UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

DIGITAL IDENTITY FOR TRADE AND DEVELOPMENT

TrainForTrade case studies in South-East Asia

Strengthening knowledge

and skills through innovative approaches

for sustainable economic development

UNITED NATIONS

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

DIGITAL IDENTITY FOR TRADE AND DEVELOPMENT

TrainForTrade case studies in South-East Asia

Strengthening knowledge

and skills through innovative approaches

for sustainable economic development

UNITED NATIONS
Geneva, 2020

United Nations publication issued by the United Nations Conference on Trade and Development.

UNCTAD/DTL/KDB/2020/1

eISBN: 978-92-1-005302-0

Notes and acknowledgements

This publication was produced in the framework of the TrainForTrade Programme of the United Nations Conference on Trade and Development (UNCTAD), financed by the United Nations Development Account Tranche 11 for South-East Asia region.

The summaries of the featured dissertations and participants' career profiles were prepared by Shuaihua Wallace Cheng, Cécile Barayre, Dominique Chantrel, Tomasz Kulaga, Debbie Francisco, Martine Julsaint Kidane, Erika Morishita, under the supervision of Mark Assaf, Chief of the Human Resources Development Section-TrainForTrade and the overall guidance of Geneviève Féraud, Head of the Knowledge Development Branch, Torbjörn Fredriksson, Chief of the Information Communication Technology Policy Section and Shamika Sirimanne, Director of the Division on Technology and Logistics of UNCTAD and the input from Luca Castellani, legal officer, UNCITRAL, Yann Duval, Chief of Trade Policy and Facilitation Section of Trade, Investment and Innovation Division of UNESCAP. The contribution of Ms. Mariann Kirsipuu, from Estonia, Mr. Rahul Goel, from India, Mr. Kwok Jia Chuan, from Singapore and Ms. Isabelle Durant, Deputy Secretary-General of UNCTAD are greatly acknowledged during the Face-To-Face workshop in Singapore.

We acknowledge the invaluable contribution of the following e-commerce experts, particularly in preparing their country case studies which serves as good reference points for knowledge-exchange in the region: Keo Buntheng from Cambodia; Ms Su Thet Hninn from Myanmar; Mrs Nanci Laura Sitinjak from Indonesia; and Mr Jose Siraj Ballesteros Murad, Mr Arnold Janssen D. Saragena and Ms Jovita J. Vence from The Philippines.

Contact:
Human Resources Development Section
TrainForTrade Programme, Knowledge Development Branch
Division on Technology and Logistics, UNCTAD
Palais des Nations
1211 Geneva 10, Switzerland
E-mail: trainfortrade@un.org
www.unctad.org/trainfortrade

Executive Summary

As connectivity within South-East Asia grows, it is critical for governments to put in place frameworks and mechanisms to leverage these developments and increase the use of digital platforms, while ensuring that there is proper governance, trust and authentication measures to support the development of the digital economy.

Often considered the foundation of a digital economy, the creation of a digital identity system is critical to enable every person to fully participate in their society and economy. Without proof of identity, people may be denied access to rights and services – such as the ability to open a bank account, attend school, access health services, collect social benefits, seek legal protection or otherwise engage in modern society.

Against this backdrop, UNCTAD's 2030 TrainForTrade Development Account Project: Leapfrogging skills development in e-Commerce in South-East Asia includes a component on Digital Identity for Trade and Development (the Project). Designed as a capacity building project, and developed in cooperation with the UNCITRAL, UNESCAP, the World Bank Group and the Ministry of Trade and Industry of Singapore, the global objective of the Project is to facilitate the identification and drafting of policies on digital identity related to trade and development and the implementation of a National Digital Identity Framework (NDIF).

This report explores in Chapter One a brief history of the Project. Chapter Two gives an overview of some of the national strategies undertaken in South-East Asia in the implementation of a digital identity. Chapter Three presents seven selected case studies prepared by the Project's participants, covering the relevant legal and policy frameworks and/or current status of Digital ID development in Cambodia, Indonesia, Malaysia, Myanmar and the Philippines. These selected case studies provide succinct examples of good practices as well as policy recommendations for further development of a National Digital Identity Framework. Chapter Four concludes the publication with a list of recommendations.

The Project's goal of sharing experiences, knowledge and expertise among participants and delegates has been well achieved. Through these case studies, participants shared their specific topics of interest, such as data protection and encryption technology, their experiences of the situation in their country, and also some recommendations for consideration. This allowed for a consolidation of a list of policy level and developer partners' assistance recommendations which are targeted at dealing with specific issues raised by the participants.

Given the participants' overwhelming interest in the implementation of the NDIF, UNCTAD will continue its effort to encourage mutual learning between countries and within their regions in the areas of digital identity. With the support and continued efforts of the respective governments, given the groundwork that is already being done in this area, more progress is expected in the implementation of NDIF across South-East Asia.

Table of contents

Abbreviations and acronyms

AMBD	Autoriti
ASEAN	Association of Southeast Asian Nations
BSP	Bangko
BVN	Bank Verification Numbers (Nigeria)
COMELEC	Commission on Elections
DITD	Digital Identity for Trade and Development
DICT	Department of Information and Communications Technology
DPO	Data Protection Officers
ETDA	Electronic Transactions Development Agency (Thailand)
e-KTP	Indonesian
eKYC	Electronic Know Your Customer
GAA	General Appropriations Act
GOCCs	Other government agencies and Government-owned and Controlled Corporations
GPPB	Government Procurement Policy Board
GSIS	Government Service Insurance System
HMDF	Home Development Mutual Fund
IDEEA	ID Enabling Environment Assessment
IDP	Identity providers
LCROs	Local Civil Registry Offices
MCMC	Malaysian Communications and Multimedia Commission
MDEC	Malaysia Digital Economy Corporation
MoU	Memorandum of Understanding
NDI	National Digital Identity
NDID	National Digital ID Company Limited (Thailand)
NDIF	National Digital Identity Framework
NEDA	National Economic Development Authority
NPC	National Privacy Commission
PbD	Privacy by Design
Philhealth	Philippine Health Insurance Corporation
PhilSys	Philippine Identification System
PHLPost	Philippine Postal Corporation
PNPKI	Philippine National Public Key Infrastructure
PSA	Philippine Statistics Authority

PSN	PhilSys
PSPCC	PhilSys
RFID	Radio-frequency identification
SDG	Sustainable Development Goals
SEC	Securities and Exchange Commission
SSS	Social Security System
TFT	TrainForTrade
UMID	Unified Multi-Purpose ID
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific

Chapter 1

Brief history of the project

ICT Masterplans 2015 and 2020

Since 2003, UNCTAD has been undertaking several activities in ASEAN countries to assist them in the implementation of the ICT Masterplans 2015 and 2020, as well as of the ASEAN Economic Community Blueprint 2025 (AEC blueprint), which set specific measures to build a digitally-enabled regional economy, and to encourage the development of electronic commerce.

While e-commerce is seen as a key component for achieving a regionally integrated economy in ASEAN, some ASEAN member States have not reached a state of readiness which would enable them to capture the many opportunities emerging from e-commerce. In particular, challenges in promoting e-commerce within the ASEAN region include concerns on cybersecurity, lack of trust in online transactions, and lack of strong methods of authentication to tackle issues relating to fraud, which underpins electronic transactions.

The Project

Arising from the above, UNCTAD's 2030 TrainForTrade Development Account Project: Leapfrogging skills development in e-Commerce in South-East Asia includes a component on Digital Identity for Trade and Development ("**Project**"). The Project is designed as a capacity building project, developed in cooperation with the United Nations Commission on International Trade Law (UNCITRAL), United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), the World Bank Group and the Ministry of Trade and Industry (MTI) of Singapore.

The global objective of the Project is to facilitate the identification and build the capacity of policies on digital identity related to trade and development and the implementation of a National Digital Identity Framework (NDIF). This includes defining the limits of data protection and digital identity, the scope of digital identity governance, and the risks and solutions related to digital identity.

The Project was implemented in the following two phases:

(a) eLearning session organised and conducted from 26 August 2019 to 27 September 2019 ("**eLearning Component**"); and

(b) Face-to-face workshop held in Singapore from 29 October 2019 to 1 November 2019 ("**Face-to-Face Workshop**").

The eLearning Component was conducted via an eLearning platform over five specially designed modules:

(a) **Module 1** – Fundamental Concepts of Digital Identity;

(b) **Module 2** – Data Protection;

(c) **Module 3** – ID Usage;

(d) **Module 4** – Governance; and,

(e) **Module 5** – ID Technology Solutions & Risks.

Each of these modules was delivered online via TrainForTrade's eLearning platform. Participants were expected to spend approximately 4 hours per week (at their own pace) to study the material, participate in the discussions on the forum and complete the online tests for each module.

