

National Digital Identity (ID) Framework for Malaysia

Public Consultation Report

August 2020



Purpose of this document

The Public Consultation Report is part of the consulting engagement for National Digital (ID) Framework for Malaysia. It outlines details of the Public Consultation, including background and objectives of the exercise, analysis of feedback and overall findings that will be incorporated into the Final Report and recommendations on the proposed National Digital ID Framework.

The feedback received from various public and private organisations, as well as the Rakyat during the Public Consultation period has been analysed and taken into consideration when finalising the National Digital ID Framework for Malaysia. Detailed analysis and findings are further elaborated in this report.

Abbreviations

Abbreviation	Description
CGS	China Galaxy Securities
FAOM	Fintech Association of Malaysia
FGD	Focus Group Discussion
ICBC Malaysia	Industrial and Commercial Bank of China Malaysia
ICT	Information and Communications Technology
JPDP	Jabatan Perlindungan Data Peribadi
KDN	Kementerian Dalam Negeri
KKMM	Kementerian Komunikasi dan Multimedia Malaysia
KTMB	Keretapi Tanah Melayu Berhad
LHDNM	Lembaga Hasil Dalam Negeri Malaysia
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit
MDEC	Malaysia Digital Economy Corporation
MIDA	Malaysian Investment Development Authority
MOH	Ministry of Health
MOT	Ministry of Transport
MUFG	Mitsubishi UFJ Financial Group
MyCC	Malaysia Competition Commission
NDID	National Digital Identity
OCBC	Oversea-Chinese Banking Corporation
PC	Public Consultation
Pej SUK Terengganu	Pejabat Setiausaha Kerajaan Terengganu
UCSI University	University College Sedaya International
USIM	Universiti Sains Islam Malaysia
UTHM	Universiti Tun Hussein Onn Malaysia
UTP	Universiti Teknologi PETRONAS

Table of Contents

Purpose of this document.....	2
Abbreviations	3
Introduction	8
<hr/>	
1.1. Background.....	8
1.2. Objectives and Approach of Public Consultation	8
Profile of Respondents	11
Analysis and Findings - Rakyat	14
Analysis and Findings - Organisation	19
Appendices	31
<hr/>	
5.1. PC Briefing Session: Presentation Slides	31
5.2. Focus Group Discussion (FGD)	45
5.3. List of Respondents' Representation	49
5.4. Public Consultation Questions	54

List of Tables

Table 1. FGD – Telco	45
Table 2. FGD – E-commerce.....	46
Table 3. FGD – Banks	47
Table 4. FGD – E-Wallet	47
Table 5. FGD – PIDM	48
Table 6. FGD – List of ministries and government agencies	51
Table 7. List of private organisations.....	53

List of Figures

Figure 1. Rakyat - Other types of NDID functions/ services.....	54
Figure 2. Other areas of concern using NDID	54
Figure 3. Why respondents' have no interest in using NDID	55
Figure 4. Organisation - Other types of NDID functions/ services	56
Figure 5. Why NDID should not be adopted in organization	56
Figure 6. Why NDID will provide added value.....	57
Figure 7. Other use cases for NDID	57

List of Graphs

Graph 1. Participants' age	11
Graph 2. Participants' gender	11
Graph 3. Participants' location of residence	12
Graph 4. Participants' representation	12
Graph 5. Rakyat's view on National Digital ID Functions	14
Graph 6. Rakyat's Top 3 concerns for using NDID	15
Graph 7. Identified Key use cases by the Rakyat	16
Graph 8. Rakyat - Is NDID beneficial	17
Graph 9. Rakyat's interest to use NDID	17
Graph 10. Organisations' views on National Digital ID Functions	19
Graph 11. Organisation - Top 3 concerns for implementing NDID Programme	20
Graph 12. Participants' support in adopting NDID Programme	21
Graph 13. Any reason why NDID should not be adopted	21
Graph 14. Potential Challenges when adopting NDID	22
Graph 15. The use of identity verification and authentication	23
Graph 16. Organisations' current challenges	24
Graph 17. Identified key use cases by organisation	25
Graph 18. Types of transactions / uses should be excluded from using NDID	26
Graph 19. Organisation – Is NDID beneficial	27
Graph 20. Organisation – Top 3 benefits for using NDID	27
Graph 21. Organisation – NDID minimising overall cost	28
Graph 22. Organisation – Regulatory Restriction	29

Introduction

1.1. Background

The purpose of the National Digital ID (NDID) Framework is to build a trusted digital identity platform to enable individuals, businesses and government to effectively participate in the digital world. A National Digital ID is a verifiable platform of trust which aims to verify and uniquely credentialise a person's identity on the internet. Moving forward, it can be used by the government and private sector to verify and authenticate the identities of individuals who utilise electronic services and perform online transactions.

The introduction of a NDID Framework is a strategic step towards the development and transformation of various service sectors, given the significant increase in demand for digitalised platforms as well as the rapid growth of the digital economy. A National Digital Identity will also serve to complement other planned governmental initiatives such as:

- Pelan Jana Semula Ekonomi Negara (PENJANA) from the Ministry of Finance (MOF)
- Industry4WRD : National Policy on Industry 4.0 and National E-Commerce Strategic Roadmap from the Ministry of International Trade and Industry (MITI)
- *Pelan Tindakan Transformasi Kerajaan Digital* from the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)
- Financial Sector Blueprint 2011 – 2020 and policy document on Electronic Know-Your-Customer (e-KYC) from Bank Negara Malaysia (BNM)

The Malaysian Communications and Multimedia Commission (MCMC) was tasked to lead the development of the NDID Framework. PwC Consulting Associates (M) Sdn Bhd (PwC) was appointed by MCMC to assist in the development of the NDID Framework.

1.2. Objectives and Approach of Public Consultation

As part of the process to develop the NDID Framework, Public Consultation (PC) was conducted with the following objectives:

- Introduce the concept of NDID and scenario of its potential uses in Malaysia
- Obtain views and input on the potential adoption of NDID across public and private sectors
- Seek feedback and validate recommendations with relevant stakeholders across various ministries, government agencies, regulators, industry players and others

To initiate the PC, a briefing session was organised by MCMC on 16th July 2020 to brief stakeholders on the proposed framework and the expectations of the PC exercise. (Please refer to appendix 1.9 for the presentation materials). The session which was conducted by PwC was attended by various public and private sector organisations.

The PC was launched to organisational stakeholders via email invitation and took place between 13th July and 7th August 2020. PC for the Rakyat was officially launched and communicated through MCMC's official media releases and SMS blast. The PC document was made available to the Rakyat via MCMC's website and was open for feedback from 24th July to 7th August 2020. Additionally, focus group discussions were also conducted with selected industry players from various sectors / focus areas including financial services, Telco, E-Wallet, E-commerce, etc. (please refer to appendix 1.10 for the responses from the focus group discussions).

67 responses from ministries / government agencies, 156 responses from private organisations and 35,160 responses from individuals were collected throughout the consultation period (please refer to appendix 1.11 for a full list of respondents' representations from ministries / government agencies and private organisations).

