeTech*

[8] GSMA (2020), *Mobile Identity Enabling the Digital World*

As long as a decade ago, the OECD noted the importance of "the development of effective and efficient digital identity management strategies to fully realize the economic and social potential of the Internet."[6] In fact, digital identities can enable the use of virtually all other digital technologies and facilitate compliance with digital economy regulations, including privacy.

Digital identity and the COVID-19 pandemic

Digital identities have become all the more important through the COVID-19 pandemic. Digital identity systems that were already in place or that could be developed quickly in the early stages of the pandemic meant that fast, secure and remote access to government support for affected individuals and businesses was made easier, and pandemic-specific responses such as vaccine 'passports' to enable safe travel could be developed. However, the increased demand for access to services digitally across many economies has also highlighted the critical importance of privacy and protection of personal data and the need for consumer and business confidence and trust in digital identity approaches.[9]

Benefits at the economy level

The McKinsey Global Institute has undertaken research into the impact of digital identities at the economy level. McKinsey examined seven mature and emerging economies and estimated that extending full digital identity coverage could enable economic value creation equivalent to 3 to 13 percent of GDP by 2030. Developing and emerging economies benefited more than more mature economies. Just over half of these benefits would accrue to individuals.[10] Benefits arise from lowered transactions costs and increased integrity in many different kinds of interactions.

"Extending full digital identity coverage could potentially unlock an additional USD$1.6 to $6.8 trillion in GDP-equivalent in the APEC region by 2030."

The APEC region generated a nominal GDP of USD$52 trillion in 2020. If the range developed by McKinsey were applied to the region's economies, extending full digital identity coverage could potentially unlock an additional USD$1.6 to $6.8 trillion in GDP-equivalent in the APEC region. The McKinsey report examines two APEC members specifically: the United States and China. In both cases, McKinsey estimated additional economic value creation of 4 percent of GDP by 2030.[11]

Separately, research by the Digital Identification and Authentication Council of Canada (DIACC) has estimated that the cost of *not* solving digital identities for people and organizations would be CAD$4.33 billion, including $236 per user to deal with password-related issues, 600 hours spent by victims of identity fraud, resulting in a loss of around $16,000 of unrealized income, and costs to companies of CAD$5.68 million per year arising from identity breaches.[12]

The relationship between digital identities and other parts of the digital economy

Digital identities are closely linked to other important elements of digital infrastructure, including requirements in relation to data protection, privacy and cybersecurity. Depending on design, in fact digital identities can not only achieve *compliance* with broader privacy and cybersecurity requirements, but can in fact *amplify* privacy protection and security in online and offline transactions.

[9] OECD (2020), 'Tracking and tracing COVID: Protecting Privacy and Data while using apps and biometrics'
[10] This section builds on McKinsey Global Institute (2019), *Digital Identification: A key to inclusive growth*.
[11] McKinsey Global Institute (2019); GDP figure from PSU (2021), *APEC in Charts 2021*
[12] https://diacc.ca/wp-content/uploads/2020/04/DIACC_English.pdf

Digital identities are also closely linked to other 'digital economy enablers' such as e-signatures and e-authentication. Improved digital identity frameworks and wider uptake could potentially achieve both more ubiquitous and beneficial use of e-signatures (in the context of a more "trusted" relationship overall), than greater use of e-signatures alone.[13]

> *"Identity and trust lie at the core of each trade interaction. As global value chains become increasingly digital, organizations need to ensure that they can trust the digital identity of legal and physical persons or products they deal with, and can efficiently link that digital identity with a real organization, specific product or device."*
>
> World Economic Forum and WTO[14]

Digital identity can help support the UN SDGs

Increased participation in the digital economy through digital identities can also be a powerful channel to support the achievement of many of the UN Sustainable Development Goals, not only SDG 16.9 ("Legal Identity for All") but also others such as economic inclusion, decent work and environmental sustainability. For example, digital ID could support important humanitarian goals such as those relating to child immunisation or refugee identities (see case study below).

Digital identities could also enable businesses to verify sustainability and labour-related claims, and be used to provide insight throughout global value chains, by enabling secure end-to-end traceability.[15]

[13] NCAPEC (2022), *Advancing Digital Transactions in APEC: Enhancing E-Signatures and Digital Signatures*

[14] WEF and WTO (2022), *The Promise of TradeTech – Policy approaches to harness trade digitalization*,

[15] WEF/WTO (2022), *The Promise of TradeTech,* page 42

Case study: Digital identities for healthcare

Despite huge progress in the last two decades, each year approximately 20 million children do not receive basic vaccinations, and 1.5 million vaccine-preventable child deaths occur. A key cause of these missed vaccinations is a lack of official identities.

NEC Corporation, along with GAVI (the Vaccine Alliance) and Simprints Technology Ltd (a UK-based non-profit social enterprise), are working to address this by developing the world's first scalable fingerprint identification system for young children in developing economies. The new system will link children's fingerprints with an accurate, complete medical record including immunisation information. Fingerprint data would be taken with the informed consent of their parents, and stored securely. An initial proof-of-concept validation has been carried out in Bangladesh.[16]

Similar systems could conceivably be used for access to services for emergency food supplies for vulnerable populations, and for refugees. More broadly, digital identity systems can potentially play a role in the efficient delivery of health services. Digital identities could simplify engagement between patients and doctors, for example in relation to checking eligibility, scheduling appointments, reducing fraud, and linking treatment to medical records or medical insurance details. Digital identities have also been used by economies during the pandemic for health services including the delivery of COVID-19 vaccines and the issuing of vaccine certificates. [17]

Digital identities for financial inclusion

Digital identities are potent tools for economic and financial inclusion – for micro-, small and medium-sized enterprises (MSMEs), as well as for populations that may not currently have a bank account or legal identity, which can be a major barrier to accessing financial services. [18] For example, India's Aadhaar system has led to the opening of over 150 million new bank accounts, including for many individuals who were otherwise "unbanked".[19]

Women also disproportionately lack formal identification in low-income economies; digital identities could address this structural disadvantage and improve their ability to access government and financial services, and healthcare.[20]

The World Bank estimated that during the pandemic, 140 million people were able to access the banking system for the first time thanks to the digitalization of government payments, including, for example, an estimated 14 percent of account holders in Thailand.[21] In a number of Southeast Asian economies, while a large number of unbanked people currently receive government payments in cash, a significant share own a mobile phone, potentially meaning that digital identities could enhance financial inclusion. For example, the Land Bank of the Philippines was able to successfully onboard 7.2 million unbanked citizens through the new 'PhilSys' digital identity system.[22]

[16] https://www.nec.com/en/press/201906/global_20190606_01.html
[17] World Bank (2021), 'Digital ID systems as an enabler of effective COVID-19 vaccination'
[18] Arner, D., Zetsche, D., Buckley, P., Barberis, J. (2018), 'The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities', European Business Organization Law Review, et a..
[19] World Bank (2019), *The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth*
[20] McKinsey Global Institute (2019), *Digital Identification – A key to inclusive growth*
[21] World Bank (2019), *The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth* , page 113.
[22] https://www.biometricupdate.com/202201/zoloz-biometric-authentication-deployed-in-philippines-financial-inclusion-push

Case Study: Papua New Guinea digital identities: YuTru

About 80 percent of the 8 million-strong population of Papua New Guinea does not currently have access to a clear form of identification.[23] A new mandatory 'National Identification Programme' has made slow progress to date, although it aims to reduce the unbanked by 2 million over the next 5 years.

The Bank of Papua New Guinea (BPNG), along with the PNG Digital Commerce Association and the Centre for Excellence in Financial Inclusion, has established a Regulatory Sandbox and has commenced accepting submissions for digital identity providers to trial products and services. A number of applications have been received for testing, including a "Digital Access" tool that has been developed in partnership between the Asian Development Bank and a digital identity provider, Digizen, on a pilot for remote communities.[24]

"YuTru", an industry-led consortium of financial services institutions, is developing a Trust Framework, with the aim that "all citizens have access to an affordable digital identity that is under their control and enables them to participate fully and safely in online commercial transactions" – providing opportunities in particular to the unbanked, women, and those in the informal economy. It hopes to "provide PNG with an opportunity to leapfrog into the modern digital world in a way that is customized for the unique PNG environment". [25]

YuTru will use a federated system including biometric identifiers, distributed ledger technology and digital wallets on smartphones. (Even remote communities are relatively well served by mobile infrastructure, meaning that smartphone-based applications have significant potential.) YuTru's initial work is with financial institutions, but with the aim of eventually broadening the scope to include other sectors. For now, the focus will be on low-risk/low-assurance transactions, working towards achieving more comprehensive digitally-based KYC (which currently requires the provision of up to five separate physical identity documents), and using a sandbox model to build confidence for both micro-lenders and consumers. A big challenge the initiative faces is public unfamiliarity with the technology and the need to develop greater confidence and trust among the community.

It is hoped that the Trust Framework, which draws on international models, will help to set the standards for similar approaches in the Pacific region. This will not only support greater financial inclusion for micro-enterprises *within* PNG, but also improved financial systems around the region, where many previous money transfer operations for remittances and other funds have struggled to remain viable through the pandemic. The hope is that one day, for example, a YuTru identity holder could use that digital identity to open a bank account in Australia.