There was a total of 188 participants (of which 70 were women) from the ASEAN countries, of which 98 participants successfully completed the eLearning Component.

Out of the 98 participants who had successfully completed the eLearning Component, 33 participants were selected (of which 10 were women) to attend the Face-to-Face Workshop. A total of 26 participants from both public and private sectors of Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, and Thailand attended the Face-to-Face Workshop.

The Workshop participants were tasked to prepare a case study on one of the modules in the eLearning Component and each gave a short presentation during the Face-to-Face Workshop on a national case study related to Digital Identity for Trade and Development. These case studies were prepared with a view of considering and explaining issues faced in each of the participant's home country.

In between the case study presentations, external speakers/partners provided presentations relating to a range of topics, including on human rights aspects of a Digital Identity Framework, the Aadhaar Digital Identification System, and the move towards paperless trade in the Asia-Pacific Region.

Chapter 2

National Strategies for Digital Identity in South-East Asia

Introduction

Often considered the foundation of a digital economy,[1] the creation of a digital identity system is critical to enable every person to fully participate in their society and economy.[2] Without proof of identity, people may be denied access to rights and services – such as the ability to open a bank account, attend school, access health services, collect social benefits, seek legal protection and safely engage in online transactions.

As indicated in the McKinsey Global Institute report on digital identification, the scope for creating economic value in emerging economies when leveraging on digital identity can be sizable, leading to average potential per-country benefit of roughly 6 per cent of GDP in 2030.[3]

As an example, it has been estimated that India's digital ID system, Aadhaar, has directly led to the opening of over 150 million new bank accounts, many of which were for people previously unable to open one. Thailand's digital ID system has similarly provided a basis for the government to realise universal health coverage within three years.[4]

Regional Strategies

The ASEAN Digital Integration Framework[5] seeks to enable ASEAN member States to prioritise existing policy actions to deliver the full potential of digital integration. Priority areas for the realisation of digital integration include to facilitate seamless trade across ASEAN, to protect data while supporting digital trade and innovation and to enable seamless digital payments, including to extend financial inclusion to underserved populations across ASEAN.

In line with the ASEAN Digital Integration Framework, the signing of the ASEAN e-Commerce Agreement[6] and the reaffirming of the ASEAN Framework on Digital Data Governance[7] in 2018 is a welcome step towards achieving a "Digital ASEAN".

1 "The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth" (2019) http://documents.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf (accessed 17 December 2019).

2 "Principles On Identification For Sustainable Development: Toward The Digital Age" http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf (accessed 17 December 2019).

3 "Digital identification: A key to inclusive growth" (April 2019) https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx (accessed 17 December 2019).

4 "The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth" http://documents.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf (accessed 19 December 2019).

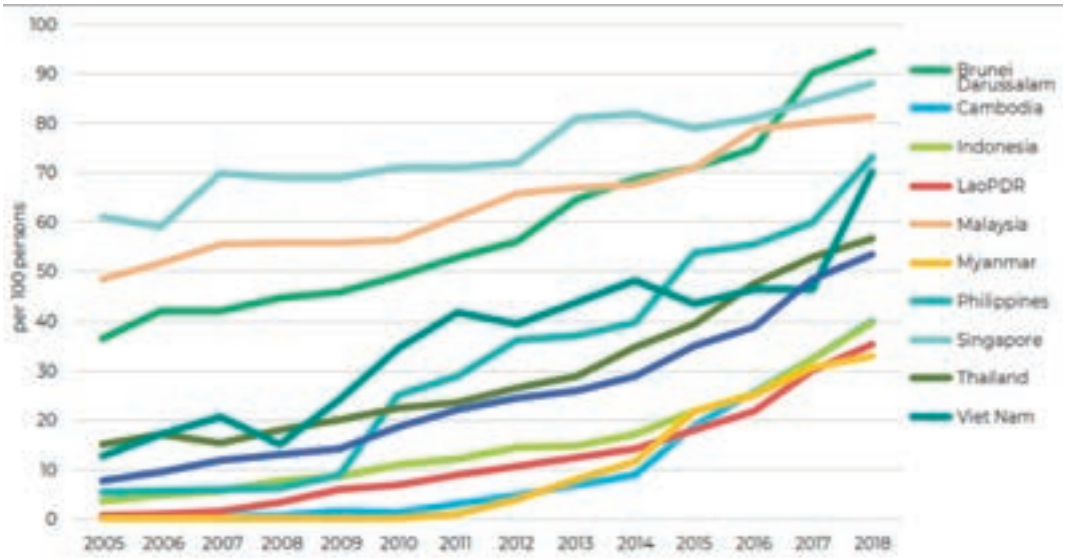
5 ASEAN Digital Integration Framework https://asean.org/storage/2019/01/ASEAN-Digital-Integration-Framework.pdf (accessed 18 December 2019).

6 ASEAN Agreement on Electronic Commerce http://agreement.asean.org/media/download/20190306035048.pdf (accessed 17 December 2019).

7 ASEAN Framework on Digital Data Governance https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf (accessed 17 December 2019).

The number of Internet subscribers in ASEAN member States has generally been increasing steadily since 2005 (see Figure 1 below).

Figure 1 Number of internet subscribers per 100 persons by ASEAN Member States, 2005 - 2018[8]



As connectivity within ASEAN grows, it is critical for governments to put in place frameworks and mechanisms to leverage these developments and increase the use of digital platforms, while ensuring that there is proper governance, trust and authentication measures to support the development of the digital economy.

National Strategies

Given the importance of digital identity in ensuring digital integration, it is worth noting that some governments from the region have been developing or have developed national strategies for the implementation of a digital identity.

In fact, five member States within ASEAN (Brunei, Indonesia, Malaysia, Singapore, and Thailand) have fully digitised their foundational identity systems, and three other member States (Cambodia, Lao and Vietnam) are in the stage of piloting their digitised foundational ID system[9].

Some of the key developments and initiatives within ASEAN on digital identity are set out below.

8 ASEAN Key Figures 2019 https://www.aseanstats.org/wp-content/uploads/2019/11/ASEAN_Key_Figures_2019.pdf (accessed 19 December 2019).

9 "The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth" http://documents.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf (accessed 19 December 2019).

Brunei Darussalam

In line with the Brunei Digital Government Strategy,[10] the government of Brunei Darussalam launched the e-Darussalam portal in July 2011 which allows users in Brunei to access online government services on-the-go upon registering at the national e-Darussalam portal, www.gov.bn.[11] The e-Darussalam portal is available to citizens, businesses, and visitors in Brunei Darussalam.[12]

Driven by the country's long-term development plan Wawasan 2035[13], the Brunei Digital Government Strategy's focus areas relate to service innovation, collaboration and integration, capability and mindset, optimisation, security, and enterprise information management of the digital government. In particular, six programmes were identified to realise the vision and to achieve the Brunei Digital Government Strategy 2015 – 2020. A key programme is the implementation of universal access for government services.[14]

This programme acknowledges identity as "a concept and mechanism that captures the uniqueness and attributes of a particular entity", and hence "having a unique and universal identity for each citizen and business makes it easier for them to access Government services".[15] The output of this programme is to achieve the following:

(a) One ID for citizens;

(b) One ID for businesses; and

(c) Services that support one ID.

Moving ahead, the Autoriti Monetari Brunei Darussalam (AMBD) has set out in the Digital Payment Roadmap for Brunei Darussalam the key strategies to achieve the Digital Payment Nation vision before 2025.[16]

10 "Digital Government Strategy: 2015 – 2020 Brunei Darussalam" https://www.gov.bn/Documents/DGS%202015%20-%202020/Brunei%20DGS%202015%20-%202020%20-%20en.pdf (accessed 19 December 2019).

11 "Brunei helps its citizens with the launched of its E-Darussalam portal" https://www.ecquaria.com/brunei-helps-its-citizens-with-the-launch-of-its-e-darussalam-portal/ (accessed 19 December 2019).

12 "e-Darussalam Portal" http://www.egnc.gov.bn/SitePages/e-darussalam.aspx (accessed 19 December 2019)

13 https://www.gov.bn/SitePages/Wawasan%20Brunei%202035.aspx

14 Digital Government Strategy: 2015 – 2020 Brunei Darussalam" https://www.gov.bn/Documents/DGS%202015%20-%202020/Brunei%20DGS%202015%20-%202020%20-%20en.pdf (accessed 19 December 2019).

15 Digital Government Strategy: 2015 – 2020 Brunei Darussalam" https://www.gov.bn/Documents/DGS%202015%20-%202020/Brunei%20DGS%202015%20-%202020%20-%20en.pdf (accessed 19 December 2019).

