

Digital Identity in ASEAN

US-ABC Financial Services Committee Whitepaper

[DATA PROTECTION]



INTRODUCTION

The need for secure, trusted, and instantly verifiable identities is rapidly growing, as people, businesses, and governments conduct more of their lives and services digitally, particularly as the COVID-19 pandemic has accelerated digital transformation in many countries. Digital identity is a form of personal identification and verification that can be authenticated through a digital channel. As ASEAN's digital economy continues to grow (more than 400 million people are now online in the region) the ability to transact digitally will become increasingly important. The Council recognizes that many ASEAN member states have begun implementing digital identity systems, including Brunei, Indonesia, Malaysia, Singapore and Thailand¹. This paper sets some context to those developments as well as some recommendations for policymakers as these schemes move forward.



1. <http://documents1.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf>

Benefits

There are two key benefits to the successful rollout of digital identity schemes in ASEAN:

1. Unlocking the digital economy

Digital ID is foundational to the digitalization of economies, removing the need for in-person authentication of individuals or documents by unlocking digital access to financial services such as insurance, payments, lending and account opening. Digital identity also has the potential to allow consumers to transact much more broadly within the digital economy. A McKinsey study for example identified six broad areas where digital identity brings specific benefits:

CONSUMERS

Secure digital payments and eKYC for financial services

WORKERS

Background verification and payroll services

MICRO-ENTERPRISES

Business registration and contracts

GOVERNMENT SERVICES

Digital tax filing, distribution of benefits

GOVERNMENT ENGAGEMENT

Online voting, school enrollment

ASSET OWNERSHIP

Facilitating sales and purchases of assets such as land and housing²

Digital identity can also provide benefits in the pandemic, via sharing traveler information (e.g., recent travel history, health certification) in a secure manner to government agencies and other related stakeholders.

2. Broadening financial inclusion

Digital identity also has significant potential as a tool for inclusion. Around 65 million people in ASEAN are thought to lack a legally recognized form of identity.³ This “identification gap”⁴ has been recognized in the UN SDGs⁵ and is an inhibitor of access to the formal economy, including financial services in countries with extensive consumer banking services.⁶

In India, the Aadhaar identity scheme has in recent years brought legal identity to many hundreds of millions of people and allowed bank penetration levels to move from 35% in 2011 to more than 80% today.⁷

Open and competitive frameworks based on international standards are the best way to promote financial inclusion and inclusive growth. These frameworks allow technology providers to interoperate and deliver services, thereby expanding reach and impact.

Availability of digital access as well as “digital identity literacy” so that citizens understand their rights are key to the success of such schemes and of particular importance to lower costs and barriers to entry. This is an area that offers opportunities for government and the private sector to work together to determine a principles-based approach to consumer data use and the processes and technologies that best achieve those goals.

“

Open and competitive frameworks based on international standards are the best way to promote financial inclusion and inclusive growth. These frameworks allow technology providers to interoperate and deliver services, thereby expanding reach and impact.

”

2. Digital Identification: a key to inclusive growth. McKinsey, 2019

3. The global figure is around one billion

4. World Bank: Identification for Development: <https://id4d.worldbank.org/global-dataset>

5. UN SDG 16.9: by 2030 provide legal identity for all including free birth registrations

6. Banking the next billion: Citi GPS: <https://ir.citi.com/pN%2BOIBahjzmpHvliXxcaHdn%2BlkONN7NB7I3YKzIQvpsbYI%2BriiOLJyscLIG8hM%2FoOLIOCKhz8IO%3D>

7. The so-called JAM framework: Jan Dhan basic accounts + Aadhaar + Mobile access. Mobile penetration levels in ASEAN for example are around 80% in Malaysia, 75% in Vietnam and around 65% in Indonesia and the Philippines (GSMA).

3. Other advantages

Further benefits from digital identity schemes include:

- *Removing system fragmentation by replacing multiple ID documents*
- *Improving efficiency by removing frictions and improving processes*
- *Increasing tax compliance through a more formalized economy*
- *Increased productivity through a reduction in time and cost savings*

Taken together these benefits can amount to more than 10% of GDP in some countries.⁸

Operating Models

There are multiple models for providing digital identity, which are often summarized as either:

Centralized: these tend to be provided mainly by the state, as in India. Centralized models can play a transformative role from an inclusion standpoint but have raised challenges around privacy rights and weak security standards.⁹ Singapore's National Digital Identity scheme (the foundational elements of which can be seen as centralized) attempts to overcome some of these challenges in the way privacy and security are managed. For example, Singapore's collaboration with the private sector to deploy a Fraud and Analytics system is further strengthening security and improving usability.

Decentralized: Under decentralized identity models, ultimate control of identity data sits with the user, thus shifting even further from traditional identity management approaches. This approach is gaining traction in places such as Europe and Canada and

among those who favor using certain technologies, such as DLT or blockchain.