Other initiatives are also underway. A digitized loan product for smallholder farmers, using a form of digital identity, is being developed.[26] Papua New Guinea has also recently released a draft plan to digitise all public services, with the aim of establishing a single biometric or digital identity technology to be used by all agencies for access to these digitalized services, potentially including land registration and voting.[27]

[23] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/Digital-Transformation-The-Role-of-Mobile-Technology-in-Papua-New-Guinea.pdf
[24] https://digizen.id/
[25] Quotes from YuTru website, https://yutru.org/
[26] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/03/DFAT-PNG-v3.1-2.pdf
[27] https://www.biometricupdate.com/202208/papua-new-guinea-digital-government-plan-draft-includes-consolidated-biometrics-system

Digital identities come with a risk of misuse

The increase in online activity in recent years, and the development of new approaches to digital ID, have come with increased concerns about data protection, cybersecurity, fraud and identity theft, the potential for profiling, and risk of abuse of human rights.[28] For example, the Indian Aadhaar system, which contains the biometric information of 1.2 billion citizens, has been the subject of multiple malicious cyberattacks.[29]

Ensuring that digital identities cannot be misused are important considerations that must be taken into account in the design of digital identity systems, and addressed with robust safeguards. At the same time, a balance needs to be struck between safeguarding these critical elements and the usability of the digital identity system – a complex and challenging exercise.

The World Bank's *Identity for Development (ID4D) Practitioner's Guide* has identified a range of possible risks arising from identity systems (depending on design), including:

- *Exclusion* – failures or biases in identity systems (for example, collecting data that is difficult for some people to provide for reasons of economic marginalization, language, or disability) or the technological underpinnings (for example, a failure of biometric authentication mechanism, or even lack of access to hardware, internet connectivity or digital literacy) may mean that some people are excluded from the system.
- *Privacy and security violations* – these are inherent in the capture, storage and use of sensitive personal data. There are risks associated with data theft and misuse, identity fraud, discrimination, and cybercrime.
- *Vendor or technology lock-in* – for example through allowing only limited suppliers or contractual arrangements – this can lead to increasing costs and reduced flexibilities for an economy. [30]

Public perceptions about digital identities

There are also issues around public perceptions and the "social licence" for digital identities that must be addressed by both policymakers and businesses. In New Zealand, for example, media reporting has noted public concerns about the risks of overreach and ethical concerns about privacy and security of digital identities – although in fact the design of the proposed New Zealand system is for a decentralized approach which builds in significant safeguards.[31]

Similarly, according to research undertaken by the Digital Identity and Authentication Council of Canada, four out of five Canadians believe that it is somewhat or very important that the government move quickly to enable a safe and secure digital identity for all Canadians, with two-thirds feeling that the pandemic has made it more important to have a secure, trusted, privacy-enhancing digital identity.[32]

---

[28] PECC, *Primer on Economic Integration Issues Posed by the Digital Economy*, page 70.

[29] World Economic Forum (2019), Global Risks Report, page 22

[30] World Bank, *ID4D Practitioners' Guide*

[31] Radio New Zealand, 18 July 2022, 'Activation of new facial recognition technology expected within the next year', rnz.co.nz/national/programmes/morningreport/audio/2018849817/activation-of-new-facial-recognition-technology-expected-within-the-next-year; and 29 July 2022, 'Risks of biometric verification technology use in public services databases flagged up', https://www.rnz.co.nz/news/national/471814/risks-of-biometric-verification-technology-use-in-public-services-databases-flagged-up

[32] DIACC presentation to ABAC, April 2022

Section 2: Digital Identity Models

The internet was not originally designed to be navigated with unique identities for individuals or organizations such as businesses. As one commentator notes, "Anonymity is a feature, not necessarily a failing, of the internet, and this directly conflicts with various customer identification requirements in finance".[33]

Early approaches to "digital identities" were driven by individual organizations or service providers seeking to develop their own identity management system. For example, Dun & Bradstreet established a database in 1841 in order to provide American merchants with reliable credit information on businesses, which it began computerizing in the 1970s. Today, the database contains information on over 285 million businesses, mainly in the United Sates, and assigns unique numeric identifiers, the "DUNS" number.[34]

Initial approaches at the economy level sought to replicate existing centralized national identity systems, sometimes in partnership with the private sector (often the finance sector). However, this model also had limitations, especially for economies that did not already have identity systems in place. Subsequently, "federated" models have been developed where accredited digital identities are not specific to a particular service, but may be re-used in different settings across the network. Increasingly there has been a shift towards empowering individuals to have greater control over their digital identities in "decentralized" or even "self-sovereign" models.

In sum, digital identity models can be grouped under three main headings:

Centralized: Centralized approaches are typically based on existing identity systems, often building on economy-level identity card systems or population registers. An example is Singapore's National Digital Identity system (Singpass and Corppass). Benefits include simplicity and high levels of user trust. On the other hand, these systems also mean that users are not in control of their identities, and the centralized model may be vulnerable to privacy and cybersecurity risks. In addition, for policy reasons, some economies and users prefer not to use a centralized system.

Federated: Under federated systems, users are able to use the same identity data to gain access to the networks and services of all the entities that are part of the system. For example, under Australia's Trusted Digital Identity Framework (TDIF), multiple entities from the public and private sector can become accredited identity providers. Individuals can choose which provider to use. Benefits include greater user control, and integration of the private sector as identity providers; however identity is still fragmented across enterprises, and systems are only available to accredited providers.

Decentralized and self-sovereign identity systems: In such systems, the user retains full control of the identity data, managing the collection of attributes (which may be issued by the public or private sector) and access to them. These models are typically underpinned by blockchain or other distributed ledger technologies, with identities contained in a digital wallet or secure cloud storage. Individuals, organizations and small businesses are able to verify information about each other without having to go through intermediaries, facilitating more peer-to-peer uses. Examples include British Colombia and Ontario's Verified Organizations Network.[35]

[33] Arner et al. (2018), 'The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities', EBI Working Paper Series 2018 – No. 28

[34] http://www.medium.com/humanizing-the-singularity/a-brief-history-of-digital-identity-9d6a773bf9f5

[35] WEF/WTO (2022), *The Promise of TradeTech*, pg 42.

Such systems are user-centric and enable individuals to retain full control of their data. They also build in strong privacy protections, whereby it is possible to limit data sharing to what is strictly necessary for the provision of a service (for example, simply confirming that an eligible individual is over 18, rather than having to share all of the information on a driver's licence). Similarly, these models can have strong integrated security: decentralized and encrypted data (for example, only unlocked with a two-part cryptographic key, of which the user alone holds one part) mean that identity theft becomes much less of an issue, even in complex, multi-party transactions. However, this model is less familiar, which may slow wide adoption, and it requires a well-defined, widely-accepted and well-executed governance model to establish trust. [36]

Case study: A (largely) centralized model: Singapore's approach[37]

Singapore has a range of "Smart Nation" centralized digital identity tools, including:

- The National Digital Identity (NDI) app "Singpass" enables users to access public and private services through a single login, and also enables e-signatures. There are more than 3.2 million users, representing 97 percent of adults. Users can access over 1,700 digital services across 460 agencies and businesses. Singpass handles around 300 million transactions a year. Use cases include seamless "SafeEntry" check-in during the pandemic; tax payments; registration of a child for government services, and work is underway for 'Know Your Customer' in financial services.
- "Myinfo" enables the pre-filling of digital forms with personal data, integrating over 700 digital public and private services. Businesses report an 80% reduction in transaction time, a 20% increase in transaction completion and a 15% increase in approvals due to better data quality.
- "Corppass" establishes a unique digital attribute that can be used to verify a firm's identity during online transactions. It enables access to government services that facilitate G2B, B2B and B2C transactions. It is used by over 550,000 participating businesses, non-profit organizations and associations. Over 250 digital services such as applying for trade licences and business grants and the filing of corporate taxes can be accessed.
- "Myinfo business" enables businesses to consent to the sharing of their corporate and applicants' personal data securely with other participating businesses. It has facilitated an average of over 500,000 monthly transactions for the public and private sectors and gives access to more than 120 G2B and over 60 private sector digital services.
- The Singapore Financial Data Exchange ("SGFinDex") utilises the NDI and a centrally-managed online consent system to enable users to access financial information such as deposits, credit cards, loans and investments on a single platform. It is a public-private collaboration including the Association of Banks in Singapore, seven participating banks and the SGX Central Depository. Since its public release in December 2020, SGFinDex has had over 150,000 unique sign-ups, linking 290,000 bank accounts and making 620,000 data retrievals.

Trust Frameworks

'Trust frameworks' set out the rules and requirements for governance and operation of a digital identity system. They typically engage both the public and private sector as identity providers (that is, verified or accredited organizations). Such systems deliver a high level of confidence for the participants in and consumers of the system, by focusing on achieving an overall outcome (in effect, the achievement of trusted use cases) rather than defining specific methods. Trust frameworks by their nature enable greater interoperability across complex ecosystems.

[36] BIS, page 12.

[37] Information in this box from www.tech.gov.sg (digital identity pages – various).

Case Study: Trust Frameworks in Australia, Canada and New Zealand

Australia has a federated digital identity system underpinned by a Trusted Digital Identity Framework (TDIF).[38] Private sector entities can be accredited as identity providers, with Mastercard joining Australia Post and the Australian Taxation Office as the first three accredited providers. The TDIF is also integrated with the Australian myGov portal for government services.[39] As of December 2021, the system was being used by over 6 million individuals and almost 1.3 million businesses. For businesses, there are reductions in operating costs – for example, the DTA estimates that a new business owner could save AUD$128 in costs and nearly four weeks by not having to mail physical documents to the Australian Business Register.