16 AMBD, "Digital Payment Roadmap for Brunei Darussalam 2019-2025" https://www.ambd.gov.bn/Site%20Assets%20%20Slider%20Home%20Page/DPR%202019-2025.pdf (accessed 20 December 2019).

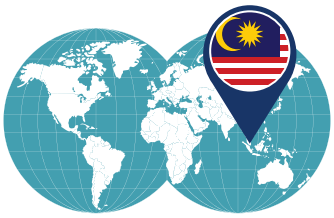
Indonesia

In Indonesia, citizens and foreigners (who have permanent residence permits) who are of at least 17 years of age, or have been married, are mandated by law to own a Kartu Tanda Penduduk Eletronik (e-KTP) or Electronic Resident Identity Card.[17]

The Director General of Population and Civil Registration Agency of the Ministry of Home Affairs, Zudan Arif Fakrulloh, announced in April 2019 that the national database for e-KTP had reached 98.22 per cent coverage nationwide.[18]

Registration for e-KTP is compulsory for activities such as voting. For example, the e-KTP or statement letter that confirmed that the identities have been recorded was a requirement to participate in the 2019 General Elections, as mandated in the Law on General Elections and the Constitutional Court's decision. For the purposes of these elections, the Indonesian Government stepped up its efforts to ensure that Indonesian citizens were able to record their identities for the e-KTP. In particular, the Population of Civil Registration Agency took measures to proactively visit certain sites such as detention centers, prisons, hospitals, nursing homes, schools, and Islamic boarding schools, to record the identities of persons. The Civil Registration Agency at regencies / cities also kept their offices open during weekends and national holidays to facilitate registration for e-KTP.[19]

Malaysia



Malaysia's identity card system, MyKad is compulsory for all citizens aged 12 and above. Since 2001, MyKad has been used as a smart card to access government online services. MyKad can be used as an identity card, public key infrastructure, a Transit card and a health document.[20]

In 2019, the Malaysian Cabinet approved the implementation of the National Digital Identity initiative. The initiative will be led by the Ministry of Communications and Multimedia,and

17 Indonesia Information Portal, How to Change the Electronic ID Card (E-KTP) Data (21 November 2019) https://indonesia.go.id/layanan/kependudukan/sosial/cara-ubah-data-ktp-elektronik-e-ktp (accessed 22 December 2019).

18 Cabinet Secretariat of the Republic of Indonesia, "Home Affairs Ministry Encourages People to Record Data for E-KTP Ahead of Election" (7 April 2019) https://setkab.go.id/en/home-affairs-ministry-encourages-people-to-record-data-for-e-ktp-ahead-of-election/ (accessed 22 December 2019).

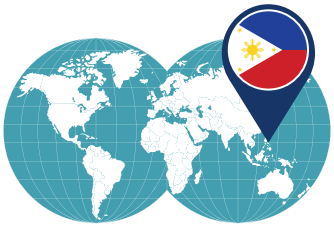
19 Cabinet Secretariat of the Republic of Indonesia, "Home Affairs Ministry Encourages People to Record Data for E-KTP Ahead of Election" (7 April 2019) https://setkab.go.id/en/home-affairs-ministry-encourages-people-to-record-data-for-e-ktp-ahead-of-election/ (accessed 22 December 2019).

20 National Registration Department, Ministry of Home Affairs, MyKad Main Applications, https://www.jpn.gov.my/en/informasimykad/main-applications/#1458812346649-140ffb9f-1f00 (accessed 20 January 2020).

carried out by the Malaysian Communications and Multimedia Commission (MCMC).[21] Called the "Digital Identity Verification Platform", the platform seeks to allow government and private service sectors to meet the needs of verifying the identities of individuals accessing electronic services, to perform transactions and to verify digital signatures provided. The objective of the National Digital Identity initiative is to enhance development of the digital economy inclusively while elevating confidence towards the Government and private online services, and to support the Government digital service efficiently.[22]

According to media reports, the MCMC has said the optional National Digital ID will not be "a substitute" for the existing National Registration Identity Card. Instead, it is intended to be an advanced method of authenticating a user's identity online, bringing benefits to citizens and businesses, by removing the need for individuals to remember different usernames and passwords for various services[23].

Philippines



by The Congress of the Philippines ratified the proposed law on creating a "national identification system" on 30 May 2018.[24] Shortly after the signing of the National ID system into law by President Rodrigo Duterte on 6 August 2018,[25] the Philippines Republic Act No. 11055 mandated the establishment of the Philippine Identification System (PhilSys) for all citizens and resident aliens of the Philippines.

The primary objectives of the Act are as follows:

"*a foundational identification system to provide a valid proof of identity for all citizens and resident aliens as a means of simplifying public and private transactions; a social and economic platform which shall serve as the link in the promotion of seamless service delivery, enhancing administrative governance, reducing corruption, strengthening financial inclusion, and promoting ease of doing business*"[26]

Recently, on 7 October 2019, it was announced that the Philippine Statistics Authority (PSA) had signed a memorandum of agreement with the Bangko Sentral ng Pilipinas (BSP) for the production of 116 million pieces of cards for IDs under the PhilSys.[27]

21 Malay Mail, "Cabinet green-lights National Digital Identity" (26 August 2019) https://www.malaymail.com/news/malaysia/2019/08/26/cabinet-green-lights-national-digital-identity/1784339 (accessed 20 December 2019).

22 MyGovernment, National Digital Identity Initiative https://www.malaysia.gov.my/portal/content/30592 (accessed 20 December 2019).

23 GSMA, News Flash: Malaysia's Pushes Ahead with Digital ID, https://www.gsma.com/identity/malaysias-pushes-ahead-with-digital-id (accessed 20 January 2020)

24 The Straits Times, "Philippine Congress ratifies national ID law" (31 May 2018) https://www.straitstimes.com/asia/se-asia/philippine-congress-ratifies-national-id-law (accessed 22 December 2019).

25 ABS CBN, "Duterte signs National ID system into law" (6 August 2018) https://news.abs-cbn.com/news/08/06/18/duterte-signs-national-id-system-into-law (accessed 22 December 2019).

26 PSA, Information on PhilSys https://psa.gov.ph/philsys (accessed 22 December 2019).

27 BSP, "BSP to Produce Cards to be Used for the Philippine ID System" (7 October 2019) http://www.bsp.gov.ph/publications/media.asp?id=5171 (accessed 22 December 2019).

Alongside the foregoing, it was also reported that the relevant authorities are in the midst of pilot-testing the national ID until about May or June 2020, with the view of rolling it out to an initial figure of 14 to 15 million people by July 2020.[28]

Singapore

The Singapore government is developing a digital infrastructure - National Digital Identity (NDI) platform - to serve as a common and universal trust framework that the public and private sectors can leverage to build value-added digital services. As an extension of the SingPass authentication system, the NDI platform allows citizens to transact with both public and private sectors through the use of one single digital identity.[29]

Currently, Singaporeans use a set of user credentials known as their "SingPass" to access various government digital services. In 2018, the Singapore government launched SingPass Mobile, a mobile application which provides a two-factor authentication method through fingerprint, facial recognition, or 6-digit passcode, for easier access to government digital services, and is aimed at reducing reliance on passwords and physical tokens for such authentication.[30]

Enhanced security features are also embedded within SingPass Mobile to protect the personal data of its users. For example, where SingPass Mobile detects that there may be a potential security breach, or if there could be malicious software present on a mobile device, the user will not be able to use SingPass Mobile on that device.[31]

The Singapore government also intends to improve on the MyInfo service. MyInfo service is a data vault service whereby SingPass users need only provide their personal data once to the Government and the MyInfo service will then automatically populate online forms that are required for certain public or private sector digital services, as necessary, enabling Singaporeans to access multiple online transactions without having to constantly resubmit their personal information.[32]

Moving ahead, the Singapore government is looking to introduce digital signature capabilities for all government services by the year 2023.[33]

---

28 Philippine News Agency, "PSA sets pilot testing of nat'l ID until May or June '20" (7 October 2019) https://www.pna.gov.ph/articles/1082498 (accessed 22 December 2019).

29 GovTech, "National Digital Identity" https://www.tech.gov.sg/scewc2019/ndi (accessed 19 December 2019).

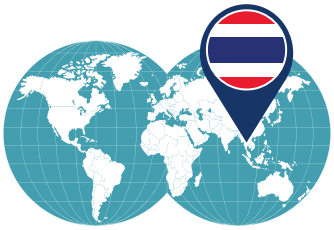
30 GovTech, "Easier and more Secure Logins with the New SingPass Mobile App" (22 Oct 2018) https://www.tech.gov.sg/media/media-releases/easier-and-more-secure-logins-with-the-new-singpass-mobile-app (accessed 19 December 2019).