Federated: Federated identity models, where several entities (perhaps through a particular framework) let subscribers use the same identity data to obtain access to the networks of all of the enterprises in the group, are being widely adopted, as open banking and other data-sharing services proliferate. Australia's Trusted Digital Identity Framework (TDIF) is an example of a federated, user-centric system, where multiple entities can become certified identity providers and the individual can choose his or her identity provider and consent to the data shared. Australia's Digital Transformation Agency led a highly collaborative public-private partnership process in developing this framework, requesting comment through multiple iterations of the industry standards. Thailand's NDID scheme also represents a more federated model, where financial institutions operate as identity providers and one of a range of "authoritative sources" with transactions taking place across the NDID platform.

Sweden's federated BankID scheme has become a key part of the digital economy in an almost cashless society. Almost 100% of the population aged 21-60 uses the scheme an average of 40-50 times per month. BankID is a credential issued by a participating banking institution that can be used for digital identification and takes various forms including mobile application, physical card and USB file.

Financial institutions play an important role in performing checks on individuals and businesses in respect of KYC, AML, and sanctions. Bank accounts are also the primary store of value in economies and banks' balance sheets the primary source of lending. Banks are therefore well positioned to play a role in providing a basis for secure digital credentials.

In addition to the operating model, other key considerations include: the regulatory environment, governance, technology, trust, privacy and security.

8. *Digital Identification: a key to inclusive growth*. McKinsey, 2019

9. <https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-why-privacy-still-remains-a-central-challenge/articleshow/65970934.cms?from=mdr>

PRINCIPLES / RECOMMENDATIONS

1. Include strong privacy and user right protections:

Effective digital identity frameworks depend on trust. Consumers will not use services or technology they do not trust. In order to promote trust among users, identity systems must ensure privacy and security are central to scheme design. For example, digital identity frameworks should incorporate “privacy by design” principles where user privacy is proactively embedded into the framework, incorporating well-established principles such as consent, user control, and data minimization will help instill confidence in the establishment of digital ID schemes.

2. Allow for risk-based KYC:

Anti-money laundering and countering the financing of terrorism (AML/CFT) and Know Your Customer (KYC) provisions are critical applications of digital identity solutions. Traditional KYC verification requirements such as multiple forms of identification and proof of a physical address can be difficult for low-income, unbanked, or marginalized individuals to provide. Proportional, risk-based, KYC frameworks can help protect the financial ecosystem while supporting financial inclusion goals by facilitating the onboarding process for unbanked and underbanked populations. Furthermore, the ability to securely, efficiently, and seamlessly identify consumers and authenticate their transactions is vital to allow mobile commerce (“m-commerce”) and e-commerce to grow, especially in developing countries.

3. Adopt open and interoperable standards:

Interoperable, harmonized, global standards ensure connectivity to the international financial system, which is necessary for financial inclusion and for economic growth, especially in developing nations. As the principles on identification for sustainable development note, “using open standards and ensuring vendor and technology neutrality” and “creating a platform that is interoperable and responsive to the needs of various users” will be important ways to develop a broadly applicable and workable scheme.

4. Adopt a collaborative approach:

One of the reasons for the success of the BankID scheme in Sweden is that the fundamental approach was one of collaboration rather than competition between participants in the system. That factor, along with others such as compliance with an existing strict set of regulatory requirements, engendered trust.

5. Provide opportunities for public and private sector collaboration:

This allows ecosystem players to contribute to the development of the frameworks in which they will participate. When governments support frameworks that allow technology providers to link in and deliver services, they expand the reach and impact of their investments.

6. Seek cross-border recognition:

The cross-border benefits of digital ID mean that efforts to seek recognition and use of domestic schemes in other jurisdictions is also important. The EU electronic Identification Authentication and trust Services (eIDAS) regulation offers one example of rules which seek to achieve mutual recognition of digital ID across borders. The Singapore-Australia Digital Economy Agreement also seeks a similar objective via an MOU in the agreement.

“

Digital identity has the potential to allow consumers to transact much more broadly within the digital economy. Availability of digital access as well as “digital identity literacy” so that citizens understand their rights are key to the success of such schemes and of particular importance to lower costs and barriers to entry.

”



CONCLUSION

There are many potential benefits of digital identity, as well as a range of different policy implications and operating models to be considered. The principles above are an attempt to formalize some of these considerations into recommendations for policymakers in developing digital ID schemes.

The US-ASEAN Business Council looks forward to discussing these issues in more detail.



ABOUT THE US-ASEAN BUSINESS COUNCIL



For over 35 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the Council's membership, more than 160 companies, generate over \$6 trillion in revenue and employ more than 13 million people globally. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years.

We believe opening and investing in the sustainability of efficient, resilient and competitive markets are critical to the continued growth of our member companies and innovation and job creation in the United States and Southeast Asia.

The Council has offices in: Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore. The Council's Financial Services Committee is made up of over 20 of the world's leading financial services institutions and markets participants operating in Asia's most dynamic regional economic community.