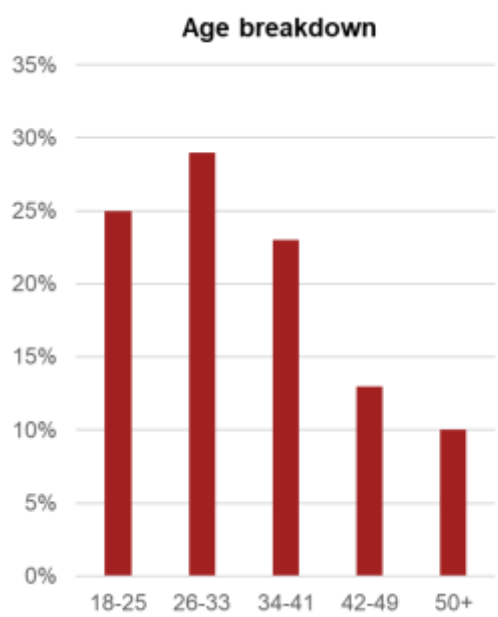


Section 2

Respondents'
Demographic

Profile of Respondents

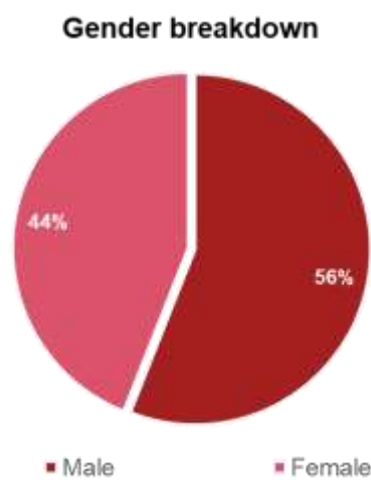
2.1. Age



Graph 1. Participants' age

- Majority of respondents are between the age of 26-33

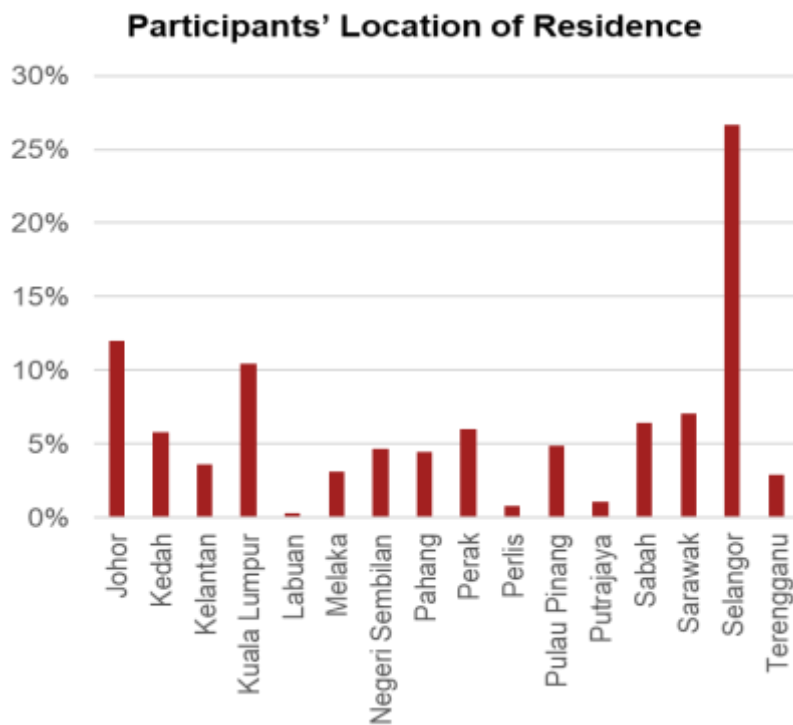
2.2. Gender



Graph 2. Participants' gender

- 56% of respondents are male and 44% respondents are female

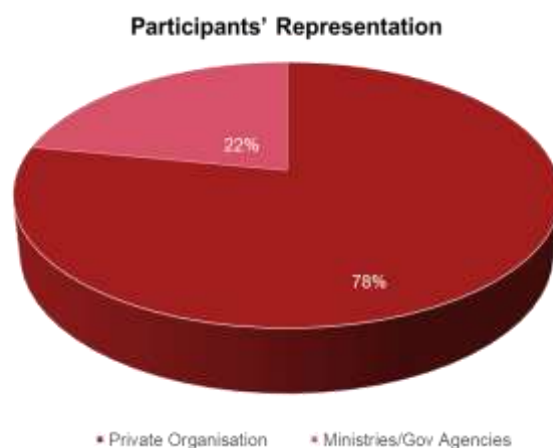
2.3. Location of Residence



Graph 3. Participants' location of residence

- The top 3 states that provided the most responses are Selangor, Johor and Kuala Lumpur
- The top 3 states that provided the least responses are Labuan, Perlis and Putrajaya

2.4. Organisation Participants' Representation



Graph 4. Participants' representation

- 78% of respondents represent Private Organisation and 22% of respondents represent ministries / government agencies



Section 3

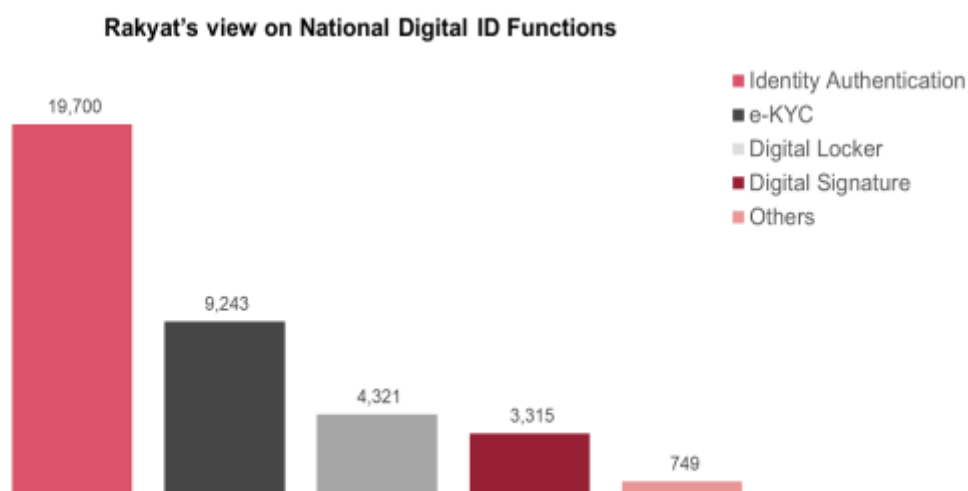
Rakyat

Analysis and Findings - Rakyat

3.1. Questions for the Rakyat

1. Based on your current understanding, which National Digital ID function/ service would benefit you the most with the implementation of the NDID programme? *Please rank your response from highest to least beneficial service*

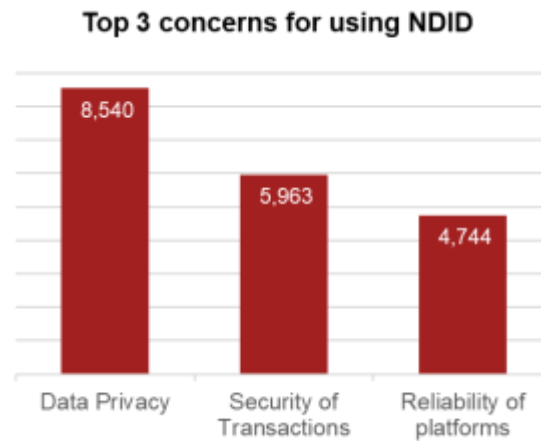
- () e-KYC () Storing of personal documents digitally in a 'digital locker'
() Identity authentication () Others (Please specify)
() Digital signature



Graph 5. Rakyat's view on National Digital ID Functions

- Overall results showed that identity authentication was deemed as the most beneficial, followed by e-KYC, digital locker and digital signature
- Other NDID functions/ services mentioned that would benefit the Rakyat include digital banking, e-Voting, EPF, financial services, e-Wallet, transportation, health and academic system, e-Tax, face recognition, driver license, insurance claims, health record, governmental application and welfare benefits
- To promote adoption and usage of NDID, it is recommended that e-KYC and digital signature be prioritised as services to be offered to the public as part of the NDID programme. Digital locker is a type of value-added service, which can be offered together with other value-added services in the future as the ecosystem matures and as the public becomes more aware of the NDID programme

2. What are your top three (3) areas of concern in relation to the implementation of the NDID Programme?
- | | |
|--|-------------------------------|
| () Security | () Technology |
| () Data privacy | () User/ Customer acceptance |
| () Cost to adopt National Digital ID | () Others (Please specify) |
| () Capacity and capability of Human Resources | |

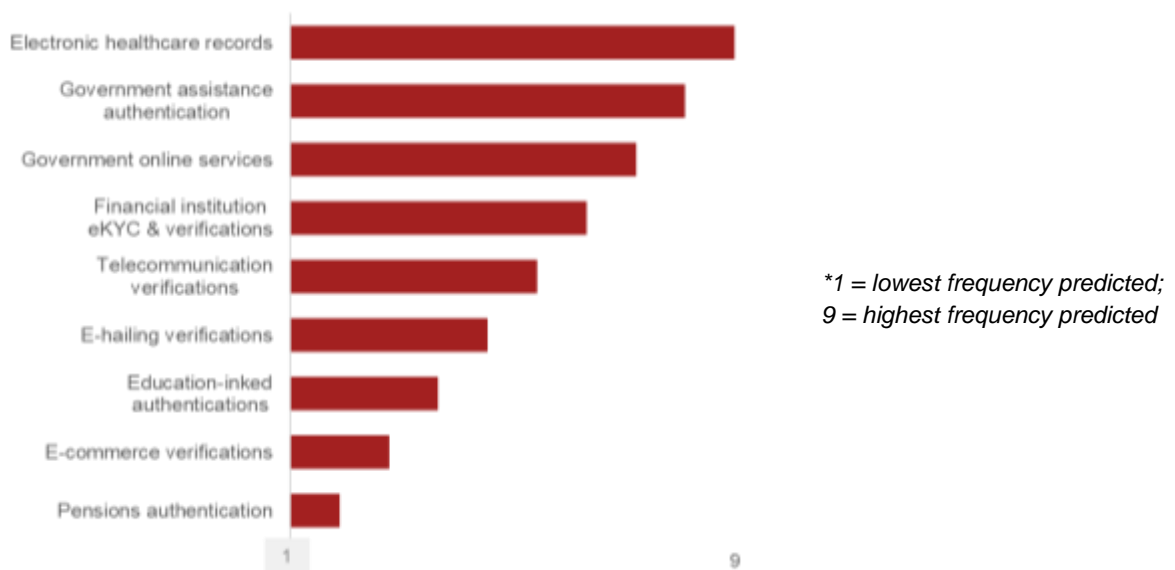


Graph 6. Rakyat's Top 3 concerns for using NDID

- The top three (3) areas of concern in relation to the implementation of NDID are data privacy, security of transactions and reliability of platforms
- Whilst the proposed NDID Programme is equipped with privacy and security by design, it is crucial that matters relating to data privacy, security and reliability of platforms are emphasised and communicated to the public through the NDID awareness campaigns. This is to build trust in the ecosystem and drive adoption of NDID

3. Please rank the nine (9) identified key use cases, based on predicted frequency of use by citizens

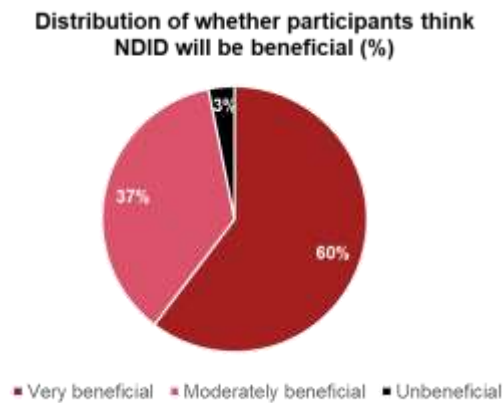
- | | |
|---|--------------------------------------|
| () Electronic healthcare records | () E- hailing verifications |
| () Government assistance authentication | () Education linked authentications |
| () Government online services | () E-commerce verifications |
| () Financial institution e-KYC & verifications | () Pensions authentication |
| () Telecommunication verifications | |



Graph 7. Identified Key use cases by the Rakyat

- The top three (3) identified key use cases are electronic healthcare records, government assistance authentication and government online services
- The three (3) use cases which were ranked the lowest scores are education-link authentication, e-commerce verification and pensions authentication
- Based on the above findings, it is recommended that the roll out of electronic healthcare records, government assistance authentication and government online services use cases be prioritised for the initial phase of the NDID programme.