The TDIF has been designed to be interoperable both domestically and at the international level. It is based on international and industry best practice and standards, and builds on layers of existing policy and legislation, including privacy-related rules applying to data entering the digital identity system.

Canada does not have a digital identity system at the federal level, but envisions an ecosystem where individuals, businesses and government are in control of identity verification data, and are enabled to participate in and benefit from the outcomes.[40] The current approach is federated to an extent, relying on the trusted digital identities established by Canadian provinces and territories – for example, Alberta's digital identity can be used to access the Canadian Revenue Agency's online services.[41] Some of the provinces and territories use decentralized systems, such as British Columbia, which has a verified credentials network for organizations, and a pilot project underway for verified credentials for people.[42]

The Digital Identity and Authentication Council of Canada (DIACC), a non-profit coalition of public and private sector representatives, is developing a Pan-Canadian Trust Framework (PCTF). The objective is to establish a "robust, secure, scalable, inclusive and privacy-enhancing digital ecosystem". It aims to achieve interoperability of public and private sector identity capabilities. Elements under development include a digital wallet and a Verified Organization Network.[43]

Possible use cases identified by DIACC include more efficient and secure healthcare, more efficient government services, better civic engagement (including by reducing fraud and poor online behaviour including trolling and spamming, and increasing trust and accountability), and in commerce (including for more secure, higher-volume retail and e-commerce, reductions in transactions and payments fraud, and increasing operational efficiencies). Other potential opportunities include open banking and payments, facilitating access to international education for students, and immigration and refugee support.[44]

New Zealand[45] is likewise in the process of developing a Digital Identity Services Trust Framework, (DISTF). Legislation is currently being considered. The DISTF aims to facilitate the use of public services, financial services and other economic activities.[46] The draft legislation establishes a Trust Framework that is technology-agnostic and will support the use of a range of identity systems, such as the government-provided RealMe service, while also encouraging the development, and safe and secure use, of identity services provided by the private sector, including the use of verifiable credentials from both the public and private sectors. It will not include a single, centralized database.

[38] https://www.digitalidentity.gov.au/.
[39] https://www.digitalidentity.gov.au/digital-identity-for-you/digital-identity-for-business-owners
[40] Digital Gov Exchange (2022), *Digital Identity in response to COVID-19: DGX Digital Identity Working Group*
[41] https://www.itworldcanada.com/article/the-state-of-digital-id-in-canada/484618#:~:text=Digital%20ID%20is%20coming%20to,secure%20access%20to%20government%20services.
[42] https://digital.gov.bc.ca/digital-trust/
[43] https://diacc.ca/the-diacc/
[44] DIACC President Joni Brennan's presentation to ABAC, April 2022
[45] https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/
[46] https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/

The draft framework was developed with extensive engagement with stakeholders, who highlighted priorities including trust, privacy and security, ease of use and data handling practices in the design of the system. The rules will also ensure that Indigenous (*Te Ao Māori*) approaches to identity are considered in trust framework governance and decision-making. The draft DISTF includes key principles that the system should be people-centred; inclusive; secure; privacy-enabling; enabling Indigenous ('Te Ao Māori') approaches to identity; sustainable; open; transparent; and interoperable (including potentially with the systems of other economies).

Utilization of digital identity systems globally

Policymakers around the world have launched around 165 digital, or partly digital, identity schemes, but with mixed track records in terms of user adoption and usage – for example, in some cases, a system may have been used only once or twice a year per person.[47] Broader utilization means that more benefits can be generated – but this requires not only that systems are of high quality, but also that consumers and businesses know about, trust and are able to access the systems.

This calls not only for good design, but also for greater public digital literacy and awareness To sustain trust (and utilization) over time, systems must also be well-maintained, accurate and secure. Accessible physical infrastructure, including access to broadband and mobile networks, will also be important.

The role of businesses in digital identity ecosystems

Business and policymakers can work collaboratively together on digital identities. As noted above, in some models, especially where there is a federated or decentralized model, the private sector can act as providers or verifiers of digital identity attributes and credentials.

The development of digital identity ecosystems also holds the promise of creating new business opportunities, where the private sector (including digital identity and 'RegTech' firms) can provide innovative trust services such as digital wallets or other value-adding services linked to digital identities, including data sharing mechanisms, e-payments and other financial services. In the future, the Internet of Things may create further opportunities for innovation in business models and services in the identity space.

In some economies, such as Canada, Singapore, the United States, New Zealand and Australia, there is already a vibrant commercial digital identity ecosystem. However markets for such services must be and remain competitive, and avoid locking in specific providers and vendors, to support greater productivity and innovation.

> *"…the value of mobile network-based authentication services is expected to approach $13 billion by 2025"*

Mobile communications operators can play an important role in enabling digital identification, and potentially also in helping to achieve broader digital identity coverage.[48] One report predicts that unique mobile identifier services are likely to become the primary source of identification for over 3 billion people by 2024 – meaning that mobile operators will increasingly become the "brokers of identity". The report also projects that nearly 40 percent of people worldwide will use identity documents via mobile

[47] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

[48] GSMA (2021), 'Commercially sustainable roles for mobile operators in digital ID ecosystems,

devices.[49] GSMA, the global mobile operators' association, notes that the value of mobile network-based authentication services is expected to approach $13 billion by 2025, showing growth of over 30 percent compounding annually between 2020 and 2025.[50]

Other private sector collaborations are also being established which have potentially significant cross-border reach. For example, the Institute for International Finance, the OpenID Foundation, the Global Legal Entity Identifier Foundation and others are advocating for a 'Global Assured Identity Network' (GAIN) which would establish a user-centric and high-trust network in which a user would ask a trusted and regulated provider, such as a bank, telecommunications provider or another regulated entity, to verify that they are who they claim to be, or hold the credentials that they claim.[51]

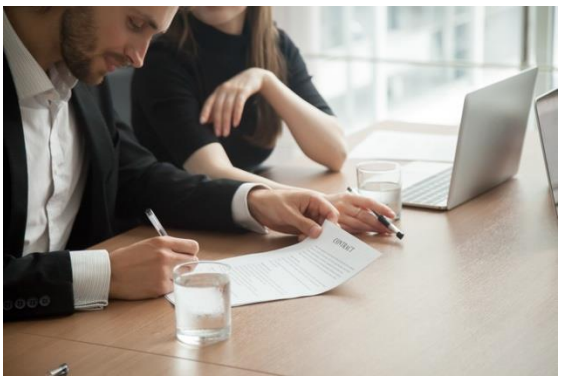
Financial services provider Mastercard is active in working with the public and private sector to develop a global identity network.[52]

In other cases, technology companies may establish their own proprietary systems – for example, the 'federated' approach developed by Meta which enables identities to be used across different products such as Facebook or WhatsApp, or a new decentralized digital identity credentials verification solution called 'Entra' developed by Microsoft.[53]

Digital identity is not just about people: corporate digital identities

Digital identities are often discussed in terms of the identity of 'natural persons'. However, digital identities can also be established for businesses and other legal entities. Attributes such as a business registration number, tax number, bank accounts or sectoral registration can be gathered and stored electronically, and together can uniquely identify the business.

Corporate digital identity is similar to personal digital identity, but with some important differences. A recent report for the Bank for International Settlements (BIS) notes that, compared to the relatively simple parameters of digital identity for a natural person, a legal entity may have a complex corporate structure and attributes such as directors, shareholders and ownership structure that may change over time, as well as different data privacy needs, "in particular since most data protection regimes differentiate explicitly between personal and non-personal (e.g. company) data".[54]



A corporate digital identity gives a business the potential to access services and interact virtually with business partners, employees, authorities and customers. In the words of the BIS report, corporate digital identity "forms a kind of admission ticket for a company to access financial and non-financial services while at the same time enhancing

[49] Juniper Research, 'Digital Identity: Technology Evolution, Regulatory Analysis & Forecasts 2019-2024', 5 August 2019, quoted in GSMA Identity news, https://www.gsma.com/identity/news-flash-7-billion-opportunity-in-digital-identity-for-operators-by-2024-as-world-turns-to-mobile

[50] GSMA (2020), *Mobile Identity enabling the digital world*

[51] GAIN (2021), *GAIN Digital Trust: How financial institutions are taking a leadership role in the digital economy by establishing a Global Assured Identity Network.* A Proof-of-Concept was developed under the auspices of the Cloud Signature Consortium, the Global Legal Entity Identifier Foundation, the IIF, OpenID Foundation and Open Identity Exchange

[52] https://www.mastercard.com/news/perspectives/2021/digital-id-in-a-virtual-world-how-to-prove-that-you-are-really-you/

[53] https://www.microsoft.com/en-nz/security/business/microsoft-entra

[54] BIS (2022), page 4.

access to information about the company for counterparties, customers, regulators and financial services providers".

Corporate digital identity can also overcome information asymmetries, meaning that investors, creditors, counterparties and others can make better evaluations in doing business – including for MSMEs, enhancing their potential inclusion.[55]

Corporate digital identities can be used for paying taxes and meeting other regulatory requirements and for more streamlined engagement with business partners and customers, including in complex trade transactions (which may include exporters, importers, banks, insurers, Customs, freight forwarders and transport services) or cross-border business. In a recent article, Citibank pointed out that, "Technological advances mean that many leading Fortune 500 companies operate an asset-light model with a limited (or non-existent) physical presence. However, they still need to transact cross-border. To do so, they must be able to establish their identity."[56] The global Financial Action Task Force (FATF) said in 2020 that it saw robust digital identity as at least as good as physical identity.[57]

Economy-level approaches to corporate digital identities

Some economies that have frameworks for individuals have also included or built on these systems to create digital identities for corporations. Singapore, Australia and New Zealand all use such an approach, utilizing existing centralized business registration systems. There is a case to be made for corporate digital identities to include a base form of identity, perhaps provided through a centralized registry, authorities or frameworks ("public good infrastructure"[58]), as well as attributes that may be provided by the private sector, in either a federated or decentralized model. Cross-border uses are also likely to require mutual recognition in relation to business law settings (see Sections 4 and 5).