31 GovTech, "Easier and more Secure Logins with the New SingPass Mobile App" (22 Oct 2018) https://www.tech.gov.sg/media/media-releases/easier-and-more-secure-logins-with-the-new-singpass-mobile-app (accessed 19 December 2019).

32 "National Digital Identity system to be cornerstone of Singapore's Smart Nation vision" https://www.channelnewsasia.com/news/singapore/national-digital-identity-system-to-be-cornerstone-of-singapore-9140090 (accessed 19 December 2019).

33 "E-Payment, digital signature option for all government services by 2023" https://www.channelnewsasia.com/news/singapore/e-payment-digital-signature-options-for-all-government-services-10368616 (accessed 19 December 2019).

Thailand



During an interview in 2018, the Minister of Digital Economy and Society revealed that, in line with the Thailand 4.0 vision, he planned to introduce a new digital identity system in Thailand, with the vision of creating a "cashless environment" using such digital identity.[34] Thailand 4.0 is the Thailand government's 20-year strategy to accelerate Thailand's development into a more advanced level. Designed to "promote and support innovation, creativity, research and development, higher technologies and green technologies, Thailand 4.0 seeks to enable green living with smart, environmentally friendly cities and towns".[35]

On 19 February 2018, the Electronic Transactions Development Agency (ETDA) signed a Memorandum of Understanding (MoU) to establish a cooperative partnership with Omise, which is an entity that that has experience in online identification and e-payment service, for the initiating of the National Digital ID project.[36]

Since then, the National Legislative Assembly of Thailand had passed certain key bills relating to data protection,[37] cybersecurity,[38] electronic transactions, digital economy, and digital ID.[39]

Accordingly, the National Digital ID Company Limited (NDID) has recently signed a cooperation agreement titled "We are ready for Thailand Digital ID" with key partners, aiming to develop Thailand's digital ID with the ETDA.[40]

34 GovInsider, "Exclusive Interview: Minister of Digital Economy, Thailand" (20 June 2018) https://govinsider.asia/digital-gov/exclusive-interview-minister-digital-economy-thailand/ (accessed 20 December 2019).

35 National strategy Thailand 4.0 official launched https://thaiembdc.org/2018/10/22/national-strategy-thailand-4-0-officially-launched/ (accessed 20 December 2019).

36 ETDA, "ETDA Signed MoU with Omise to Boost the New Government Initiative: National Digital ID Project" (19 February 2019) https://www.etda.or.th/content/etda-signs-mou-with-omise-for-driving-national-digital-id.html (accessed 20 December 2019).

37 Bangkok Post, "The reach and liabilities of the Personal Data Protection Act" (3 September 2019) https://www.bangkokpost.com/business/1741919/the-reach-and-liabilities-of-the-personal-data-protection-act (accessed 20 December 2019).

38 Bangkok Post, "Cybersecurity Bill passed" (29 February 2019) https://www.bangkokpost.com/thailand/general/1636694/cybersecurity-bill-passed (accessed 20 December 2019).

39 OpenGov, "Six digital bills passed in Thailand by NLA" (12 February 2019) https://www.opengovasia.com/six-digital-bills-passed-in-thailand-by-nla/ (accessed 20 December 2019).

40 OpenGov, "Thailand is ready for digital ID" (23 November 2019) https://www.opengovasia.com/thailand-is-ready-for-digital-id/ (accessed 20 December 2019).

Vietnam

Currently, Vietnam has several identity databases with a large coverage, such as the database of health insurance participants, taxpayers database, subscriber database of network operators etc. However, Vietnam still does not have any official identity providers (IDP). To facilitate IDP, the managing units of these databases in Vietnam need to build and integrate the 'Identity Gateway' to be able to connect to the entire digital ecosystem. [41]

Recognizing the important role of ICT in socio-economic development, the government of Vietnam is developing a Decree to regulate digital identity . Moreover, Vietnam is considering the establishment of the National Digital Identity based on the 'Vietnam Trusted Digital Identity Framework'.[42] The Ministry of Information and Communication was assigned to preside over the construction of a 'Shared digital identity infrastructure', including the National Digital Identity Exchange, the Digital Identity Portal, and the Government API.

41 http://aita.gov.vn/tham-luan-ve-dinh-danh-va-xac-thuc-dien-tu---hoi-nghi-%E2%80%9Cso-ket-6-thang-dau-nam-2019-cua-bo-thong-tin-va-truyen-thong%E2%80%9D--572019-

42 http://aita.gov.vn/Data/Images/Articlefiles/Tham%20luan%20ve%20Danh%20tinh%20so-HuuLQ%2022_3_2019(1).pdf

Chapter 3

Digital Identity for Trade and Development Case Studies

The case studies are key components of the TFT methodology. After the completion of the 5 weeks eLearning Component on DITD, 26 participants (out of 98) were selected to attend the Face-to-Face Workshop in Singapore and presented a case study related to Digital Identity for Trade and Development of their respective countries.

Thanks to the e eLearning Component participants were able to prepare case studies and generate a well-informed roadmap for action for a compelling policy agenda. The sharing of case studies effectively stimulated fruitful exchanges of good practices among entire group and helped identify policy options and recommendations to build an effective NDIF.

Two options were provided to the participants to prepare their case studies: to use a personal experience based on his or her work; or to select a topic which inspired the participant during the online training. The eLearning Component covered five modules: 1) Fundamental concepts of Digital Identity, 2) Data Protection, 3) ID Usage, 4) Governance and 5) ID Technology Solutions & Risks.

Participants were advised to follow the structure below, that explains key elements:

- **Presentation of the subject selected**
- **Why did you choose this topic? Why does this matter to you?**
- **What is the current situation and evolution?**
- **What are the main issues that you are facing?**
- **What support do you need?**
- **Conclusion and Perspective / Recommendations.**

The case studies in this chapter are based on original submissions and interviews of the seven selected participants who attended the DITD workshop in Singapore.

Case study 1

Legal Frameworks on Personal Data Protection and Privacy in Cambodia

"The emergence of e-Commerce has brought about many benefits to our economy and individuals; however, it is important to develop legal frameworks and solid regulations for data protection and privacy in Cambodia"

***Mr Keo Buntheng**, Deputy Chief of Commercial Law Bureau, Ministry of Commerce the Kingdom of Cambodia*

Why this topic?

Digital marketplaces could drive economic growth across Cambodia, with e-commerce likely to grow to US$537m by 2024.[43] Yet, there are challenges to Cambodia's digital economy growth. Entrepreneurs battle low consumer trust and face legal and cultural barriers to cross border e-payments, and regulations have not kept pace with the online market developments.

Policies shape the business environment, affecting everything from consumers protection to e-commerce transactions, and how data is treated, collected, processed, stored and governed. They can boost the digital economy by reducing business uncertainty and compliance costs.

Current situation and evolution

Although some e-commerce policies and strategies are in place,[44] Cambodia falls behind on providing key regulations on data protection and data privacy. At present, the legal framework is rooted in four sources of law:

1. The **Constitution of Cambodia**; article 40 (c) provides some basic guarantee for privacy and data protection.
2. Although the **e-Commerce Law** has been approved in October 2019, it is not yet in force - the law (articles 32, 33, and 60) safeguards consumers' personal data and imposes sanctions and fines for failure to comply with data protection obligations.
3. The **Law on Telecommunication** also provides legal grounds on data protection under the article 65 (b).
4. Other relevant laws such as the **Civil Code**, **Labour Law** and **Law on Press** provide safeguards and obligations to banks, financial institutions, the media, medical professionals, Cambodian citizens and residents in terms of breaching confidentiality, disciplinary punishments and penalties.

Policy recommendations

- Develop solid legal instruments with regards to cybersecurity and personal data protection
- Enhance collaboration between ministries to deal with e-commerce laws

[43] Statista, e-Commerce, Cambodia, [Online]. Available at: https://www.statista.com/outlook/243/185/ecommerce/cambodia(Accessed: 3 November 2019)

[44] UNCTAD. (2017), 'Cambodia: Rapid eTrade Readiness Assessment' [Online]. Available at: https://unctad.org/en/PublicationsLibrary/dtlstict2017d2_en.pdf (Accessed: 3 November 2019)

Case Study 2

The Right to be Forgotten in Indonesia

"We need to understand the concept of the right to be forgotten as part of personal data protection and human rights regime in general, and related to the digital economy in particular"

***Mrs Nanci Laura Sitinjak**, Ministry of Communications and Informatics of Indonesia*

Why this topic?

Personal data protection is paramount to increase consumers' trust in digital trade. ASEAN countries and Indonesia in particular, are encouraging the acceleration of regulations relating to data protection and its implementation to provide safeguards and guarantees to digital trade users.