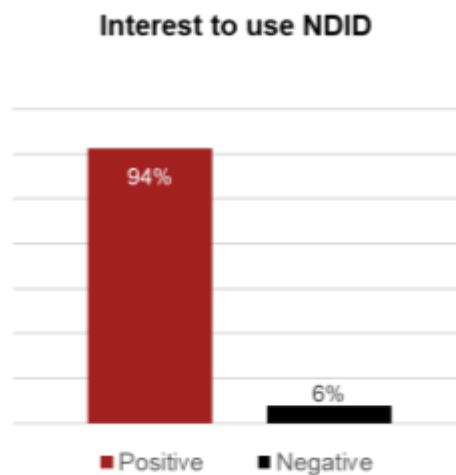
4. How will the National Digital ID Programme benefit you?



Graph 8. Rakyat - Is NDID beneficial

- 60% of the participants voted very beneficial, 37% voted moderately beneficial and 3% voted unbeneficial

5. In the future, when National Digital ID is made available to the public, will you be interested to use Digital ID when transacting with both public and private sectors?



Graph 9. Rakyat's interest to use NDID

- 94% of respondents are interested to use NDID when transacting with both public and private sectors
- 6% of respondents are not interested to use NDID. Reasons given include privacy issues, stability and security of the system, reliability of the platform and abuse of personal data



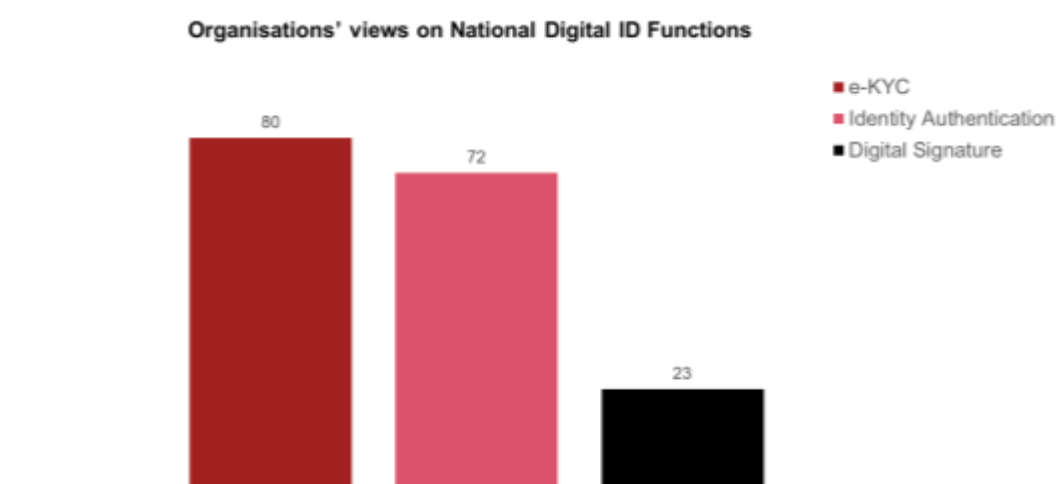
Section 4

Organisations

Analysis and Findings - Organisation

4.1. Questions for the Ministries / Government Agencies & Organisation

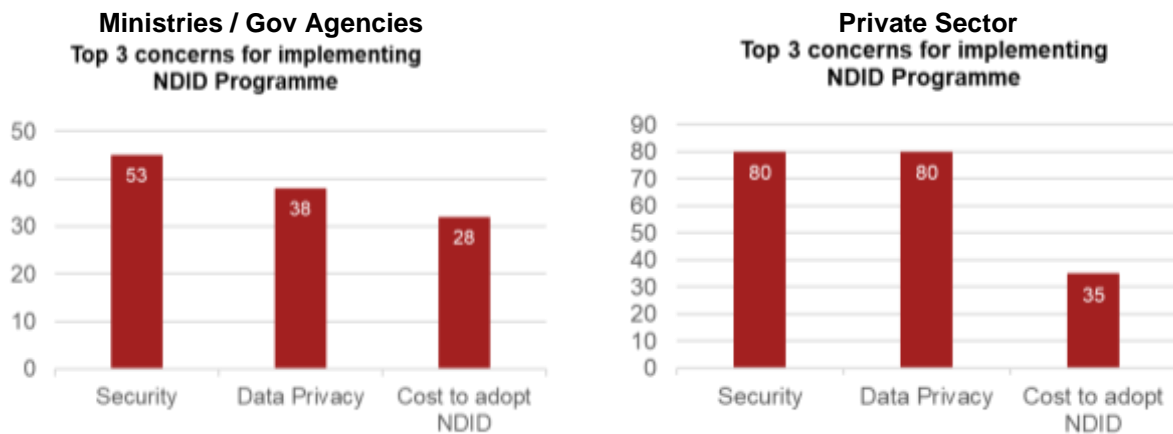
1. Which of the following National Digital ID functions would be most relevant and beneficial to your ministry / agency / company? *Please rank your response from highest to least beneficial services*
() e-KYC
() Identity authentication
() Digital signing
() Others (*Please specify*)



Graph 10. Organisations' views on National Digital ID Functions

- Overall result showed that e-KYC was deemed as the most beneficial, followed by identity authentication and digital signature
- Other Digital ID functions/ services mentioned that would benefit organisations include digital asset ownership, EPF income and employment verification, credit and bankruptcy check, crime case history, single sign on for all services, driver license information, online income verification, crowd tracking, better customer on-boarding experience and document authenticity verification from exam results and certificates
- To drive adoption of NDID amongst organisations, it is recommended that e-KYC, identity authentication and digital signature be included as part of NDID services. Other services can be added in the future as the ecosystem matures and as the public becomes more aware of the NDID programme

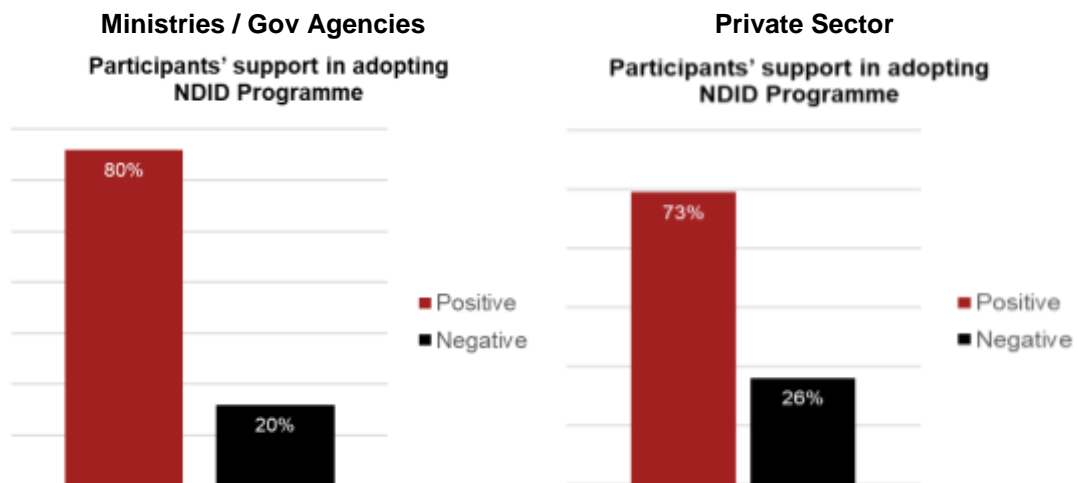
2. What are your top three (3) areas of concern in relation to the implementation of the NDID Programme?
- | | |
|--|-------------------------------|
| () Security | () Technology |
| () Data privacy | () User/ Customer acceptance |
| () Cost to adopt National Digital ID | () Others (Please specify) |
| () Capacity and capability of Human Resources | |



Graph 11. Organisation - Top 3 concerns for implementing NDID Programme

- Both ministries / government agencies and private sector respondents voted security, data privacy and cost to adopt NDID as the top three (3) areas of concerns to implement NDID
- Whilst the proposed NDID Programme is equipped with privacy and security by design, it is crucial that matters relating to data privacy and security are emphasised and communicated to organisational stakeholders through the NDID awareness campaigns. This is to build trust in the ecosystem and drive adoption of NDID.
- Additionally, it is recommended that engagement sessions be held with potential service providers / organisations on the adoption requirements to allow them to better plan and coordinate for the implementation of NDID within their organisations / operations, including cost requirements

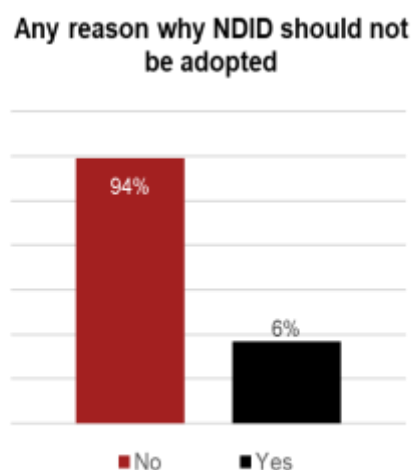
Do you foresee opportunities for National Digital ID to provide added value to your services / products?