Cross-cutting approaches for legal entities: GLEIF

One cross-cutting model for corporate digital identity is the 'Global Legal Entity Identifier' system. The G20 established the Legal Entity Identifier (LEI) in 2011 and then the not-for-profit GLEI Foundation (GLEIF) in 2014 to govern and administer the LEI system. The LEI is a 20-digit code based on ISO standards, which contains information about the company's structure and links. By July 2022 only 2.2 million companies had acquired an LEI, including around 436,000 in APEC economies, but wider uptake would enable greater consistency and a higher level of assurance in financial transactions, including 'Know Your Customer' requirements, de-risking and financial inclusion for MSMEs – with the added advantage that this is a globally-recognised system.[59]

Digital identities can also be established for physical and digital objects

Physical and digital objects can also have digital identities. These can help to confirm a product type in e-commerce, for example, or the movement of a product through supply chains, making it easier and less costly to monitor what is happening in supply chains and to demonstrate compliance with regulatory requirements and standards such as those for environmental, safety or other goals. However, there is no consistent global model for the way that objects or locations are identified, although GS1 is working to develop one approach

[55] BIS (2022), *Corporate digital identity: no silver bullet, but a silver lining', page 1.*

[56] https://www.citibank.com/tts/insights/articles/article154.html

[57] https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

[58] BIS, page 5.

[59] https://www.gleif.org/en/lei-data/global-lei-index/lei-statistics.

Case Study: Digital identities of physical objects and locations: GS1 approaches

Products and trade items: GS1 has established a system to classify products called the Global Trade Item Number (GTIN). These identification numbers have been developed in partnership with industry over the past 50 years, including some of the world's biggest brands. GTINs are used by businesses to uniquely identify products, verify product data, including product type, country of origin and content. More than 200 million standardized product SKUs are freely available online. This provides a rich, living open-source database that allows for the unique identification of products, for example for use in e-commerce. More data-rich identification of products also has the potential for greater value-adding for business, in both the B2B and B2C area.

Customs and other border agencies are increasingly requiring traders to provide GTINs as well as HS codes on Customs declarations. Linking the GTIN system with HS codes more formally could provide important insights into the movement of goods trade internationally by fostering transparency, reducing fraud and strengthening risk management. It would also reduce compliance costs for businesses since they would only need to input data once, avoid duplication and repeated manual inputting when preparing supply-chain and Customs documentation.[60]

Locations: GS1 has also developed a Global Location Number, GLN, and associated Registry. This system enables business entities to identify their locations anywhere in the world by using a globally unique identifier. Three different types of location can be identified: a fixed physical location (for example, a warehouse); a mobile physical location (such as a food truck); or a digital location (for digital twins). Any physical object can be connected with any location, enabling greater visibility for supply chain management, procurement, logistics and traceability.

The Registry will help the business community to create, store and verify GLNs to support data-sharing in trade. It can accommodate alternative identifiers discussed above such as the DUNS number, or the LEI, a UN Location Code or a decentralized digital identifier, and provides searchable links to the original data so users can easily refer back to the more detailed information they may require. The use of a registry containing links to original sources, rather than a large consolidated database *per se*, mitigates risks around trust, data integrity and data protection requirements. Data owners retain full control of the access to the original data.

There are a number of 'use cases' for the GLN Registry, including connecting to other data for B2B and B2G purposes (for example, detailed logistics around moving a container from a port to a final destination), and for accessing information about the other parties in the supply chain. The Registry can substantially improve the efficiency, effectiveness and safety of transport and logistics. In terms of uptake, millions of organizations in different sectors already use GLNs. At the economy level, some are more active than others, especially Singapore, New Zealand and Australia.

[60] Interview with Patrik Jonasson, GS1, and WEF/WTO (2022), *The Promise of TradeTech: Policy Approaches to Harness Trade Digitalization*

Section 3: A snapshot of approaches across the APEC region

Approaches to digital identities vary significantly across APEC economies, with some economies using centralized systems based on existing ID cards, others using federated or decentralized systems, and a number of economies which are still in the development or conceptual phase. Table 1 below gives a snapshot of current activities, as do the case studies which have featured earlier in the paper.

Table 1: Economy-level digital identity systems in a range of APEC economies[61]

Economy	Digital Identity approach
Australia	A 'Trusted Digital Identity Framework' is in place, used by 6 million individuals and 1.3 million businesses (see case study). Australia Post and the Australian Taxation Office also offer digital identities (MyGovID).
Brunei Darussalam	An 'e-Darussalam' platform is based on a national identity card. It provides a single nationwide digital authentication key that gives access to multiple online services provided by the government. Work is underway to broaden this system and use cases.
Canada	The Digital Identity and Authentication Council of Canada is leading development of a Pan-Canadian Trust Framework, in addition to various models in place at the federal and provincial level (see case study). The 'Verified.Me' decentralized self-sovereign network is run by major Canadian financial institutions. Identified use cases include financial transactions but also the gaming sector (for user age and geographic verification, and to prevent account fraud), education (providing student IDs), eKYC for insurance companies, and verified client identification for lawyers.[62]
Chile	The ClaveÚnica system was launched in 2012 for accessing online services (as a complement to an existing physical ID card), and is now being expanded. It is intended to allow for data authentication, a data wallet, electronic signatures, a citizen mailbox and a web portal electronic identity.
China	A digital version of the national identity card system is planned for 2022.[63] Other projects and initiatives include WeChat Government ID and an Alibaba Digital ID Project.
Hong Kong, China	The 'iAM Smart' app, developed by the Office of the Government Chief Information officer, is linked to mobile phones and provides a digital identity that can be used for individual authentication, form-filling, personalised notifications and digital signatures.[64] Individuals can access a range of online public services and public utilities. It will include APIs for commercial organizations, financial institutions and other public bodies to adopt iAM Smart in their online services. Work is underway on a business version using the same platform.
Indonesia	The 'eKTP' provides a digitised foundational identity system, covering approximately 98% of adults, based on the Single Identity Number (with centrally-held electronic databases). There is an ongoing process involving more than 3,000 stakeholders from the public and private sectors to integrate, verify and validate data. A smart card is planned. The development of a formal digital identity is considered a priority area and will be carried out in conjunction with the establishment of personal data protection legislation.

[61] Information from various sources (unless otherwise specified), including World Bank (2019), *The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth;* World Bank (2019), *ID4D Practitioners' Guide;* OECD (2019), *Digital Government in Chile – Digital Identity*, OECD (2021), *G20 Collection of Digital Identity Practices,* McKinsey Global Institute (2019), *Digital Identification: a Key to Inclusive Growth;* UNCTAD (2021), *Digital Identity for Trade and Development*; and Emerging Payments Asia, *Digital Identity Operational Framework* (2021).

[62] https://verified.me/industry-use-cases/

[63] https://www.scmp.com/news/china/politics/article/3170214/china-plans-digital-version-national-identification-card-later

[64] https://www.info.gov.hk/gia/general/202012/29/P2020122900647.htm

Economy	Digital Identity approach
Japan	A 12-digit 'My Number' digital identity card is in use, but with plans for expanded uptake and functionality including for financial services. A new digital agency will lead a broader digitalization process including further work on the digital identity system.[65]
Korea	The 'PASS app' has been used by more than 1 million users in a pilot scheme that will be rolled out more broadly in 2022. The scheme is a collaboration between mobile operators and the Korean National Police Agency, linked to the driver's licence system. It can be used as a driver's licence but also as identification at convenience stores, as well as filing civil complains, receiving a qualification certificate, verifying identity at the airport, and for private contracts. [66]
Malaysia	A digitised foundational identity system, the "National Digital ID" (IDN), is currently going through Proof of Concept. (An existing identity card system, MyKad, has been used as a smartcard to access government services since 2001.) The NDI will be optional and will provide trusted digital certification and verification for individuals. It can be used to access public and private services, perform transactions and provide e-signatures.
Mexico	Mexico is working on implementing various digital identity initiatives. In 2020, a law was passed which paves the way for a new national digital identity system, the *Cédula Única de Identidad Digital* (CUID), in which digital identities will be issued for all Mexicans, including biographical details and biometric data. The *Clave Única de Registro de Población* is a national identification number already used to access public services.
New Zealand	New Zealand has taken a broad and collaborative approach to the development of a new digital identity system. A new Digital Identity Services Trust Framework is under development (see case study). The legislation, when passed, will be technology-agnostic and citizen-centred, offering individuals greater control over their identity-related data.
Papua New Guinea	A trust framework is under development (see case study).
Peru	A National Electronic ID card provides citizens with a digital identity that can be authenticated physically and virtually. Includes two digital certificates that allow the cardholder to sign electronic documents. Can also be used as a travel document.
Philippines	A biometric national identity card, the PhilID, is being developed. The PhilID can be used for accessing financial services as well as for identity verification for social welfare programmes. A new system, PhilSys, is also being developed that will provide seamless access to public services.[67]
Russia	A foundational digital identity system, the Unified Identification and Authentication System, is in place, covering approximately 84% of the adult population. There are also sector-specific digital identity solutions in place.
Singapore	The National Digital Identity (NDI) including Singpass, Corppass, Singapore Financial Data Exchange (see case study). Singpass covers 97% coverage of adults. Also a real-time payments system (PayNow) linked with Thailand's PromptPay.
Chinese Taipei	A number of initiatives to introduce digital identities have been introduced, but the most recent proposal from 2019 is currently on hold. Chinese Taipei's Digital COVID-19 Certificate will include a holder's national identification number.[68]
Thailand	The National Digital ID (NDID) provides a digital identity platform for financial institutions – currently used to verify identity for natural persons but to be expanded to include legal