Data protection in electronic systems includes the protection of the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, erasure of personal data and the right to be forgotten.[45]

In Indonesia, the right to be forgotten has begun to be implemented from 2016. Yet a key question remains as to whether the right to erase "irrelevant" information is the same as the right to be forgotten.

Current situation and evolution

The Indonesian Law on Electronic Information and Transactions provides some elements on privacy protection, and the concept of the right to be forgotten takes form in two ways: the right to erasure, carried out based on the request of the owner of the relevant personal data; and the right to delisting, carried out based on a court decision.[46]

Indonesia has yet to introduce personal data protection beyond a draft of such laws as there are gaps that must be taken into account at the time of its implementation: (i) the need to have a deletion mechanism in place to deal with the request; (ii) to identify who will be considered a "relevant person"; (iii) to define how or in which circumstances electronic information or documents will be deemed as "irrelevant"; and (iv) to have a balance between the right to be forgotten and the right of free press.

The latest is because the fulfilment of an individual's right to be forgotten may result in regulators asking publications or websites to delete certain information, or they may ask search engine operators to prevent the information from being found through online searches. This could be seen as an impediment to free speech.

Policy recommendations

- A greater understanding of the concept of the right to be forgotten and its constitutional footings in Indonesia
- The establishment of a legal/constitutional mechanism implementing the right to be forgotten
- To develop a balance between the right to be forgotten and the right of freedom of expression

[45] The 'right to be forgotten' is a legal concept that is fast evolving in the European Union under the field of cyberlaw. It was first introduced from the desire to restore individual's function of control of personal information circulated on the internet.

[46] Article 26 paragraph (3) and (4) of the Law Number 19 of 2016, and the Revision to Law Number 11 of 2008, Electronic Information and Transactions Law

Case Study 3

Adoption of Digital Identity to Boost Economic Growth in Malaysia

"The development of a harmonised, inclusive and trusted digital identity framework will allow Malaysians to take advantage of the opportunities that the digital economy offers"

***Ms Wan Aimi Wahida Mohd Azmi**, Business Strategist di Pos Digicert Sdn Bhd*

Why this topic?

A harmonised Digital Identity framework in Malaysia could drive economic growth. The booming of the digital economy draws the immediate need for an authorised or legitimised Digital Identity platform for both individuals and businesses in Malaysia, propelling more secure, more transparent and safer online transactions.

Current situation and evolution

Malaysia has an identity card system that dates back to 1949 under the British colonial rule. The current identity document known as MyKad is compulsory for all citizens aged 12 and above. The current format of MyKad introduced in 1990 has a 12-digits numbering system rooted in citizen's characteristics such as birthdate, place of birth and gender.[47]

Figure 2 Malaysia ID card

MyKad is a physical identity card designed to enable face-to-face transactions among entities, and since 2001, has been used as a smart card to access the government's online services. The national ID system has security features including a secure chip platform, symmetric-key cryptography, and multi-layered operating systems with firewalls. Also, it incorporates two types of biometric technology for identification purposes, a colour photograph of the cardholder and a digital certificate.[48]

47 Ministry of Home Affairs of Malaysia, National Registration Department, Introduction to MyKad, [Online]. Available at: https://www.jpn.gov.my/en/informasimykad/introduction-to-mykad (Accessed: 15 December 2019)

48 Ibid.

The national postal services, Pos Digicert, has about 11 million validated and verified e-IDs users under MyKad's number. Yet, the challenge is to provide all citizens with an e-ID with non-discriminatory attributes. Other gaps and challenges include the risk of fraud, data leakage, cyber-attacks as well as the low adoption of e-government applications.[49]

E-ID can enable trust in e-commerce; a trusted Digital Identity system is needed, one grounded in biometric data protected by a digital certificate – that is trusted by all as a catalyst to achieving an inclusive digital economy. E-ID promises to enable economic value creation that increases efficiency, reduces growth barriers, generates new revenues and promotes financial inclusion.

Policy Recommendations

- Creation of a digital identity with enhanced biometric data which is protected by a digital certificate as a catalyst for achieving a total digital economy
- ID numbers should be based on random numbers with non-discriminatory attributes
- For countries to have exposure to UN activities (including site visits to successful countries and companies to be selected as pilot users)
- For countries to have continued access to knowledge (UN research and case studies, new standards, policies, or regulations from other countries relating to Digital Identity and eKYC)
- For countries to obtain technical assistance and mentorship services on the development of the digital identity solution
- For countries to obtain funding support from international organisations such as the UN to support the development of a digital identity system

[49] MyCert. (2018), Statistics, [Online]. Available at: https://www.mycert.org.my/portal/publications?id=7f17bda3-7d91-42e2-93fd-39476d75d35f (Accessed:15 December 2019)

Case Study 4

Emerging e-Commerce Trends and the need to adjust Government Policies in Myanmar

"We need to have a sound legal background on data protection and privacy to keep up with the emerging e-commerce trends to enjoy the benefits that the digital economy provides"

***Ms Su Thet Hninn**, Assistant Director, Ministry of Commerce in Myanmar*

Why this topic?

Myanmar is one of the fastest growing economies in the region after opening up the market and returning to engaging with the international community. Based on the findings of the Rapid eTrade_**Readiness Assessment for Myanmar** by UNCTAD (hereafter referred to as "eT Ready report"), the country has unprecedented opportunities to go for the digital economy preceded by the liberalisation of the telecommunication sector in 2014.[50]

Yet, substantial obstacles are in place for entrepreneurs and start-ups. The eT Ready points to insufficient data protection and data privacy as barriers to the country's readiness for e-commerce. The existing regulatory framework can be improved by enabling the World Bank's approach to managing and minimising potential privacy risk by combining ID Enabling Environment Assessment ("IDEEA") and Privacy by Design (PbD).[51]

Current situation and evolution

After the liberalisation of the telecommunication market in 2014, smartphone penetration reached 80 per cent, creating opportunities for entrepreneurs to explore online marketplaces, increasing online transactions and consumers.[52] Yet, the performance of most online stores shows several weaknesses: having poor return policies, lack of customer warranties and proper consumer protection.

Although some policies and strategies to support the digital economy are in place, including the establishment of Data ID Card System,[53] Myanmar falls behind on providing regulations on data protection and privacy. The system is still limited as it is fragmented; there is limited interconnectedness for data sharing. Cyber laws are partially implemented with not all measures being in place. Data protection and privacy laws are either ill-drafted, too broad, or incomplete.

Support is needed to improve the legal framework for a digital economy, as well as e-commerce laws based on UNCITRAL texts. Ensuring the privacy and security of the personal data of citizens and residents should be one of the government's priorities to build an effective National Digital Identity System.

50 UNCTAD, (2018), Myanmar: Rapid eTrade Readiness Assessment, [Online]. Available at: https://unctad.org/en/PublicationsLibrary/dtlstict2018d1_en.pdf (Accessed: 15 December 2019)

51 World Bank, (2019), Identification for development, Practitioner's Guide, [Online]. Available at: http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf (Accessed: Accessed: 15 December 2019)

52 UNCTAD, (2018), *Myanmar: Rapid eTrade Readiness Assessment*, p.1

53 Myanmar e-Government Master Plan (2016-2020)

Policy recommendations

- As several governmental agencies have their own ID systems, work will need to be put in to assess each of the systems, as well as the nation's present legal and administrative framework to pinpoint specific areas of improvement (such as for data protection, non-discrimination, etc.)
- Users should be educated of their rights vis-à-vis their own data
- There should be a legislation to promote regional integration and the acceleration of legal and regulatory reforms to keep up with regional trade agreements
- The Myanmar government is now developing a cybersecurity framework with the support of the World Bank. Myanmar, as a starter of national digital identification system, should consider the example of Singapore's Cybersecurity Act 2018 on implementing a standalone cybersecurity legislation covering the essential services

Case Study 5

Philippines' National Public Key Infrastructure

"It is a breakthrough for the Philippines to take the first step and develop a PKI system. It is never too late for the Philippine government to re-evaluate its policies and implementation strategies to optimize the system fully."

***Mr Jose Siraj Ballesteros Murad**, Trade Facilitation Consultant, Department of Finance, Republic of the Philippines*

Why this topic?