Graph 12. Participants' support in adopting NDID Programme

- 80% of ministries / government agencies and 73% of Private Sector respondents foresee opportunities for NDID to provide added value to their services / products

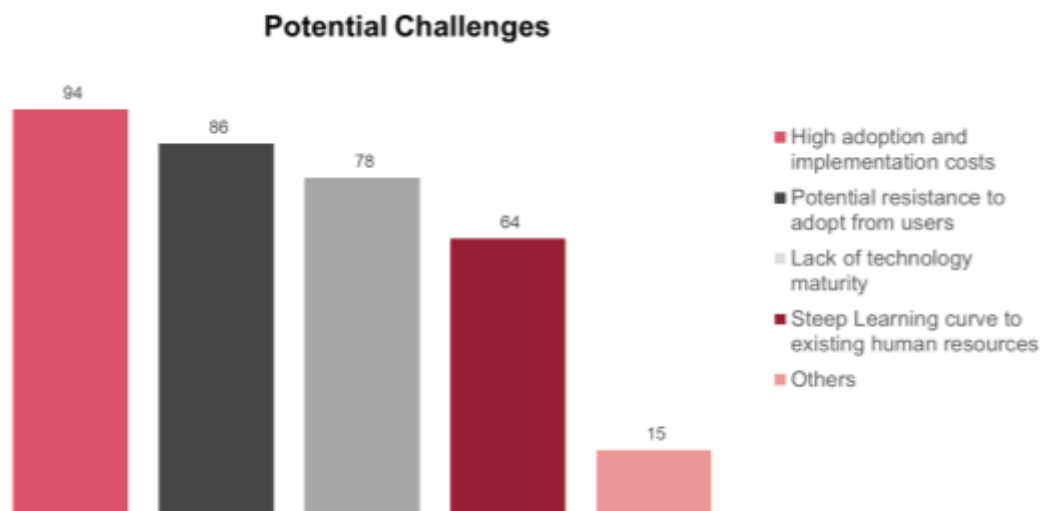
3. Do you foresee any reasons why the NDID Programme **should not** be adopted within your ministry / agency / company?



Graph 13. Any reason why NDID should not be adopted

- 94% of the respondents do not foresee any reason why the NDID Programme should not be adopted in their ministry / agency / company
- However, the remaining 6% believe that the NDID Programme should not be adopted due to the lack of resources, high cost, security and capability of the programme and lack of interest from citizens due to privacy concerns.

4. What are the potential challenges that may be faced by your organisation when adopting NDID? *You can select multiple options*
- | | |
|--|--|
| () Lack of technology maturity | () Potential resistance to adopt from users |
| () High adoption and implementation costs | () Others (Please specify) |
| () Steep learning curve to existing human resources | |

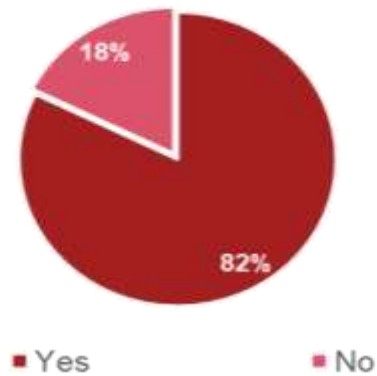


Graph 14. Potential Challenges when adopting NDID

- The top three (3) potential challenges when adopting NDID are high adoption and implementation costs, potential resistance to adopt from users and lack of technology maturity
- Other potential challenges include:
 - Data breach
 - Customers' willingness to adopt NDID
 - Lack of clarity on evidentiary value of digital signature
 - Prevention of data corruption
 - System & data integration
 - Privacy & security
 - Non-holistic implementation approach
 - Poor funding & support from government
 - Poor marketing & Got-To-Market strategy for users' awareness and education
- It is recommended that engagement sessions be held with potential service providers / organisations on the adoption requirements to allow them to better plan and coordinate for the implementation of NDID within their organisations / operations, including technology requirements, change management, customer awareness etc.

5. Currently, does your organisation perform any form of identity verification and authentication?

Organisation perform any form of identity verification and authentication



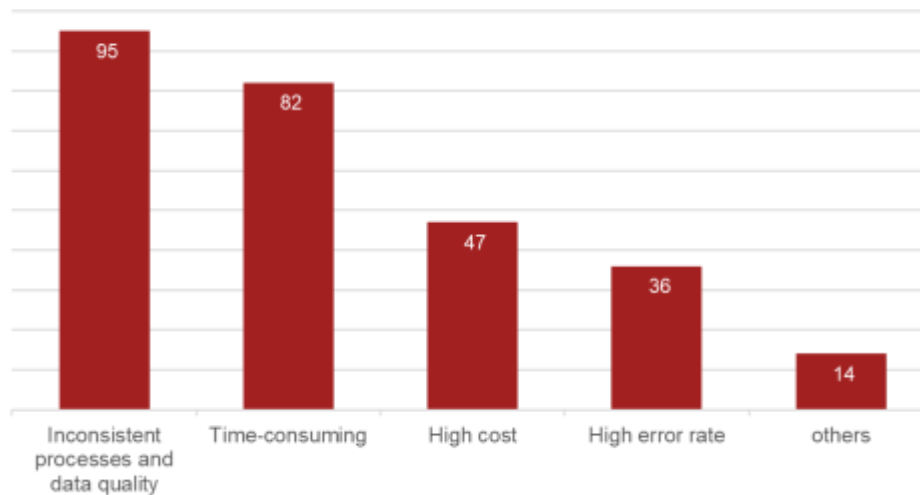
Graph 15. The use of identity verification and authentication

- 82% of organisation currently do perform some form of identity verification and authentication whilst 18% organisation do not

6. What are the current challenges faced by your organisation in relation to customer identity verification / authentication processes? *You can select multiple options*

- ☐ Time-consuming
- ☐ High cost
- ☐ Inconsistent processes and data quality
- ☐ High error rate
- ☐ Others (Please specify)

Organisations' Current Challenges

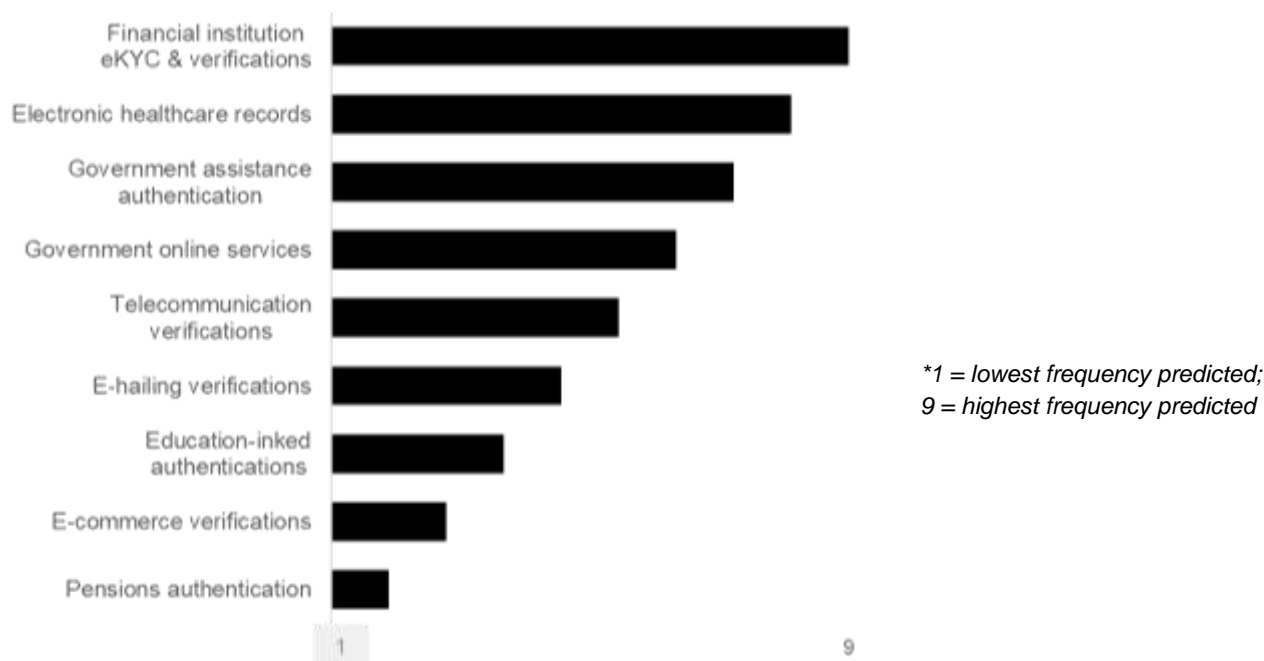


Graph 16. Organisations' current challenges

- The top three (3) current challenges faced by organisations in relation to customer identification / authentication processes are time-consuming processes, inconsistent processes and data quality and high cost
- Other current challenges faced by organisation in relation to customer identity verification / authentication process are:
 - Services that violate PDPA and privacy
 - Instability of MYKad reader
 - Falsification of documents
 - Validation to National Registration Department for digital channels
 - Customers need to physically visit the branches to get verified
 - Limitations on e-KYC process

7. Please rank the nine (9) identified key use cases, based on predicted frequency of use by citizens

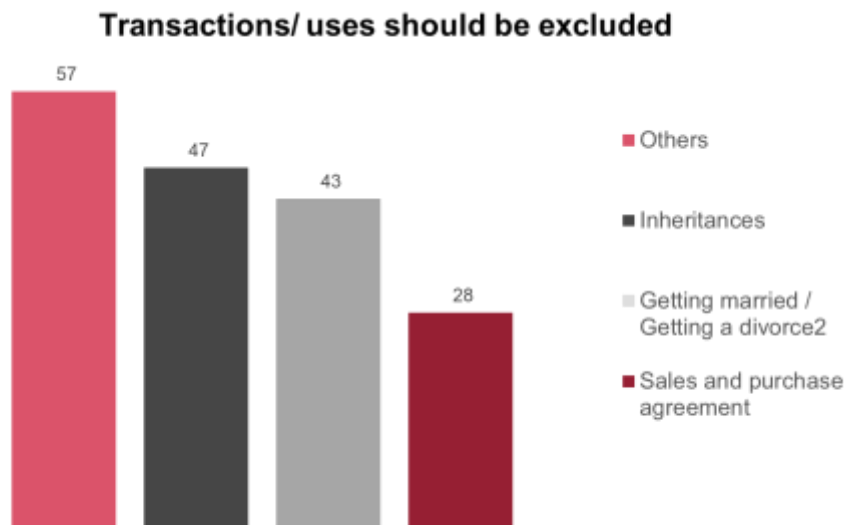
- | | |
|---|--------------------------------------|
| () Electronic healthcare records | () E- hailing verifications |
| () Government assistance authentication | () Education linked authentications |
| () Government online services | () E-commerce verifications |
| () Financial institution e-KYC & verifications | () Pensions authentication |
| () Telecommunication verifications | |



Graph 17. Identified key use cases by organisation

- The top three (3) identified key use cases are financial institution e-KYC & verifications, electronic healthcare records and government assistance authentication
- The three (3) use cases which were ranked the lowest scores are education-link authentication, e-commerce verification and pensions authentication
- Based on the above findings, it is recommended that the roll out of financial institution e-KYC, electronic healthcare records and government assistance authentication use cases be prioritised for the initial phase of NDID programme.