[65] https://www.japan.go.jp/kizuna/2021/03/new_id_card_system.html
[66] https://www.korea.net/NewsFocus/Sci-Tech/view?articleId=210616; https://www.biometricupdate.com/202201/south-korea-launches-mobile-drivers-license-trial-plans-mid-year-general-availability
[67] https://www.biometricupdate.com/202202/philippines-aims-for-92m-biometric-philid-target-in-2022; https://www.biometricupdate.com/202201/zoloz-biometric-authentication-deployed-in-philippines-financial-inclusion-push
[68] https://www.taipeitimes.com/News/editorials/archives/2022/01/01/2003770515 and https://www.cdc.gov.tw/En/Bulletin/Detail/LSlTGOfej27iTC2oziPydw?typeid=158

Economy	Digital Identity approach
	persons.[69] NDID is a federated model where financial institutions act as identity providers. Thailand has announced new investment into six key projects including the One Identification Program aimed at MSMEs, a welfare platform, agricultural data, a legal portal to enhance public participation and health and medical services.[70] A real-time payment system (PromptPay) is linked with Singapore's PayNow.
United States	The US has a system of federated digital identities. Identities are generated at the local government level and used to create state-level identity credentials. At the federal level, the US is working to recognise identities from the state and local levels to enable secure digital access to federal services while prioritising privacy, minimising data collection and ensuring user consent before data is used or shared.
Viet Nam	A partially digitised foundational identity system is under development, to be based on a national digital identity framework. The system will use biometrics. Currently Viet Nam has several identity databases with significant coverage, including for health insurance participants, taxpayers and others – but no single official identity provider.
ASEAN	In the ASEAN Digital Masterplan 2025, ASEAN economies are looking at how to introduce digital identities "in a way which safeguards civil liberties". The Masterplan proposed that ASEAN undertake a study that will develop principles for introducing full functionality digital identity systems which can be used for transactions as well as information in both the public and private sectors, and which will work across the ASEAN region through mechanisms such as mutual recognition. Singapore, Brunei, Thailand and the Philippines are developing digital identity systems with transaction capability which will function across borders into other ASEAN economies.[71]

Use cases for business and trade in the region

Digital identities can be utilized in a range of different use cases relevant to business. Many of these have already been noted in this paper – such as meeting regulatory requirements, onboarding customers, business processes such as concluding e-contracts, e-documents and data sharing, facilitating asset transactions, and verifying worker credentials (for example, health and safety certification, or professional qualification and registration), social and environmental compliance and supply chains.

Financial services

The financial services sector has been active in developing concepts and approaches to digital identities, recognising the efficiency and integrity gains for 'Know Your Customer' (e-KYC), anti-money laundering and ultimate-beneficial owner requirements, to onboarding customers and setting up bank accounts, loans or mortgages, verifying income for credit checks, authentication of payments, fraud prevention or detection, or even just enabling customers to log in to a bank account more easily and securely.

These activities can entail significant compliance costs for both the financial services provider and the customer, especially across borders.

The Asia Pacific Financial Forum (APFF) has advocated for digital identities for many years, and provided important inputs to ABAC in this

[69] https://www.biometricupdate.com/202203/thailands-ndid-partners-with-mastercard-to-connect-digital-ids-internationally
[70] https://www.biometricupdate.com/202112/thailand-finland-invest-94m-amid-digital-id-funding-partnership-flurry
[71] ASEAN Digital Masterplan 2025, https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

area. In 2020, a Digital Identity Project was established in conjunction with Emerging Payments Asia to develop a technical report and hold dialogues with policymakers and regulators on digital identities.

In its recommendations to APEC Finance Ministers in 2020, ABAC underscored the need for more inclusive e-KYC processes, including the need for more work on legal frameworks around the acceptance of digital signatures, enabling trusted data sharing and other elements, and also noted the value of "a strategy that focuses on standardisation to enable interoperability within a decentralized framework, and enlisting the regulated banking sector as the trusted keeper of identities".[72]

Other services

A digital identity that can be used across geographical boundaries opens up exciting possibilities for services to be offered across borders. Examples include education services, e-commerce and in the travel and tourism sector, as is discussed below.

Case study: Digital Identities in the travel and tourism sectors: NEC

NEC Corporation is the world leader in biometrics, including ranking first for both speed and accuracy of its biometric systems. It undertakes a wide range of projects for the public and private sector. In the tourism and travel sector, for example, NEC is developing innovative solutions to improve customer experiences and enhance security and safety. Building on earlier work with airlines, it is currently working with the Star Alliance to develop a biometrics hub. This is intended to enable seamless, secure and contactless boarding at airports around the world with a single mobile enrolment. Pre-enrolment allows passengers to pass through security checkpoints and boarding gates without physical contact, using facial recognition technology. This improves the accuracy and efficiency of boarding procedures, as well as improving passenger convenience and access to other services (the latter offered in accordance with the passenger's informed consent).

The platform has been designed for compliance with existing data protection and privacy laws such as the EU's General Data Protection Regulation. Successful trial projects have been undertaken in Europe to date.[73]

NEC is also working with Nanki Shirahama Resort in Japan on a near-future "Only Here" facial recognition trial. This would enable guests to pre-register their biometric facial information and credit card details, and then use those credentials to access services in different locations and activities in the resort, including making cashless payments.[74]

Digital identities can also be used to authenticate and authorise activities and achieve greater visibility in supply and distribution chains – see the case study below relating to air travel distribution chains.

[72] ABAC (2020), *Report to APEC Finance Ministers: Accelerating Recovery and Reshaping Financial Services in the Wake of the Pandemic*.
[73] https://www.youtube.com/watch?v=pCTyQViuvEA
[74] https://www.nec.com/en/global/insights/article/2020033101/index.html

Case study: The air travel distribution chain

Current identification standards in airline distribution are based on technology that dates back to the 1960s; while this has worked very well for forty years, some key challenges have emerged which robust and interoperable business-to-business digital identities can help to solve. These challenges include enabling participants to be able to identify all parties in the distribution value chain, achieve the scale needed for industry coding systems, and ensure end-to-end data security.

The International Air Transport Association (IATA) is the trade association for the airline industry and has launched a 'Digital Identity for Distribution' initiative. New Zealand-based digital identity firm MATTR is partnering with IATA on the initiative, demonstrating how digital identity can be used to enable the secure identification and authentication of organizations involved in the travel distribution chain to improve security and reduce the level of fraud risk for both airlines and travel intermediaries such as travel agents. The approach shows that a decentralized identity ecosystem built on open standards can enable all parties in the ecosystem to identify who they are doing business with quickly and securely, and in a way that protects user data by design. Similar initiatives could be used for the verification of cargo.[75]

Section 4: The case for interoperability, and how to get there

The discussion above highlights the need for greater regional coherence on digital identities within and across economies, and for a more active focus on achieving future interoperability across a broad range of online services and systems. Siloed approaches reduce efficiency and increase the risks of data breach and identity theft; encourage businesses to provide only low-risk services through online channels, inhibiting innovation and productivity gains; and represent a missed opportunity to generate economic benefits and foster innovation.[76]

At the same time, achieving interoperability, or even just greater coherence within and across economies, is a complex challenge. At a minimum it requires significant collaboration between the public and private sectors.[77]

Interoperability across multiple layers of the ecosystem

"Interoperability", whether within an economy or across a border, requires services or systems to be able to transact seamlessly across many layers of the digital identity ecosystem.

Important elements include:

- Sharing common definitions and terminology;
- Alignment at the semantic level (enabling systems to 'talk' to each other, by ensuring that the specific meaning of information is understandable and data can be processed by different applications) and on technical standards (enabling linking of systems or services);
- Alignment of legal and regulatory frameworks;
- Greater coherence in policy settings;
- and achieving wide uptake (potentially requiring consumer awareness and digital literacy).

Mutual recognition

Mutual recognition is one potential pathway to cross-border interoperability at economy level, but requires considerable work to achieve the necessary alignment. Some trade agreements are starting to integrate this goal, as is discussed further in Section 5. In other cases, such as between Australia and New

[75] See https://mattr.global/solutions/iata/ and https://www.iata.org/en/programs/innovation/digital-identity/
[76] See OECD (2015), Working Party on Security and Privacy in the Digital Economy
[77] GSMA (2018), *Digital Identities – Advancing digital societies in Asia Pacific*

Zealand, there are regulator-to-regulator workstreams in train (in this case, seeking to achieve mutual recognition of digital identity services – see case study below).

Sector-specific use cases can also achieve interoperability, as for example between Singapore and Thailand, where the world's first linkage of real-time retail payment systems has been achieved, linking Singapore's PayNow and Thailand's PromptPay, meaning customers of participating banks can securely transfer funds from one account to another between the two economies, using only a mobile number.[78]

Case Study: Trans-Tasman digital identities

Australia and New Zealand have each made significant progress towards developing trust frameworks and enabling policies for domestic digital identity systems (see case studies above). They are also working towards interoperability between the two economies' systems (a "trans-Tasman" approach), through the goal of mutual recognition of digital identity services.[79] This is part of a longstanding work programme to create a seamless 'Single Economic Market' between the two economies.