As more and more people rely on the use of online applications over unsecured networks like the Internet, the need to secure files and ensure their information confidentiality and integrity increases, as does the need for a dependable Public Key Infrastructure (PKI). As its name implies, PKI is an infrastructure that secures communications between individuals and government agencies and ensures that the government's delivery of services to citizens and businesses becomes safer, faster and more efficient.[54]

The successful implementation of an information system requires the development of a holistic governance model,[55] as any system must be fundamentally rooted in both legal and operational base of accountability and trust amongst its various stakeholders.[56]

The Philippine National Public Key Infrastructure (PNPKI) was established subsequent to the launch of the country's iGovPhil program, wherein providing data security through the PKI is an essential component of the program. Since the launch of the system in 2014, the Department of Information and Communications Technology (DICT) has reported that 4000 registered individuals have been issued Digital Certificates, an electronic imprint that possesses weight as their non-digital ID that would allow users to prove their identity virtually.[57]

Current situation and evolution

The PNPKI system is a production-ready, shared service system funded, owned, managed, and administered by the Philippine government through DICT. It provides government agencies with trusted authentication facility for web applications, virtual private networks, wireless networks, in addition to the ability to digitally sign and encrypt documents and electronic mail messages through the use of digital certificates or digital tokens.[58]

Among the certificates that the PNPKI issues to private individuals as well as government agencies, there are the following: Authentication certificate, used in applications that require

54 Department of Information and Technology. (n.d.). FAQs – PNPKI. [Online]. Available at: https://dict.gov.ph/frequently-asked-questions-pnpki%EF%BB%BF/ (Accessed: 10 October 2019)

55 UNCTAD, Types of Governance Models, Digital Identity for Trade and Development, p. 9.

56 World Bank Group, Governance, Principles on Identification for Sustainable Development: Toward the Digital Age, pp. 16-17. [Online]. Available at: http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED- English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf (Accessed: 10 October 2019)

57 Andrade, J. (2014, August 14)., DoST launches Internet infra to protect netizens from cybercrime, Philippine Daily Inquirer, [Online]. Available at: https://technology.inquirer.net/38111/dost-launches-internet-infra-to-protect- netizens-from-cybercrime#ixzz62hvsuUrD (Accessed: 11 October 2019)

58 Department of Information and Communications Technology, Philippine Digital Transformation Strategy 2022, p. 10.

the user to login and can be used to encrypt email; Signing certificate, used to digitally sign documents; SSL certificate, a certificate for machines, e.g., web servers, application servers, routers, Wi-Fi devices, and others.

The governance model that the Philippine DICT adopted is that of the government being directly involved by acting as both Identity Provider and Regulator. In the Philippine context, the roles of the following are all played by DICT: Root Certification Authority (Root CA); Certification Authority (CA), which issues digitally-signed public key certificates and attests that the public key embedded in the certificate belongs to the particular subscriber as stated in the certificate; and Registration Authority (RA), the authority designated by the CA to perform administrative tasks such as end-user registration by registering and verifying the information provided by the person requesting the certificate.

The model that the Philippines adopted has seen effective use in numerous governments, leveraging on its local presence and current infrastructure.[59] India and Estonia, in particular, were able to use the model to their advantage and come upon exemplary results. The same however, could not be said of the Philippines.

The sole PNPKI RA accredited by DICT is itself. This logistical issue is further hampered by DICT's lack of mandate to issue a valid identification. DICT depends on other identification documents issued by other government agencies mandated to provide identification for a specific purpose; e.g. the Department of Foreign Affairs and the passport as a travel document.

PNPKI enrolment and verification is a challenge due to numerous identification requirements one must have in order to avail of its services, a scenario faced by the Filipino citizen at any government office with the ability to provide and authenticate identification. For context, the Philippines lacks a centrally generated national system for the unique identification of a person. Also, there are 16.3 million Filipinos who do not have any proof of identity.[60]

This conundrum is a known fact and DICT made prior plans to have other government agencies take the role of RAs, such as the implementers of the Unified Multi-Purpose ID (UMID). However, a suggestion made towards that has been ignored to date, despite assurances of the placement of technical, organizational, and legal security measures.

There is also the tedious process of government agencies wanting to become an RA with all costs involved in the course of the assessment being the responsibility of the RA applicant,[61] i.e. additional paperwork and sourcing of funds. This is a risk for an interested agency to reconsider participating.

The PNPKI system also has an insignificant number of registrants from government itself regardless of the direction with Executive Order (E.O.) No. 810, series 2009, which institutionalized the certification scheme for digital signatures and directed the application of digital signatures in e-Government Services. Perhaps, it is the very nature of the PNPKI's legal key stone that impedes the proliferation of its registrants, as an executive order is not a comprehensive law covering all parts of the state; it lacks the power to compel.

---

59 United Nations Conference on Trade and Development, Types of Governance Models, *Digital Identity for Trade And Development*, p. 9.

60 Porcalla, D. (2019, October 11). Nat'l ID system to benefit farmers, fisherfolk. *The Philippine Star*, p. 4.

61 Department of Information and Communications Technology, Memorandum Circular No. 2014-001.

The low utilization rate, as DICT learned during focus group discussions conducted in the initial data gathering stages of developing the digital transformation strategy, can also be attributable to the following conditions:[62] a) lack of awareness (agencies were not made fully aware of the existing services, do not fully understand how these services will benefit their organization, or do not know how to move forward with the information they received about the services); b) lack of training and capacity development programs, and/or the lack of funding on the part of the agency to sustain the use of available services; c) high attrition rates of qualified technical personnel; d) lack of confidence that the government could handle production support requirements and sustain service level commitments required by public-facing systems and services; and e) the implicit notion that maintaining the status quo is the safest posture as there are no explicit incentives for innovation.

Nevertheless, there are policies that support PNPKI, such as Republic Act No. 8792, otherwise known as the Electronic Commerce Act. Its Implementing Rules and Regulations specifically confirm that contracts cannot be denied enforceability merely because they are concluded electronically, and the Supreme Court's Rules on Electronic Evidence (A.M. No. 01-7-01-SC) recognize the use of digital signatures as evidence. This is being practiced with the Securities and Exchange Commission (SEC) on the online submissions of RBCA reports, and the Government Procurement Policy Board (GPPB) approval for the use of digital signature in all procurement-related documents.

Policy Recommendations

- Streamline the Philippine National Public Key Infrastructure (PNPKI)
- Create an online registration system
- Make revisions to section 4 of the Executive Order No. 810, series 2009 in relation to enhanced promotion and enforcement
- Study demographics to determine which regulatory authorities would be best suited to partner with PNPKI in order to achieve the highest coverage
- Review of Executive Order No. 810, series 2009, and possibly make amendments to newly enacted laws such as Republic Act No. 11055 (which establishes the Philippine Identification System)

62 Department of Information and Communications Technology, *Philippine Digital Transformation Strategy 2022*, p. 13.

Case Study 6

Philippine Identification System (PhilSys) and Blockchain

"A blockchain-based solution for the Philippine Identification System would meet the wider aspirations of seamless service delivery, greater administrative governance, ease of doing business and reducing corruption."

***Mr Arnold Janssen D. Saragena**, Trade and Industry Development Specialist, the Philippines Department of Trade and Industry*

Why this topic?

ID plays a critical role for individuals to interact with the government and private organizations. Every individual needs to answer the question "*who are you*"; whether we are in a coffee shop to buy our favourite cup, in a bank to open an account or in a hospital to get health care services, and it requires proper proof of identification. Identity is defined as "a set of attributes that uniquely describes an individual or entity"[63] and Identification (ID) is the evidence or attestation of one's identity.

In the Philippines, proving one's identity usually requires presentation of at least two valid/government-issued IDs. These IDs are typically non-electronic cards; a credential technology (CT) that is affordable, easy to deploy and use. However, using non-electronic cards has disadvantages such as card loss, tampering, and lack of biometric authentication support which is a more reliable form of identification. Amongst government and private agencies, there is confusion on which ID is considered primary, secondary or even "valid."[64]

In recent years, other kinds of CT were made available to the Philippines such as RFID cards, biometrics, contact and contactless smart cards, among others. Despite having these technologies, individuals and resident aliens still need to present two valid proofs of identification due to the absence of a unified national identification system.

The current identification system is fragmented between different public service agencies and institutions. It is also hindered by its susceptibility to disruptions and hacking attempts. Implementing blockchain-based solutions can simplify public and private transactions and provide a **"national identity"** to each citizen and resident alien of the Philippines. The decentralised nature of a blockchain-based solution would alleviate vulnerabilities whilst reducing the risk of inoperability. This would meet the wider aspirations of seamless service delivery, greater administrative governance, ease of doing business and reducing corruption.

Current situation and evolution

The "Philippine Identification System" or PhilSys aims to provide identity for all citizens and resident aliens to simplify public and private transactions; promote seamless service delivery; enhance administrative governance; reduce corruption; strengthen financial inclusion; and promote ease of doing business.[65]

---

63 UNCTAD, (2019) Digital Identity for Trade and Development and Development, *Module 1: Fundamental Concepts of Digital Identity*.