8. In your opinion, which of the following examples of transactions / uses should be **excluded** from using National Digital ID? *You can select more than one option*
- () Getting married / getting a divorce
 - () Sales and purchase agreement
 - () Inheritances
 - () Others (*Please elaborate*)



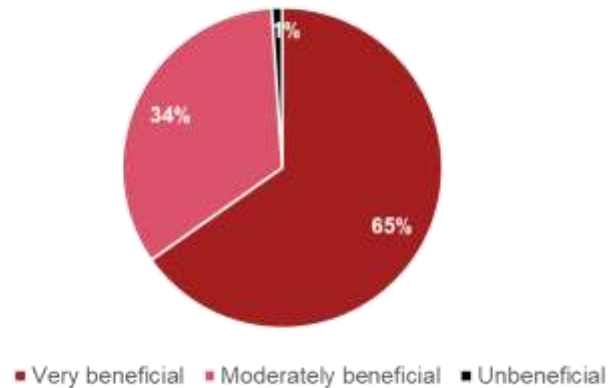
Graph 18. Types of transactions / uses should be excluded from using NDID

- Majority of the respondents chose other transactions / uses such as:
 - Services that violate PDPA and privacy
 - Geo-location, phone calls
 - Buying and selling goods
 - Molecular biology and genetics data
 - Information for adoption
 - Transactional logging system
 - Transactions that requires high commitment from users
 - Online gaming
 - Groceries transaction

9. How will the adoption of NDID Programme benefit your ministry / agency / company?

- Very beneficial
- Moderately beneficial
- Not beneficial

Distribution of whether participants think NDID will be beneficial (%)



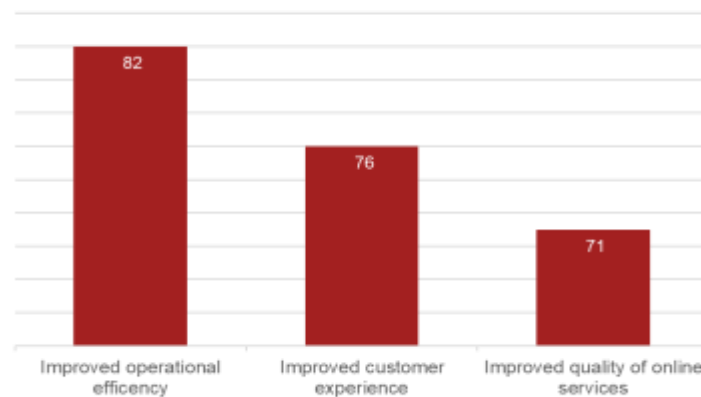
Graph 19. Organisation – Is NDID beneficial

- 65% of the participants voted very beneficial, 34% moderately beneficial and 1% unbeneficial

10. What are the top three (3) benefits to your ministry / agency / company with the adoption of NDID?

- () Improved operational efficiency
- () Reduced operating cost
- () Improved quality of online services
- () Improved customer experience
- () Others (Please specify)

Top 3 benefits for using NDID

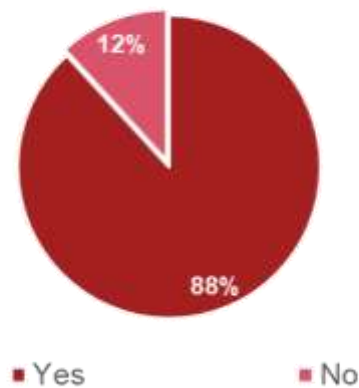


Graph 20. Organisation – Top 3 benefits for using NDID

- The top three (3) benefits are improved operational efficiency, improved quality of online services and improved customer experience
- Other benefits identified include reduction of fraud and internal misconduct, increased labour productivity and efficiency, increase technology awareness and customer experience.

11. Do you foresee National Digital ID minimising the overall cost for identity verification processes?

Organisation foresee NDID minimise overall cost for identity verification processes

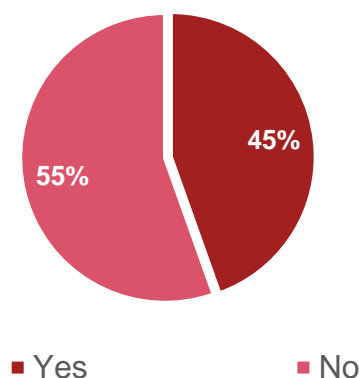


Graph 21. Organisation – NDID minimising overall cost

- 88% of participants foresee NDID minimising overall cost for identity verification processes.
- 12% of participants do not foresee National Digital ID minimising the overall cost for identity verification processes due to:
 - Numbers of additional hardware or system integration
 - Huge investment required
 - Cost in training for human resources
 - Cost for maintenance and support
 - The need to integrate new systems and processes

12. Do you foresee any regulatory restrictions within your organisation / industry that would pose a challenge in the implementation of National Digital ID?

Regulatory Restriction that poses a challenge implementing NDID



Graph 22. Organisation – Regulatory Restriction

- 55% of participants do not foresee any regulatory restriction within their organisation that would pose a challenge in the implementation of National Digital ID
- 45% of participants foresee potential regulatory / legal changes that are required within their ministry / agency / company to facilitate the adoption of NDID for the following reasons:
 - Possibly Personal Data Protection Act, depending on the security of the system. There will probably be needed to review how the user data is provided and what we should store in future.
 - Risk evaluation, legal terms and condition around privacy of data and customer consent, security of connectivity
 - Legal validation for new work processes and legal age for online onboarding (e-KYC)
 - Digital Signature Act; Potential changes to customer privacy and data protection law.
 - A clear guideline from BNM would be required on the adoption of NDID to establish banking relationship with the Bank.
 - Understanding the security measured framework in place
 - Statutory requirements for processes under the National Land Code, the National Land Code (Penang and Malacca Titles) Act
 - Legal - Need clarity and details over the scope of application. For example, whether and how this applies to the signing, authentication and filing of powers of attorney and instruments of dealings for land and properties, etc. How and by who will the documents be retained and who are the parties to sign section 90A Evidence Act certificate when adducing evidence in court, etc.



Section 5

Appendix

Appendices

5.1. PC Briefing Session: Presentation Slides



Objectives of Public Consultation

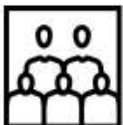
- 1 Introduce the concept of National Digital ID and the scenario of its potential uses in Malaysia
- 2 Seek feedback and validate recommendations with relevant stakeholders across various ministries, government agencies, regulators, industry players and others.
- 3 Obtain views on the potential adoption of National Digital ID across public and private sectors

What is National Digital ID?

National Digital ID is a digital form of identification used to obtain digital services and carry out online transactions in a more secure manner



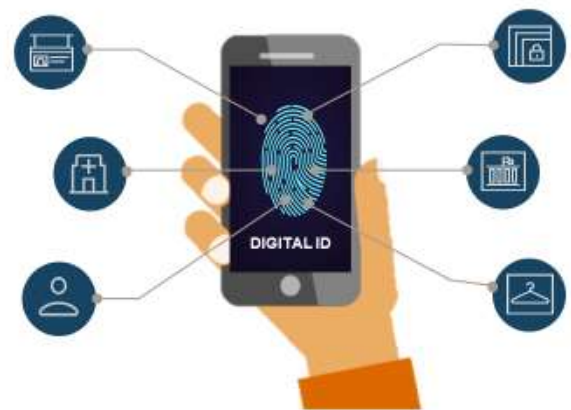
A secure and trusted platform to verify and authenticate the identity of an individual when transacting digitally
"Proving who you say you are"



Targeted at the citizens and permanent residents of Malaysia

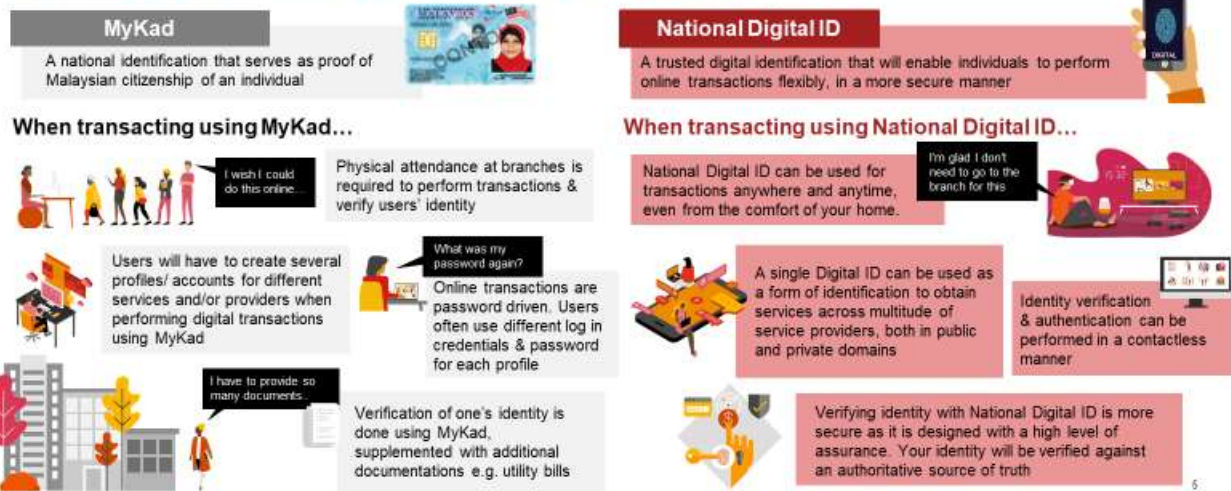


National Digital ID will NOT be replacing MyKad



How will National Digital ID complement MyKad?