In 2019, a joint report by the Australian Productivity Commission and the New Zealand Productivity Commission recommended mutual recognition of digital identities (along with a range of other cooperation activities relating to digital trade and e-government) to grow the digital economy and maximise opportunities for MSMEs.[80]

Trans-Tasman digital identity work builds on workstreams across a number of related digital economy and business law harmonisation areas between Australia and New Zealand, including the mutual recognition of business registration numbers and the creation of an Australia and New Zealand Electronic Invoicing Board and adoption of the PEPPOL standard for e-invoicing. Interoperability of drivers' licences has also been proposed.[81]

Both economies have also prioritised international interoperability in the design of their individual trust frameworks – in New Zealand's case, for example, explicitly seeking to align with trust frameworks in Australia, Canada and the United Kingdom, and both integrating mutual recognition into recent trade agreements.[82]

[78] https://www.mas.gov.sg/news/media-releases/2021/singapore-and-thailand-launch-worlds-first-linkage-of-real-time-payment-systems
[79] https://www.beehive.govt.nz/sites/default/files/2022-07/Joint%20Statement%20-%20ANZLM%202022.pdf
[80] Australian Productivity Commission and New Zealand Productivity Commission (2019), *Growing the Digital Economy in Australia and New Zealand*
[81] Radio New Zealand, 18 July 2022, 'Activation of new facial recognition technology expected within the next year', rnz.co.nz/national/programmes/morningreport/audio/2018849817/activation-of-new-facial-recognition-technology-expected-within-the-next-year
[82] https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/about-the-digital-identity-programme/

Principles for mutual recognition

The development of a common set of principles for digital identity systems across economies could help to foster confidence about the basis for regulatory frameworks. Such principles-based approaches have been discussed internationally in recent years.

For example, the Digital Identity Working Group of the 'Digital Government Exchange' (DGX) is chaired by Australia's Digital Transformation Agency and involves APEC economies Australia, Canada, New Zealand and Singapore, while China (represented by Shanghai) and the United States (represented by New York) are also in the broader DGX group.[83]

The Working Group published a report and set of principles for mutual recognition of digital identities in early 2022.

The report finds that mutual recognition and interoperability are important goals for digital identities, but still several years away, with foundational activities needed first including the creation of a common "language" and definitions across digital identities; the assessment and alignment of respective legal and policy frameworks; and the creation of interoperable technical models and infrastructure.

Positively, the report also finds that most existing centralized, government-led initiatives have been designed with mutual recognition and interoperability in mind – even where international interoperability was not considered as an immediate use case.

The 11 DGX principles include:

- *openness;*
- *transparency;*
- *reusability;*
- *user-centricity;*
- *inclusion and accessibility;*
- *multilingualism;*
- *security and privacy;*
- *technology neutrality and data portability;*
- *administrative simplicity;*
- *preservation of information;*
- *and effectiveness and efficiency*

Similarly, the World Bank has also developed a set of principles on "identification for sustainable development", grouped into three categories of inclusion, design and governance. The principles are similar to those of DGX and include concepts of:

- *universal, non-discriminatory access;*
- *a responsive and interoperable platform;*
- *the use of open standards to help prevent vendor and technology lock-in;*
- *privacy and security by design; the need for financial and operational sustainability;*
- *the need to safeguard rights through comprehensive legal and regulatory frameworks;*
- *and the enforcement of legal and trust frameworks through independent oversight.*[84]

Four APEC economies (Korea, Canada, Mexico and New Zealand) are also members of the 'Digital Nations' group, which has its own working group on digital identity and has endorsed the World Bank principles.[85]

[83] https://www.tech.gov.sg/media/corporate-publications/digital-government-exchange-reports

[84] https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

[85] https://www.leadingdigitalgovs.org/digital-identity

Case Study: The European Union's cross-border eIDAS system

The most successful "cross-border" model to date is in the European Union (EU). In 2014 the EU developed a sophisticated system to enable the interoperability of Member States' electronic identification schemes.[86] European citizens and businesses can use their national electronic identity to access public services in other EU members which also have electronic identity systems. The eIDAS system means that there can be secure, legally-recognised and seamless digital transactions across the EU economies, supporting other workstreams seeking to create a European Digital Single Market. The Network consists of a number of interconnected eIDAS Nodes which can either request or provide cross-border authentication. Public or private "Service Providers" can connect to this network and offer access via a digital wallet. The EU is currently in the process of updating this system with new digital wallets that could link national digital identities with proof of other attributes such as a driver's licence or bank account.[87]

Other institutional approaches to tackle fragmentation

There are also various international initiatives in train to try to address the issue of fragmentation. Extensive policy work has been undertaken by the Organization for Economic Development and Cooperation (OECD), World Bank, and the World Economic Forum on the policy issues and design of robust digital identity approaches.

At a more practical level, in 2021 the UN Commission on International Trade Law (UNCITRAL) developed a draft model law, the 'Draft Provisions on the Use and Cross-Border Recognition of Identity Management and Trust Services'.[88] This aims to promote uniformity in the development and application of operational rules, policies and practices for identity management. The draft points towards the use of international standards and suggests that enacting jurisdictions determine equivalency of "reliability" in the other economy's system.

Cross-border interoperability via specific use cases, sectors or providers

Another possible approach to achieving greater cross-border coherence, at least for trade and business, could be to focus on the interoperability of specific use cases or systems established by providers such as mobile operators, financial institutions or technology companies which offer large networked platforms and have become de facto digital identity gatekeepers.

Sector- or provider-specific approaches clearly fall short of addressing fragmentation within and across economies – that is, enabling individuals or firms to have a portable digital identity they can use *anywhere*, for *anything* – but there could be benefits in enabling greater integration in specific sectors as a transitional approach while the broader digital identity infrastructure is developed within and across economies.

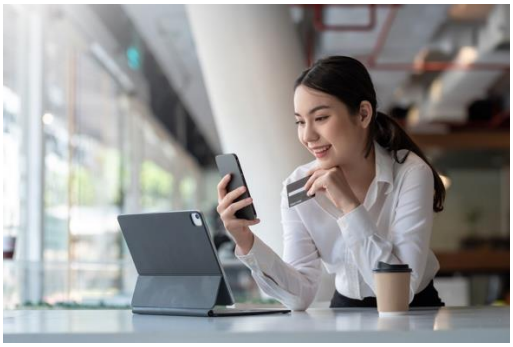
On the other hand, there may also be risks and disadvantages in such approaches: such systems (unless open source/open access) can potentially have an outsized influence on the development of this foundational infrastructure, given the size and reach of some providers' customer bases and their dominance in the digital economy (whether in financial services/payments markets, or with respect to devices or the delivery of services). It seems clear that no single stakeholder can achieve all of the needed changes to facilitate cross-cutting digital identity infrastructure, whether of individuals or corporate entities – but also that there is strong value in close

[86] OECD (2021), G20 Collection of Digital Identity Practices
[87] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663
[88] https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/009/38/PDF/V2200938.pdf?OpenElement

partnerships between policymakers and the private sector.

Examples of initiatives with cross-border or global reach include:

- The Institute of International Finance (IIF) is collaborating with the OpenID Foundation, private sector firms and officials in the **'Open Digital Trust'** initiative. The initiative aims to develop a vibrant marketplace for Digital Trust services (provided by banks and insurers) to help individuals and entities to confirm identity and understand and manage risk.[89]
- As earlier noted, IIF, the OpenID Foundation, the Global Legal Entity Identifier Foundation and others are advocating for a **'Global Assured Identity Network' (GAIN)** which would establish a user-centric and high-trust global network.[90]
- The **ID2020 Global Alliance**, founded by Microsoft, Accenture and others from the private, non-profit and public sector, is seeking to accelerate the uptake of robust, ethical digital identities, including through establishing a Certification Mark.[91]
- The **'Mobile Connect'** programme of the GSMA is a global, open and common framework which supports authentication, authorisation, identity and attribute sharing and verification via mobile operators. It combines a user's unique mobile number and authentication factors to verify the user. Combined with the mobile device, mobile network and operators' business-process security, it can enable e-commerce, payments and services.[92]
- **Mastercard** is working with the public and private sector to develop a global identity network.[93] It has gained DITF accreditation in Australia and wants to conduct a series of private sector-led pilots to verify age and identity in the retail sector.[94] It is also partnering with Thailand's National Digital Identity (NDID) system for pilots for bank account opening and mobile phone registration,[95] and is in discussion with Singapore about possible collaboration.[96] It has also partnered with Microsoft for fraud prevention in e-commerce.[97]
- **Multinational technology companies** such as Apple, Google, Meta and Microsoft provide identities to access multiple platforms or online services around the world.