64 Primary IDs: Philippine passport, Driver's license, SSS UMID card, Philhealth ID, TIN Card, Postal ID, Voter's ID, PRC ID, Senior Citizen ID, and OFW ID. Secondary IDs: NBI Clearance, Police Clearance, Barangay Clearance, PSA Marriage Contract/Certificate, NSO Birth Certificate, GSIS ID, IBP ID, OWWA ID, Diplomat ID and GOCC and Government Office ID. Source: https://www.moneymax.ph/government-services/articles/valid-ids-philippines/

65 https://psa.gov.ph/philsys

The Philippine Statistics Authority (PSA), in collaboration with the Department of Information and Communications Technology (DICT) - the agency responsible for the overall planning, management, and administration of the PhilSys - will collect the relevant information for the PhilSys as follows:

Figure 3: PhilSys in the Philippines

Demographic Data	Biometric Information
1. Full Name	1. Front Facing Photograph
2. Sex	2. Full Set of Fingerprints
3. Date of Birth	3. Iris Scan
4. Place of Birth	
5. Blood Type	
6. Address	
7. Filipino or Resident Alien	
8. Marital Status (optional)	
9. Mobile number (optional)	
10. Email Address (optional)	

A citizen or resident alien will be issued with a Phil ID[66] with a corresponding PhilSys Number (PSN)[67] which can be used to access the following services:

Figure 4: Uses of Phil ID and PSN

Uses of Phil ID and PSN	
1. Social welfare and benefits granted by the government	5. Opening of bank accounts
2. Passports and driver's license	6. Registration and voting purposes
3. Tax-related transactions	7. Transactions for employment purposes
4. Admission in schools/government hospitals	8. Cardholder's criminal records and clearances

To avail of a Phil ID and PSN, a citizen or resident alien may register at the following centres:

Figure 5: Phil ID Registration Centres

Registration Centres	
1. PSA Regional and Provincial Offices	6. Home Development Mutual Fund (HMDF)
2. Local Civil Registry Offices (LCROs)	7. Commission on Elections (COMELEC)
3. Government Service Insurance System (GSIS)	8. Philippine Postal Corporation (PHLPost)
4. Social Security System (SSS)	9. Other government agencies and Government-owned and Controlled Corporations (GOCCs)
5. Philippine Health Insurance Corporation (Philhealth)	

The collected information will be stored and maintained at the PhilSys Registry. A pilot testing of the PhilSys started in September 2019 and will run until June 2020. The PhilSys is expected to be released and opened to the public in July 2020.

66 A Phil ID is a nontransferable card preferably be issued to all citizens or resident aliens registered under the PhilSys. Source: https://psa.gov.ph/philsys

67 A PhilSys Number is a randomly generated, unique, and permanent identification number that will be assigned to every citizen or resident alien upon birth or registration by the PSA, Source: https://psa.gov.ph/philsys

Blockchain vis-à-vis PhilSys

The PhilSys is anchored on PSA's data centres. Data centers are "traditional" data management solutions, being highly available and offering first-hand interaction with the data source. Yet, there are several disadvantages:

- Needs a dedicated space with the right environmental conditions (i.e., void of humidity, elevation, stable power supply and cooling mechanism)
- Prone to natural and man-made destruction (i.e., flood, earthquake, bomb explosion, and fire)
- Susceptible to hacking; needs multiple layers of safety protocols
- Will be obsolete in a few years upon installation
- Subject to regular utility maintenance services; possibly resulting in downtime

As data management solutions continue to evolve, innovative technologies (i.e., cloud computing, and blockchain) have been used as a data repository. Blockchain or distributed ledger technology is a decentralized registry that is hosted across peer-to-peer (P2P) infrastructure wherein computer systems are connected to each other online. Data can be shared between systems without the need of a principal server which makes computer systems both a server and a client. The only requirement of blockchain technology is an Internet connection and P2P software. Member computers are allowed to search for data on other participating networks but only within a designated location while satisfying a security protocol.[68]

Hacking blockchains require 51 per cent proof of work in order for a transaction to be deemed as "valid"; similar to convincing 6 out of 10 people that what you are proposing (in this case change introduced by hackers) is true. Modern blockchains continue to evolve to further enhance security (i.e., adding layers of access, isolation of transactions, among others), removing vulnerabilities like any other technical solution.[69]

Policy Recommendations

To consider the possibility of relying on blockchain to facilitate PhilSys (or other digital ID systems), due to the advantages it may bring, including:

- Reduce / eradicate the need for dedicated spaces as data centres are not vital in blockchain systems
- Reduce the risk of inoperability due to natural or manmade destructions
- Reduce the risk of hacking (as significant effort and skill is needed to overturn a command in a blockchain system)
- Minimize the risks of obsolescence as the framework is software-based and Internet reliant, hence allowing updates to software
- Eliminate the need for a utility service maintenance as the framework is not based on hardware
- Enable users the control over their profile by authenticating changes via biometrics or private key

[68] techterms.com/definition/p2p

[69] https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Case Study 7

PhilSys Through the Looking Glass: Governance Policies and Measures

"Philippine national ID is also a ticket for the people to be part, to be included in the economic mainstream of the country."

***Ms Jovita J. Vence**, Assistant Division Chief, Bureau of Trade and Industrial Policy Research, the Philippines Department of Trade and Industry*

Why this topic?

The Philippines' ID System (PhilSys) is administered by the Philippines Statistics Authority (PSA) with the aim of promoting seamless service delivery. PhilSys has been rolled out in phases, with priority use given to the Department of Social Welfare and Development. The 5-year program will culminate in 2022 with the mass registration of 105 million Filipinos. Yet, challenges remain such as a lack of accountability, the lack of public trust and a lack of budgetary support.

Current situation and evolution70

Phase 1 (Jan-Dec 2019)

The PhilSys implementation is currently in Phase 1 (Jan-Dec 2019): procurement, testing of core technology infrastructure, organizational development of the PhilSys Registry Office (PRO), and launch of target registration. Key accomplishments targeted include:

- Pilot-Test Registration (2 Sept-June 2020) – biometric and demographic capturing processes (involving roughly 6 million) from the National Capital Region
- Procurement of registration kits
- Biometric tech system final testing
- Biometric ID Card production – PSA-Bangko Sentral ng Pilipinas (BSP) partnership

Phase 2 (Jan-Jun 2020)

- Development and full operationalization of core technology infrastructure, development of a mass registration ecosystem, use case development, and registration of pre-registered persons
- Testing of the end-to-end system (deduplication, generation of unique PhilSys Numbers (PSN), and card printing and issuance)

Phase 3 (Jul 2020-Jun 2022)

- Mass registration of 105 million Filipinos and resident aliens, including overseas Filipino workers (OFWs); and

Phase 4 (Jul-Dec 2022): Issuance of PhilSys Numbers (PSNs) to newborns.

This case study shall view the governance policies and measures relative to Philsys vis-à-vis the three key aspects of the governance of e-ID systems which are based on World Bank's Identification for Development (ID4D) Principles on Identification for Sustainable Development:[71]

70 See http://www.neda.gov.ph/govt-on-track-with-national-id-implementation/ for facts included in this section

71 World Bank, (2019), *Identification for development, Practitioner's Guide*

1. *Ensuring data privacy and security and safeguarding users' rights by setting up a comprehensive and robust legal and regulatory framework*

The DITD Module 2 Manual Introduction underscores two choices for governments to ensure the privacy and security of the personal data of citizens and residents of the country stored in the country's digital ID system: (1) There is a data protection law of general application in place and determine if the NDIS fits under it; or (2) The NDIS has its own set of data protection principles. In case of the PhilSys, the legal and regulatory framework governing it are:

- Republic Act (RA) 11055 or the Philippine Identification System (PhilSys) Act and its Implementing Rules and Regulations (IRR) 2018
- Assures that PhilSys registry is protected from unauthorized access, use, disclosure and against accidental or intentional loss, destruction or damage;
- Mandates that all individuals shall be informed adequately upon registration for PhilSys on how their data will be used;
- Provides penalty for unlawful use of the ID, as well as acts such as willful submission of or causing to be submitted of a fictitious name or false information in application or renewal; and
- Follows Privacy-by-Design features ensuring that PSN-holders have full control over the access and use of their personal data.
- RA 10173, also known as the Data Privacy Act of 2012, and its IRR
- Strict controls over what circumstances the data in the PhilSys registry can be accessed and shared
- RA 10175 – Cybercrime Prevention Act 2012, and its IRR
- Lists, among others, as a punishable act with penalties: 1) Offenses against the confidentiality, integrity and availability of computer data and systems: Illegal access, illegal interception, data interference, system interference, misuse of devices, and cyber-squatting; and 2) Computer-related offenses: Computer-related forgery, computer-related fraud, and computer-related identity theft.