National Digital ID will not be replacing MyKad as the proof of citizenship, but rather will complement it as a form of digital identification used when transacting digitally



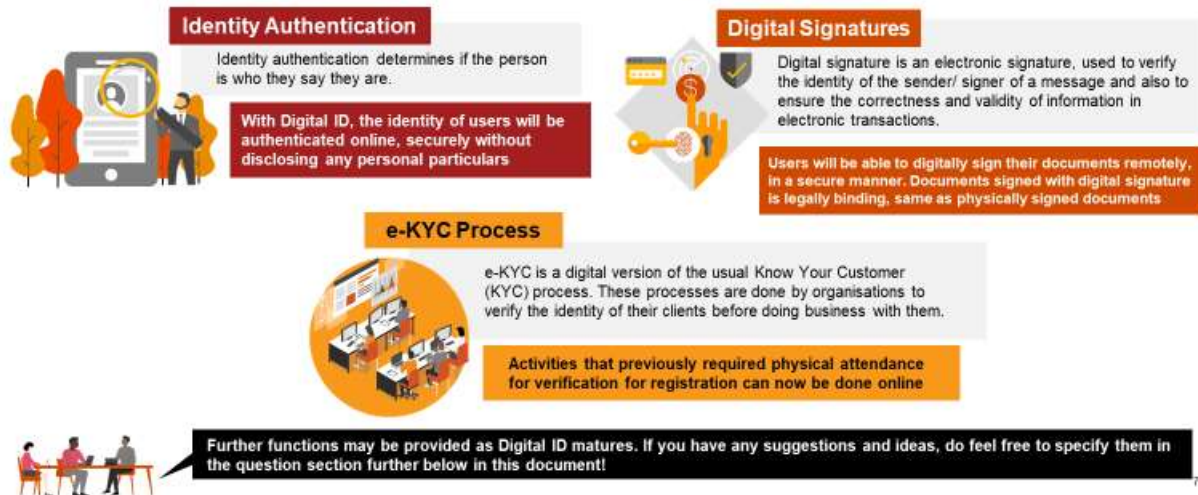
Who are the players in the National Digital ID ecosystem?

The success of National Digital ID will materialise through the dynamic interaction of the following key players in the ecosystem

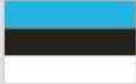


What are the functions of National Digital ID?




The uses of Digital ID revolve around safely verifying who you are in a convenient and secure manner. Below are some examples of activities that will be enabled by National Digital ID



How is it done in other countries?

	Description	Uses of Digital ID
 Estonia	<ul style="list-style-type: none">Estonia has become one of the most digitally integrated countries in the worldObjective of the program was to introduce a reliable and trustworthy identification system, with high acceptance by citizens and businesses to achieve effectiveness and efficiency of its use on a daily basis	<ul style="list-style-type: none">Over 900 organisations and enterprises use the Digital ID platform67% citizens use ID card regularlyLegal Travel ID for Estonian citizens travelling within EUNational Health Insurance Cardi-Votinge-Bankinge-Tax Board
 India	<ul style="list-style-type: none">Many of the Indian residents did not have any valid proof of identity available with them. Therefore, many govt. services and benefits did not reach the correct beneficiariesGovernment of India established the UIDAI to issue a unique ID to every resident of India to eliminate fake and duplicated identity	<ul style="list-style-type: none">1.25 bil residents registered for Digital IDScholarships by the governmentOpening of a bank accountIssuance of a new SIM cardRegistration and issuance of cooking gasDisbursal of ration, subsidies and cash transferHealth insurance schemeGuaranteed employment and pension scheme







How is it done in other countries? (2/2)

	Description	Uses of Digital ID
 Canada	<ul style="list-style-type: none"> Objective of the program was to use digital identities of citizens and residents available with banks and e-government services for verification and authentication. 	<ul style="list-style-type: none"> 80+ e-Government services can be accessed, including: <ul style="list-style-type: none"> Canada Pension Plan Old Age Security Benefits Access to Registered Retirement Savings Plan information and contribution limits Tax Benefits 2 years after the launch of the program, 1 million digital identity transactions per month were monitored
 Morocco	<ul style="list-style-type: none"> Purpose of this program was to deliver online and real-time identification services 	<ul style="list-style-type: none"> This project envisages to set up the "Unique digital ID system" which can authenticate citizens and residents in real time to deliver social benefits and commercial services.
 Australia	<ul style="list-style-type: none"> Government of Australia wants to have a Digital ID program that will give the Australian people and businesses a single, secure way to use government services online. 	<ul style="list-style-type: none"> Australian job search E-Tax Old Age Homes Health Record Medicare and health services

9

What are the potential uses of the National Digital ID for Malaysia? (1/2)




The proposed National Digital ID has various potential applications across a multitude of sectors, each with their own socioeconomic benefits. Nine (9) key use cases have been identified for NDID across various sectors.

Use Case	Description	Use Case	Description	Use Case	Description
1  Electronic healthcare records	Patients will be able to access their healthcare records online by logging into a secure e-health portal securely with their National Digital ID. These healthcare records can be shared by the patient with different parties upon their consent. Furthermore, they are able to review doctor visits, current prescriptions and check which doctors have had access to their files.	2  Government assistance authentication	With National Digital ID, citizens are able to automatically check their eligibility and register for government assistance programmes online. Less paperwork and documentation is required for registration and claiming processes. Incentives will be disbursed to recipients' bank accounts automatically upon online identity verification.	3  Government online services	National Digital ID will allow for more efficient and integrated e-government services. Citizens are able to access various government services (i.e. electronic tax claims, e-Business registration, e-voting and driving license application) online, in a more secure manner. Their identity will be verified and authenticated using National Digital ID, with minimal paperwork required.
4  Financial institution eKYC & verifications	National Digital ID will be able to facilitate a quicker and more seamless method of customer authentication to financial institutions. Using their National Digital ID, customers will be able to open bank accounts and perform various transactions such as applying for loans entirely from their mobile phone.	5  Telecommunication verifications	National Digital ID could help eliminate repetitive verification processes across consumers' lifespan with the company. Examples include updating of personal details (address etc), change of SIM card or when the customer loses his/her online account password.	6  E-hailing verifications	National Digital ID will improve the overall customer and driver experience by reducing time spent on identity verification during on-boarding for both customers and drivers. National Digital ID will also allow registration and verification of drivers to be done online, with minimal documentation to be submitted. This will increase trust and credibility of e-hailing platform.

10

What are the potential uses of the National Digital ID for Malaysia? (2/2)

The proposed National Digital ID has various potential applications across a multitude of sectors, each with their own socioeconomic benefits. Nine (9) key use cases have been identified for National Digital ID across various sectors.

Use Case	Description	Use Case	Description	Use Case	Description
7  Education linked authentications	National Digital ID will be able to facilitate the safe keeping of students attendance records along with helping in school and university entry applications and transfer requests. Other applications include scholarship applications and applications for work after graduation.	8  E-commerce verifications	National Digital ID will be used for buyer and seller verification. For the buyer verification, this would reduce the time spent by buyers on repetitive verification processes and thus improve the customer experience. For seller verification, this would improve the level of trust and assurance on the e-commerce platform.	9  Pensions authentication	With National Digital ID, pension management will be more convenient. Citizens will be able to update their personal details online (i.e. bank account, address, second beneficiaries), with minimal paperwork. Additionally, other pension benefits (e.g. medical benefits) can also be linked to National Digital ID. Citizens will no longer have to furnish their pension card when claiming for benefits.

Project Saya

Benefits of National Digital ID to various stakeholders



All personas and examples of use cases are recommended uses for National Digital ID in the future, and will require agreement from relevant stakeholders prior to implementation

Aisyah is a 24 year old graduate from UiTM Perlis who has been offered an engineering job in a large MNC in Kuala Lumpur...