Technical standards to support interoperability

Greater alignment with recognised international, open standards could help to boost the economic benefits of digital identities, creating economic value more

[89] https://www.iif.com/Innovation/Open-Digital-Trust-Initiative

[90] GAIN (2021), *GAIN Digital Trust: How financial institutions are taking a leadership role in the digital economy by establishing a Global Assured Identity Network.* A Proof-of-Concept was developed under the auspices of the Cloud Signature Consortium, the Global Legal Entity Identifier Foundation, the IIF, OpenID Foundation and Open Identity Exchange

[91] https://id2020.org/

[92] GSMA (2018), *Digital Identities – Advancing digital societies in Asia Pacific;* and https://mobileconnect.io/operators/

[93] https://www.mastercard.com/news/perspectives/2021/digital-id-in-a-virtual-world-how-to-prove-that-you-are-really-you/

[94] https://www.zdnet.com/article/mastercard-and-dta-to-scope-out-digital-id-service-for-age-verification/

[95] https://www.biometricupdate.com/202203/thailands-ndid-partners-with-mastercard-to-connect-digital-ids-internationally

[96] https://www.biometricupdate.com/202111/cross-border-digital-id-is-coming-mastercard-plans-to-supply-infrastructure

[97] https://news.microsoft.com/2022/04/25/mastercard-launches-next-generation-identity-technology-with-microsoft-to-help-more-consumers-shop-online-safely/

quickly and widely, both within and across economies, by fostering cross-economy interoperability at the technical level. A number of standards are being developed internationally, including:

- the International Standards Organization (relating to cybersecurity and privacy standards for digital identities, biometric application programming interfaces and IT security techniques for biometric information) [98];
- the FIDO Alliance, an open industry association which develops standards for authentication and device attestation[99];
- the World Wide Web Consortium (W3C), a non-profit international standardisation organization whose member organizations collaboratively develop Web standards. W3C is seeking to develop a set of standards to interlink different sources of data under the control of the user. It has developed a Verifiable Credentials Data Model and Decentralized Identifiers protocol to provide a standard way to express identity credentials for any subject (people, company, physical or digital objects or even documents).[100]
- The Decentralized Identity Foundation (DIF), an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interop between all participants. Through its range of working groups extending and profiling the W3C Verifiable Credentials (VC) and Decentralized IDentity (DID) specifications, it develops the essential 'plumbing' needed to scale decentralized identity. With over 200 DID methods published, the future interoperability challenges and choices are self-evident for platform and wallet providers
- Trust over IP Foundation (ToIP), developed under the auspices of the Linux Foundation that joins together Governance and Technology into a stack of protocols (the from W3C and others) and rules to deliver both technical trust and human trust to the decentralized identity ecosystem.
- Open Wallet Foundation (OWF), a nascent group which seeks to develop an open source engine to enable secure and interoperable multi-purpose wallets anyone can use to build solutions. The OWF aims to set best practices for digital wallet technology through collaboration on open source code for use as a starting point for anyone who strives to build interoperable, secure and privacy-protecting wallets.

Many businesses and other organizations also make use of APIs (application programming interfaces – a technical 'interoperability' mechanism), allowing their services to access user data (with user consent) from other services, provided the format and structure of data is broadly similar.

[98] For example, ISO/IEC 24760-1:2019 IT and ISO/IEC 24745:2011. TRPC (2020), *Australia-Singapore Digital Trade Standards*

[99] https://fidoalliance.org/overview/

[100] https://www.w3.org/

Section 5: Using trade agreements to address digital identities

It is somewhat surprising that few of the region's trade agreements – even those with ambitious digital trade chapters – include provisions on digital identities. For example, digital identities are not explicitly referenced in any of the largest FTAs in the Asia-Pacific, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Regional Comprehensive Economic Partnership Agreement (RCEP), the US-Mexico-Canada FTA (USMCA), the US-Japan Digital Trade Agreement, or the ASEAN E-Commerce Agreement. This is despite these agreements including many other "modern" digital trade provisions, including closely related issues such as e-signatures and electronic authentication.[101]

Notable exceptions are the handful of "digital economy agreements" (DEAs) that have been developed by a number of APEC economies since 2020. These include the Digital Economy Partnership Agreement (DEPA) among New Zealand, Singapore and Chile (to which Korea is in the process of acceding, and China and Canada are seeking to accede); the Australia-Singapore Digital Economy Agreement (SADEA); and the UK-Singapore Digital Economy Agreement (UKSDEA), both of the latter closely linked to comprehensive bilateral FTAs. The Singapore-Korea Digital Partnership Agreement, still being finalised, similarly foreshadows the inclusion of digital identities.

DEA approaches to digital identity

The approach taken in DEAs on digital identities reflects the fact that policy development on cross-border interoperability is at a relatively nascent stage. The preambular or framing language typically used in the DEAs recognises the value of cooperation on digital identities to enhance regional and global connectivity, and also acknowledges that economies may have different legal and technical approaches – but also that this should not necessarily stand in the way of deeper cross-border integration. A recent press release on the Singapore-Korea Digital Partnership Agreement negotiations sets out the case for cross-border action:

> *"In the digital world, secure and trusted digital identities enable greater and easier access to services for both individuals and companies. Singapore and the Republic of Korea seek to cooperate to promote interoperability between the respective digital identity regimes, which can bring benefits such as more reliable identity verification and faster processing of applications. This would in turn reduce barriers in cross-border trade and enable businesses and individuals to navigate the international digital economy with greater ease, confidence and security."*[102]

None of the agreements includes a definition of "digital identities" as such, although of note, the DEPA explicitly encompasses both corporate as well as individual digital identities. In the main, the provisions focus on cooperation, and in particular, signal the intention to pursue interoperability or compatibility across the economies' different regimes.

This interoperability is tackled across multiple "layers" – including technical interoperability

[101] Other than the DEAs discussed in the subsequent paragraph, other trade agreements including digital identities appear to be limited to the recent United Kingdom-New Zealand and United Kingdom-Australia FTAs, and the India-UAE Comprehensive Economic Partnership Agreement, all concluded in late 2021 and 2022. See the TAPED database developed by Mira Burri at the University of Lucerne, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/

[102] https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA

or common technical standards; the development of comparable protection of digital identities under each Party's respective legal frameworks, or the recognition (either autonomously, or through mutual recognition) of the legal effects of those frameworks; and support for the development of international frameworks for digital identities.

The DEAs also typically direct the participating economies to exchange knowledge and expertise on best practices when it comes to policies, regulations, technical implementation and security standards, and on the uptake of digital identities by users. In the case of both the Australia-Singapore DEA and the UK-Singapore DEA, separate Memoranda of Understanding (MoUs) set up detailed work programmes aimed at achieving mutual recognition – see the case study below.

Case Study: Singapore MoUs on digital identity with Australia and the United Kingdom

Singapore and Australia have agreed an MoU on the mutual recognition of digital identities in connection with their bilateral Digital Economy Agreement.[103] The MoU sets up a work programme which focuses on sharing best practices and working cooperatively to explore issues around legal, regulatory, policy and user uptake elements. The areas of cooperation include:

- legal and regulatory frameworks supporting digital identities (including the status of electronic signatures and other trust services; liability and contracts legislation; accreditation of digital identity operators; and data storage and data privacy);
- technical standards for the implementation of digital identities (including conceptual architecture models for mutual recognition; specifications of identity management systems; security and monitoring requirements; and vocabularies and schema of data elements);
- policies relating to digital identities (including business processes, responsibilities and expectations; scope and governance of digital identities and trust frameworks; documentation of rules; and audit requirements);
- and adoption of digital identities by individuals and businesses to promote the use of digital transactions.

An even more detailed work programme is established by an MoU agreed between Singapore and the UK.[104] This includes a similar approach to the Singapore-Australia MoU on cooperation across legal and regulatory frameworks, governance and operational processes, standards and adoption, but providing significantly more granular detail on cooperative activities, and incorporates new elements such as market development and the interdependencies between digital identities and other policy and product innovation areas such as cross-border digital trade facilitation, financial services, digital currencies, payments, e-signatures, e-KYC and anti-money laundering requirements. It also provides for the development of pilot projects such as opening bank accounts and applying for visas using digital identities.

It will be worth watching exactly how economies seek to resolve the challenges of mutual recognition, given some significant differences in digital identity approaches in respective economies – for example, between Singapore (a centralized system), Australia (a federated system) and New Zealand (a decentralized approach which is still under development), and whether over time this leads to more coherent approaches across the region overall.

[103] https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement

[104] https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA

Section 6: Conclusions

There are significant upsides to building the foundational infrastructure of trusted digital identities in the APEC region – and significant downsides and missed opportunities in failing to do so.

Digital identities can help to achieve critical elements in the region's resilience and renewed growth in the face of ongoing pandemic and other disruptions, including the potential to:

- unlock significant economic value
- achieve greater inclusion within and across economies, including for MSMEs and underserved groups
- facilitate more streamlined and straightforward access to government services
- reduce friction in e-commerce and in services trade
- achieve more secure and simple financial services transactions and stability in financial markets
- enable more trusted and secure business processes
- achieve better privacy and data protection
- and facilitate safe and seamless travel –.

Economies should ideally develop their own robust approaches, integrating critical features such as strong privacy, cybersecurity, inclusion, and interoperability elements. Digital identity approaches will also need to be scalable, sustainable, and trusted – this points not only to good design, but also to economies actively seeking to raise awareness of the potential benefits of digital identities and how consumers and businesses can access them and exercise their rights. Ensuring that systems are supported by strong digital physical infrastructure (broadband and mobile) will also support uptake.

Business and policymakers can, and indeed, must work collaboratively on all of these elements. The private sector can play an important role in building out the infrastructure, for example by gaining accreditation as identity services providers, and helping to drive greater interoperability through their own initiatives. At the same time, the development of digital identity ecosystems holds the promise of creating valuable new business opportunities, where the private sector can provide innovative and competitive over-the-top value-adding services linked to digital identities.