2. *Setting out clear institutional mandates and establishing accountability*

Philippine government agencies that are mandated to carry out and support the implementation of PhilSys include the following with their respective scope of accountability:

- Philippine Statistics Authority (PSA) - an attached agency of the National Economic Development Authority (NEDA), leads PhilSys' implementation (overall planning, management, maintenance and administration) under the guidance of the PhilSys Policy and Coordination Council (PSPCC), an inter-agency body composed of NEDA (as Chair), PSA (as Co-Chair), Department of Budget and Management (DBM) (as ViceChair) and 11 other member agencies (DFA, DICT, DOF, DSWD, DILG, NPC, BSP, GSIS, PhilHealth, SSS, and PHLPost);[72]
- Department of Information and Communications Technology (DICT) - the primary government entity mandated to plan, develop, and promote the national ICT development agenda (RA 10844) and tasked, among others with cybersecurity policy and program coordination; and

[72] https://psa.gov.ph/philsys

- National Privacy Commission (NPC) - a regulatory and quasi-judicial body (RA 10173, 2016) and data privacy and data protection watchdog with the mandate to administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection.73

3. *Leveraging on independent oversight and proper adjudication of grievances to bolster legal and trust frameworks*

For its part, NPC had put in place specific measures, access mechanisms and multi-stakeholder initiatives to bolster legal and trust frameworks which PhilSys could readily utilize to its advantage, viz:

- NPC Circular 16-03 – Personal Data Breach Management: Provides the management of personal data breach to include prevention, incident response, mitigation and compliance when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud
- NPC Circular 16-04 – Rules of Procedure: Provides for the application of the rules to all complaints filed before the NPC or such other grievances, requests for assistance or advisory opinions, and other matters cognizable by the agency for violations of the Data Privacy Act by any person who is the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of the Data Privacy Act.
- Access and Correction: Citizens have the right to ask for a copy of any personal information the NPC holds about them, as well as to ask for it to be corrected if they think it is wrong through e-mail: info@privacy.gov.ph.
- Multi-stakeholder coalition to protect the “digital Filipino”: An NPC-initiated covenant of unity for the protection of the digital Filipino to strengthen the protection of peoples’ personal data formed in May 2019; composed of more than 2,000 Data Protection Officers (DPO) from major government offices and leading businesses, executives from DICT, DTI, DoJ, PNP and Laban Konsyumer, an advocacy group.
- PhilSys Act provides penalties for employees or officials responsible for keeping the PhilSys registry of 3-6 years imprisonment and a P1-3M fine for negligence resulting in the registry being accessed by unauthorized people.

The case study adopts the following ways forward with regard to PhilSys:

- Address capacity issues in the implementation of the PhilSys programs and projects: full operationalization of specific PSA offices with competent technical personnel and sufficient capital outlay for technology and digital skills acquisition; development and implementation of a long-term strategic plan to finalize risk management strategies, data privacy management, and technological interfacing;
- Strengthen PhilSys partners to manage reforms requiring their assistance; and
- Annual budgetary support through the General Appropriations Act (GAA) to cover implementation and maintenance costs (approx. Php 25-30B or US$462-563M over five years).

73 https://www.privacy.gov.ph/

Policy Recommendations

- Ensure the integrity of key/lead institutions implementing the PhilSys as critical in building public trust on PhilSys
- Enhance public perception on PhilSys through accentuation of the quality of its governance and articulation of its attributes by conducting multi-stakeholder, multi-level, and multi-media advocacy activities to proactively engage the public and secure their backing and maximizing the use of social platforms to intensify it
- Pursue the continuing establishment of necessary systems for the seamless implementation of the enacted laws governing Philsys so as to streamline the delivery of services to the people
- Ensure that the PhilSys processes are efficient, the systems are fully functional, and all information within the system are secure
- Build organizational capabilities in preparation for the digital identity transformation by addressing digital skill gaps and investing in resources and technologies
- Overcome PhilSys barriers by identifying the processes, logistics, cultural elements and other factors that could hinder it, and devise strategies to move past each of these barriers
- Build a transformation method that reacts to feedback quickly and continually

Chapter 4

Overall Recommendations

The success of a digital identity project is dependent on its ability to achieve sustainable development. In this regard, policies and solutions put in place by governments or private entities alike should take into account the Sustainable Development Goals (SDGs).

The United Nations SDGs provide the ambitious target that all people will be able to obtain a "legal identity" by 2030 (SDG 16.9). This is part of Goal 16, which is to promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.

Much of such were discussed during the Face-to-Face Workshop, particularly to identify and understand issues faced by each country regarding the implementation of the NDIF. The participants also had the opportunity to hear from experts from various countries regarding a range of issues surrounding the implementation of the NDIF. In particular, the experts included:

(a) Mr. Luca Castellani, who presented on the human rights aspects of an NDIF, focusing on the legal aspects of identity management;

(b) Ms. Mariann Kirsipuu, who gave a presentation on how Data Protection and Cybersecurity have been effectively managed in Estonia;

(c) Mr. Rahul Goel, who shared the progress of India's Aadhar Digital Identification System;

(d) Ms. Isabelle Durant, who shared her experiences as an ex-Minister in the Belgian federal government;

(e) Mr. Yann Duval, who presented on promoting paperless trade in the Asia-Pacific region; and,

(f) Mr. Kwok Jia Chuan, who presented on the evolution of digital identity in Singapore.

Given the expert views, and each of the participant's presentation on an aspect of digital identity, a list of recommendations was defined by the participants during the Face-to-Face Workshop:

At the policy level

(1) Sensitize Governments' institutions and the private sector about the question of Digital Identity and its cross-cutting functions for social and economic development

(2) Create glossary of terms used in digital ID to ensure common understanding across organisations and countries in the ASEAN

(3) Formulate a clear vision on objectives of digital ID system, as the objectives will shape the form of ID system and framework adopted

(4) Assess the existing ID systems of governmental agencies, as well as countries' present legal and administrative framework to pinpoint specific areas of improvement (such as for data protection, non-discrimination, etc.)

(5) Prepare an inclusive framework for digital ID (services/registration/statistics collection) including local government and municipalities

(6) Explore the use of a National Digital Identity Framework for identification in accessing government and private services such as driver's license, voter's ID, taxes, banks, etc.

(7) Promote digital readiness of citizens and access to digital technologies, including through mobile platforms

(8) Educate citizens on risks and obligations of digitalization by conducting multi-stakeholder/multi-level advocacy activities

(9) Strike the balance between users' convenience and privacy requirements of digital ID systems (data protection)

(10) Design interoperable digital ID systems taking into account best practices and international standards within the ASEAN countries

(11) Build trust in digital ID systems in particular with interaction between public/private service providers and users

(12) Enhance inter-ministerial/agencies collaboration on legislation pertinent to the digital economy, fostering compliance and cross-border issues

(13) Engage in ongoing efforts to develop reference legal texts on identity management and trust services including cybersecurity and personal data protection aspects

(14) Establish effective institutional mechanisms in charge of oversight of digital ID, cybersecurity and data protection

(15) Establish strong collaboration with the private sector and provision for the budget to explore the use of distributed ledger technology

(16) Undertake regular audit and adapt digital ID systems to ensure fit for purpose and minimise risks of obsolescence

(17) Build technical knowledge of civil servants regarding digital technology implementation in particular with digital ID systems

Development partners' assistance

Offer assistance aimed at increasing capacity in the legal and technical requirements needed to implement Digital ID systems and the relevant legal infrastructure, including in the area of data protection, e-payment and e-commerce platforms

Ensure continued access to latest knowledge (UN research and case studies, new standards, policies, or regulations from other countries relating to Digital Identity)

Offer technical assistance on developing digital identity solutions and systems (from the World Bank, UNCTAD, UNCITRAL, UNESCAP and others)

Conclusion

An NDIF is an important foundation block in today's digital economy, not only to promote global trade, but also to improve access to basic services and amenities. Given the participants' overwhelming interest in the implementation of the NDIF, UNCTAD will continue its effort to encourage mutual learning between countries and within their regions in the areas of digital identity. With the support and continued efforts of the respective governments, given the groundwork that is already being done in this area, more progress is expected in the implementation of NDIF across ASEAN.

TRAIN FOR TRADE

Strengthening knowledge
and skills through innovative approaches
for sustainable economic development

TRAIN FOR TRADE

Strengthening knowledge
and skills through innovative approaches
for sustainable economic development

Printed at United Nations, Geneva – 2012969 **(E)** – October 2020 – 330 – **UNCTAD/DTL/KDB/2020/1**