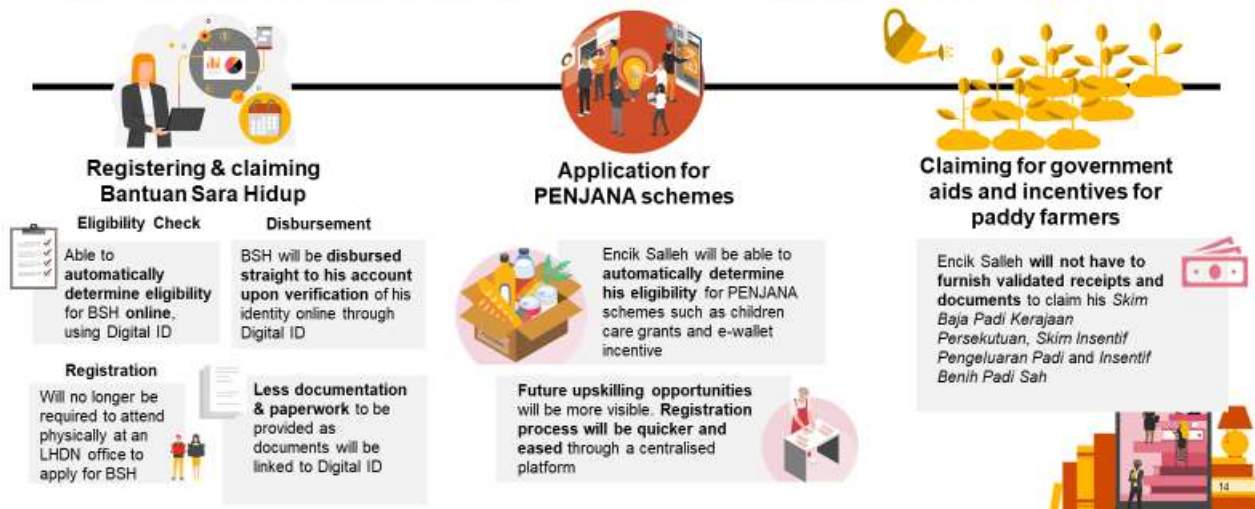
Digital ID can help Aisyah complete her job onboarding along with registering for a new bank account and telco subscription without facing the hassle of compiling old documents or even leaving her home



Encik Salleh is a 37-year old paddy farmer in Kedah who lives a very busy life, juggling his job and responsibilities as a single father of 2 children...



Digital ID will save his time, allowing him to focus on his job and children by enabling quick & easy claims of his B40 aids such as Bantuan Sara Hidup ("BSH") and other government assistance programmes



How can National Digital ID be used in e-government services?

Based on experiences of other countries, the following e-government services are enabled through National Digital ID:

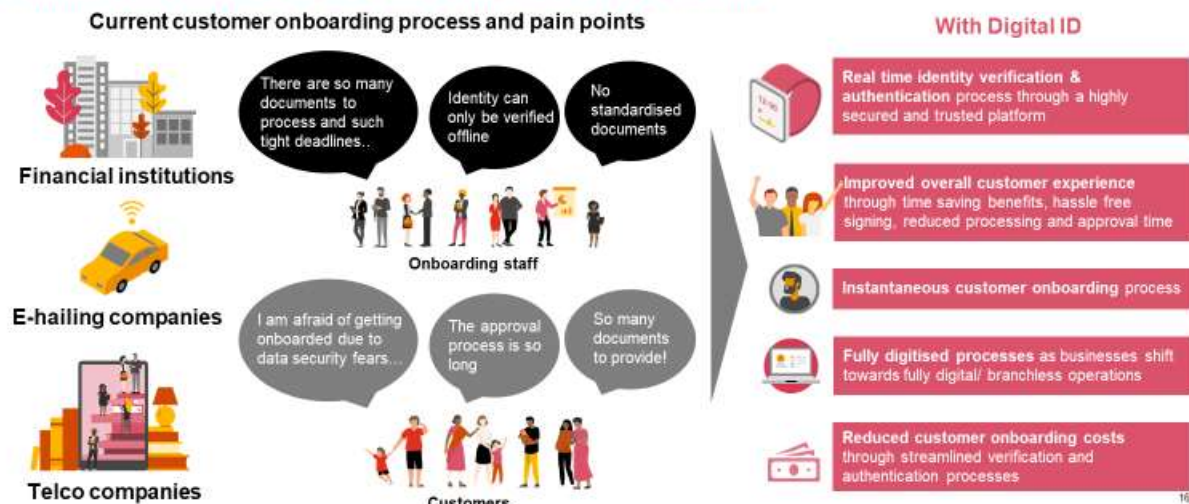
National Digital ID will unlock the following benefits...



Ministries & Government Agencies	The Public
<ul style="list-style-type: none"> Increases quality of e-government services Potential savings from reduced administrative costs, resulting from a more streamlined and automated authentication and verification process Robust and targeted welfare/ aids disbursement programmes to effectively target underprivileged segments of society 	<ul style="list-style-type: none"> Time saved from reduced travelling and elimination of repetitive identity authentication & verification processes Reduce possibility of users' identity being stolen and wrongfully used in performing online transactions Improve overall customer satisfaction




Digital ID will be able to alleviate pain points in the customer onboarding process across several industries

Digital ID will bring cost saving benefits through process improvements, along with added revenue from increased service adoption, due to improved user experience



16

Indicative roadmap for the implementation of National Digital ID Programme

		PHASE 1 (Y1) Quick Wins	PHASE 2 (Y2 – Y3)
 Onboarding	Eligibility	Covers citizens and permanent residents	
	Registration/Enrolment	Leverage existing demographics & biometrics data in JPN database (2 thumbprints and photo)	Additional biometrics to be collected (i.e. iris, 10 fingerprints)
 Authentication via Mobile ID for remote online services	Mobile ID Registration & Issuance	<ul style="list-style-type: none"> Upon enrolment, user will obtain Mobile ID as a credential through in-App on boarding process Digital Certificate to be issued upon registration of Mobile ID App (For authentication & digital signing) 	
	Authentication	Mobile ID is the channel to perform identity authentication, e-KYC and digital signing for online transactions	
	Authentication Factors	<ul style="list-style-type: none"> NDID no. (Mykad/MyPR) Hybrid of biometrics (device-based local authentication) – using existing biometrics in JPN database PKI 	<ul style="list-style-type: none"> NDID no. (Mykad/MyPR) Hybrid of biometrics (device-based local authentication) – using additional biometrics gathered PKI
 Authentication for proximity/ face-to-face services	Authentication	<ul style="list-style-type: none"> Proximity transactions/ services i.e. entering a building/ barrier gates, ATM machines - User can use biometrics to perform authentication via service provider's authentication devices i.e. existing readers, cameras Service counters – User shall continue using MyKad based authentication for all services 	
Features		<ul style="list-style-type: none"> ✓ Easier and quicker implementation ✓ Less risk in managing user perception ✗ Limited biometrics authentication capabilities 	<ul style="list-style-type: none"> ✓ Future proof ✓ Higher biometrics authentication capabilities ✗ Higher cost for additional biometrics collection ✗ Greater awareness efforts required to encourage users to provide additional biometrics

This proposed roadmap is still being developed, and will be further refined based on discussions with key stakeholders

17

Project

Saya

Q&A



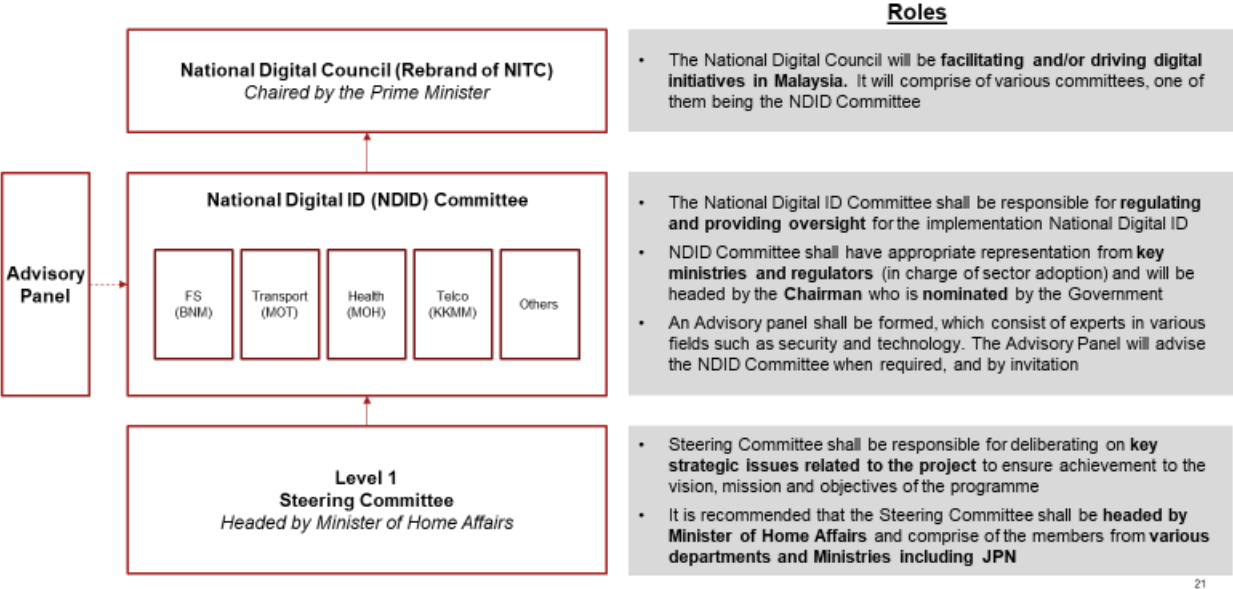
Project

Saya



Governance Framework

Proposed Governance Framework for the implementation of National Digital ID Programme



Legal & Regulatory Framework

Existing Legal and Regulatory Framework in the Identity Landscape

Relevant enabling laws and regulations, which must be considered to develop the national digital identity framework