There is significant promise in achieving digital identities that can be interoperable across borders as well as within them. Economies will have their own policies and approach to the design of digital identity systems, but it should be possible – albeit challenging – to develop more coherent approaches.

APEC provides an ideal platform for economies to work collaboratively to develop such cross-regional approaches. It has a track record of working collaboratively on approaches to important digital economy issues such as privacy, as well as practical tools like the digitalized APEC Business Travel Card.

APEC also has the advantage of a solid foundation for strategic action in the form of the APEC Internet and Digital Economy Roadmap (AIDER). Although the AIDER does not specifically refer to digital identities, taking action in this area would resonate with many AIDER priorities, including the development of digital infrastructure, promotion of interoperability, the promotion of coherence and cooperation in regulatory approaches, the adoption of enabling technologies and services, enhancing trust and security, enhancing inclusion and facilitating e-commerce and digital trade.

APEC economies could start the process by sharing experiences and best practices, and build on these to develop a set of "APEC Principles for Digital Identity" as a basis for a more coherent and interoperable regional approach.

Recommendations

- Economies should design digital identity systems at the economy level that incorporate strong privacy and cybersecurity protections, are user-centric, are inclusive, sustainable and scalable, and integrate interoperability. This should be based on a set of coherent principles for good digital identity developed in APEC;
- Economies should engage closely with the private sector on the design and implementation of digital identity systems, and foster an enabling and competitive business environment and ecosystem;
- Economies should seek to boost uptake and foster cross-border interoperability, including by strengthening awareness and digital literacy, and pursuing interoperability mechanisms including mutual recognition and tailored approaches for specific use cases.

Glossary

Digital identity systems use a number of specialized terms to describe different components of the system.[105] These terms include:

- "**attributes**" – small pieces of information that make up a digital identity. They are normally distinct characteristics of a subject or of an object that help to describe it, such as a name, address, or date of birth for a subject; or for an object, geocoordinates or product/location characteristics may be used.
- "**credential**" – a package of information or evidence which is provided to an identity provider which contains authenticated information about an individual and that allows them to gain access to services or the network. The most common credentials are a username or passport.
- "**biometrics**" include fingerprints, facial recognition or an iris scan, used for identification. Biometric identifiers can themselves be used for digital identities, but also as a secure way to open a digital wallet containing other digital identity credentials.
- "**authentication**" is the process of confirming a claimed identity. ("Who are you?") For example, logging in to a secure website requires authentication.
- "**authorization**" is the activity or access to the service that your digital identity unlocks ("What are you allowed to do?")
- "**verification**" is the process of establishing, to a required level of assurance, the authenticity of a digital identity.
- "**assurance**" is a positive declaration intended to give confidence in the authenticity of an identity. There can be different levels of assurance given, depending on the level of risk.
- "**identity provider**" provides identity information about an individual, organization or object.
- "**relying party**" is a provider of services that are being accessed by an individual or entity using a digital identity – that is, they *rely* on the identity information being offered in order to provide the service. For example, a bank may be a relying party when it comes to meeting compliance requirements for anti-money laundering regulations.
- "**user**" is the individual, firm or entity that is being identified.

[105] Definitions are drawn from the World Bank (2019) ID4D Practitioner's Guide (idem), and from the New Zealand Service Innovation Lab Toolkit's *Digital Identity Glossary* https://serviceinnovationlab.github.io/digital-identity-glossary .

References

Arner, D., Zetsche, D., Buckley, R., Barnberis, J. (2018), 'The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities', European Business Organization Law Review, Forthcoming UNSW Law Research Paper No. 18-45, European Banking Institute Working Paper Series 2018 No. 28, University of Luxembourg Law Working Paper No. 2018-008, University of Hong Kong Faculty of Law Research Paper No. 2019/029, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3224115

Australian Productivity Commission and New Zealand Productivity Commission (2019), *Growing the Digital Economy in Australia and New Zealand,* www.productivity.govt.nz/research/growing-digital/

Digital Gov Exchange (2022), *Digital Identity in Response to COVID-19*, DGX Digital Identity Working Group; Digital Transformation Agency of Australia, https://www.tech.gov.sg/media/corporate-publications/digital-government-exchange-reports

GAIN (2021), *GAIN Digital Trust: How financial institutions are taking a leadership role in the digital economy by establishing a Global Assured Identity Network*, https://gainforum.org/

Garber, E., Haine, M., Knobloch, V., Liebbrandt, G., Lodderstedt, T., Lycklama, D., Sakimura, N. et al (2021), *GAIN Digital Trust, How Financial Institutions are taking a leadership role in the Digital Economy by establishing a Global Assured Identity Network,* European Identity and Cloud Conference, Munich, Germany, 13 September 2021, https://gainforum.org/GAINWhitePaper.pdf

GSMA (2021), 'Commercially sustainable roles for mobile operators in digital ID ecosystems, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/03/Commercially-Sustainable-Roles-for-Mobile-Operators-in-Digital-ID-Ecosystems.pdf

GSMA (2018), *Digital Identities – Advancing digital societies in Asia Pacific*, (Report authored by James Robinson, Barbara Arese Lucini and Jeanette Whyte, TRPC), https://www.gsma.com/asia-pacific/resources/digital-identities-advancing-digital-societies-in-asia-pacific/

HK Financial Services Development Council (2018), *Building the Technological and Regulatory Infrastructure of a 21st Century International Financial Centre: Digital ID and KYC Utilities for Financial Inclusion, Integrity and Competitiveness*, FSDC Paper No.35, https://www.fsdc.org.hk/en/insights/building-the-technological-and-regulatory-infrastructure-of-a-21st-century-international-financial-centre-digital-id-and-kyc-utilities-for-financial-inclusion-integrity-and-competitiveness

Leung, D., Nolens, B., Arner, D. and Frost, J., (2022), *Corporate Digital Identity: No Silver Bullet, but a Silver Lining*, BIS Papers No. 126, Bank for International Settlements (2022), https://www.bis.org/publ/bppdf/bispap126.htm

McKinsey & Company (2020), 'How governments can deliver on the promise of digital ID', report by Domeyer, A., McCarthy, M., Pfeiffer, S., and Scherf, G., https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

McKinsey Global Institute (2019), *Digital Identification: A key to inclusive growth, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth*

Monetary Authority of Singapore (2021), *Foundational Digital Infrastructures for Inclusive Digital Economies*, https://www.mas.gov.sg/-/media/MAS/Fintech/FDI/Foundational%20Digital%20Infrastructures%20for%20Inclusive%20Digital%20Economies.pdf

NATA, JAS-ANZ and GS1 (2022), *Digitalisation of Conformance and Accreditation Processes*, https://nata.com.au/supplychain/

NCAPEC (2022), *Advancing Digital Transactions in APEC: Enhancing E-Signatures and Digital Signatures*, NCAPEC Working Group on E-Signatures, March 2022

OECD (2021), *G20 Collection of Digital Identity Practices - Report for the G20 Digital Economy Task Force*, August 2021. https://read.oecd-ilibrary.org/governance/g20-collection-of-digital-identity-practices_75223806-en#page9

OECD (2020), 'Tracking and tracing COVID: Protecting Privacy and Data while using apps and biometrics', https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

OECD (2019), *Digital Government in Chile – Digital Identity*, https://www.oecd.org/gov/digital-government/digital-government-in-chile-digital-identity-9ecba35e-en.htm

PECC and Access Partners (2021), *PECC Signature Project on the Digital Economy: Primer on Economic Integration Issues Posed by the Digital Economy*, 22 October 2021, https://www.pecc.org/resources/digital-economy/2705-pecc-signature-project-primer-on-economic-integration-issues-posed-by-the-digital-economy/file

TRPC (2020), *Australia Singapore Digital Trade Standards Research Report*, https://www.dfat.gov.au/publications/trade-and-investment/australia-singapore-digital-trade-standards-research-report

UNCTAD (2022), *Why robust digital identity systems are essential in fostering trade and development*, Policy Brief No. 96, March 2022, https://unctad.org/webflyer/why-robust-digital-identity-systems-are-essential-fostering-trade-and-development

UNCTAD (2021), *Digital Identity for Trade and Development: TrainForTrade Case Studies in Southeast Asia, https://unctad.org/system/files/official-document/dtlkdb2020d1_en.pdf*

World Bank (2021), 'Digital ID systems as an enabler of effective COVID-19 vaccination', by Marie Eichhotzer and Jonathan Maskell, 25 November 2021, https://documents1.worldbank.org/curated/en/347681639416116412/pdf/Digital-ID-Systems-as-an-Enabler-of-Effective-Covid-19-Vaccination.pdf

World Bank (2020), *ID4D 2020 Annual Report*, http://documents1.worldbank.org/curated/en/625371611951876490/pdf/Identification-for-Development-ID4D-2020-Annual-Report.pdf

World Bank (2019), *ID4D Practitioner's Guide*, World Bank Working Paper number 137292, 11 June 2019, https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

World Bank (2019), *The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth*, Information and Communications for Development. World Bank, Washington, D.C.. License: Creative Commons Attribution CC BY 3.0 IGO, https://openknowledge.worldbank.org/handle/10986/31803

World Bank Group, GSMA, Secure Identity Alliance (2016), *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, July 2016, https://www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/

World Economic Forum (2019), Global Risks Report, page 22; https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

World Trade Organization and World Economic Forum (2022), *The Promise of TradeTech – Policy approaches to harness trade digitalization*, https://www.wto.org/english/news_e/news22_e/publ_12apr22_e.htm