Identity Database	<ul style="list-style-type: none"> Immigration Act 1959/63 ("IA") Immigration Regulations 1963 ("IR") National Registration Act 1959 ("NRA") National Registration Regulations 1990 ("NRR") 	<ul style="list-style-type: none"> IA / IR govern admissions into and departures from Malaysia; entry permits; procedures on arrival in Malaysia & removal from Malaysia; offences and special provisions for East Malaysia NRA / NRR provide for the registration of persons in Malaysia and for the issuance of identity cards. NRA / NRR are key legislation which legitimise the national identity of a person
Enablers of e-Government and e-Commerce	<ul style="list-style-type: none"> Electronic Commerce Act 2006 ("ECA") Electronic Government Activities Act 2007 ("EGAA") Digital Signature Act 1997 ("DSA") 	<ul style="list-style-type: none"> ECA facilitates the development of e-Commerce in Malaysia, as it legitimises commercial transactions made by electronic means EGAA facilitates the development of e-Government in Malaysia and allows Government to conduct public services virtually DSA facilitates e-Commerce and e-Government electronic activities for public and private sectors by using digital signatures to verify and authenticate legal and commercial transactions
Privacy and Cybersecurity	<ul style="list-style-type: none"> Personal Data Protection Act 2010 Personal Data Protection Regulations 2013 Personal Data Protection Standard 2015 Communications and Multimedia Act 1998 Computers Crimes Act 1997 Penal Code 	<ul style="list-style-type: none"> Regulates the processing of personal data in commercial transactions but does not apply to non-commercial transactions and Federal and State Governments Regulates the converging areas of communications and multimedia to ensure information security and network reliability and integrity in Malaysia Provides for offences relating to misuse of computers and unauthorised access to networks

Preliminary legal recommendations relevant to the implementation of National Digital ID framework in Malaysia

Identity Database	<ul style="list-style-type: none"> Immigration Act 1959/63 ("IA") Immigration Regulations 1963 ("IR") National Registration Act 1959 ("NRA") National Registration Regulations 1990 ("NRR") 	<ul style="list-style-type: none"> Amend IR / NRR to expressly allow data exchange between governmental entities such as JPN and JIM. Issue regulations under the NRA to provide for matters relevant to the implementation of NDID by JPN (e.g. the issuance and regulation of a digital identity; establishment and maintenance of a register; data protection; exchange of data; cybersecurity).
Enablers of e-Government and e-Commerce	<ul style="list-style-type: none"> Electronic Commerce Act 2006 ("ECA") Electronic Government Activities Act 2007 ("EGAA") Digital Signature Act 1997 ("DSA") 	<ul style="list-style-type: none"> No amendment required.
Privacy and Cybersecurity	<ul style="list-style-type: none"> Personal Data Protection Act 2010 Personal Data Protection Regulations 2013 Personal Data Protection Standard 2015 Communications and Multimedia Act 1998 Computers Crimes Act 1997 Penal Code 	<ul style="list-style-type: none"> Issue regulations / guidelines under PDPA for processing of data by data users.

24

Relevant laws, regulations and guidelines that must be considered with reference to key use cases identified in the National Digital ID framework

Key use cases	Laws, regulations & guidelines
Electronic health records	<ul style="list-style-type: none"> Private Healthcare Facilities And Services (Private Hospitals And Other Private Healthcare Facilities) Regulations 2006 Private Healthcare Facilities and Services (Private Medical Clinics or Private Dental Clinics) Regulations 2006 Malaysian Medical Council Guidelines on Confidentiality / Medical Records & Reports / Audio & Visual Recording / Code of Professional Conduct Medical Act 1971
Government subsidy	N/A
Pensions	Pensions Regulations 1980
E-hailing	Garis Panduan Perkhidmatan E-hailing Di Bawah Perniagaan Pengantaraan
Telecommunications	Guidelines on Registration of End-Users of Prepaid Public Cellular Service
Education	N/A
Financial services	<ul style="list-style-type: none"> Financial Service Act / Islamic Financial Services Act 2013 BNM Exposure Draft on e-KYC Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 / Policy Documents on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for DNFBPs and NBFIs & for FIs Electronic Commerce Act 2006
E-commerce	N/A
Government online services	Depends on the services provided

25

Level of Assurance (“LOA”) & Identity Authentication

LOA1 to LOA4 options are available within the program

#	Authentication Factors considered in the design
1	Biometrics (iris / face / fingerprint)
2	OTP (TOTP, SMS, Email)
3	Digital Certificate (Mobile ID)
4	Pin / Password

LOA 1	Any factor
LOA 2	Biometric or OTP or Digital certificate or PIN / Password
LOA 3	Biometric + OTP, Biometric + Digital certificates, Biometric + PIN/Password, OTP + Digital certificate, OTP + PIN/Password, Digital certificate + PIN/Password (cryptographic protection for secret keys)
LOA 4	Biometric + OTP, Biometric + PIN/Password, OTP + PIN/Password (In person identity proofing, PII/Sensitive information in authentication protocol to be cryptographically protected) Note: Digital certificate as one of the authentication parameters only if tamper resistant hardware for storage of secret or cryptographic keys.

Note: Level of assurance in practice is dependent upon correct implementation and successful implementations have been demonstrated by other programs/projects.

As a platform, the National Digital ID program can provide different type of authentication services with different levels of assurance depending on the service requirement..

Levels of assurance

In the case wherein the user is operating from Mobile device to onboard on the Mobile ID, we have suggested to carry out biometric based authentication using his MyKad along with OTP based authentication on the registered mobile number.

The citizen has to perform the following steps:

1. Provide his personal MyKad number to initiate the onboarding
2. Carry out Biometric Authentication (integrated with liveliness detection feature)
3. Be in the possession of the SIM card registered at Digital ID system
4. Carry out OTP-based authentication

Carrying out such authentication at the time of Mobile ID onboarding wherein a user is expected to provide his personal MyKad number, Biometric authentication and OTP based authentication will collectively result in very-high level of assurance.

Facial recognition is becoming one of the most acceptable means of biometric authentication, as it does not require contact with anyone. The inaccuracy rates in facial recognition technology were relatively higher a few years ago, but today it may not be the case.

Based on the recent NIST FRVT report, Facial recognition's FNIR 0.0027 (0.27%) FNIR @ FMR = 0.00001 (10^{-5}). This is already better or equally strong as compared to the fingerprint authentication.

"The major result of the evaluation is that massive gains in accuracy have been achieved in the last five years (2013-2018) and these far exceed improvements made in the prior period (2010-2013). While the industry gains are broad – at least 28 developers' algorithms now outperform the most accurate algorithm from late 2013 – there remains a wide range of capabilities.

With good quality portrait photos, the most accurate algorithms will find matching entries, when present, in galleries containing 12 million individuals, with error rates below 0.2%. The remaining errors are in large part attributable to long-run ageing and injury."

– NIST FRVT 2018 Study

28

Channels for Authentication

NDID platform provide different types of authentication catering to Service Provider requirements

Service Counters where currently MyKad is used for Verification

1. At existing Service Counters authentication (Offline mode) can be fulfilled by MyKad, which is currently widely used. However, going forward JPN can decide to introduce Digital ID as an option to the Service Providers.

Service Provider Counters (New NDID Use Cases – Education, Healthcare, etc.)

2. Various new use cases around healthcare, government benefits, education, etc. have been elaborated in the report. These services can consider NDID platform for authentication.
 - Apart from the above use cases, proximity services, entry / exit system, etc. can also be considered for Digital ID
 - The online authentication at Service Provider counter using the application will be done only through trusted and registered authentication devices.

Web-portals / Mobile App / etc.

3. Currently authentication using biometric devices (iris and fingerprint auth. devices) from web portal by the citizen will have very limited use as it is not envisaged that the citizen will be asked to purchase devices.
 - However, the citizen can on his smart phone enable Mobile ID and can use that platform for facial authentication.
 - Mobile ID will require facial authentication (ISO30107 compliant) and OTP authentication for onboarding. There are multiple controls built in the above multifactor authentication to address issues around fraud, replay attack.
 - Facial authentication implementation - Mastercard rolled out 12 countries, India is launching facial authentication, Australia has undertaken no. of field trials, Philippines and Morocco are planning to implement facial authentication

29

5.2. Focus Group Discussion (FGD)

5.2.1. Telco

#	Areas	Organisation	Key points
1.	Potential uses of National Digital ID in your organisation/ sector	U Mobile	<ul style="list-style-type: none"> NDID would be beneficial in allowing better customer reach, especially in the recent light of Covid-19 pandemic
		Maxis	<ul style="list-style-type: none"> e-KYC enabled by NDID will help drive services provided by e-commerce platforms, as well as improving customer outreach through remote means
		Telekom Malaysia	<ul style="list-style-type: none"> NDID usage can be extended beyond customer onboarding / registration. It can also facilitate B2B, B2G services to ensure a more streamlined, effective and efficient supply chain management. It was suggested that NDID's usage should be extended to a global scale i.e. G2G transactions, e-commerce. Stamping of document by LHDN can be digitised
2.	ID verification/ authentication practices (how is it being done currently, technology used, authentication costs, how can NDID be adopted)	Telekom Malaysia	<ul style="list-style-type: none"> Currently utility bill is requested to validate customers' last address
		Maxis	<ul style="list-style-type: none"> Based on current onboarding process, new customers / users are required to be present at physical stores to get registered for telco subscriptions. It would be beneficial if NDID could help by improving and facilitating customer outreach remotely
		Telekom Malaysia	<ul style="list-style-type: none"> RM 0.10 indicative cost per authentication is expensive
		Digi	<ul style="list-style-type: none"> Need to look at the whole process ecosystem before providing details on authentication costs
3.	Potential adoption of National Digital ID (key considerations/ readiness to adopt etc.)	Telekom Malaysia	<ul style="list-style-type: none"> There are various factors that will determine the adoption of NDID i.e. security of systems, compliance to existing regulations, technology and solutions design. Decisions to adopt is dependent on the assessment of these factors Security and trust are key factors to determine adoption of NDID. Suggested that Interim solutions be combined with the full NDID solutions to ensure delivery of high security, high assurance platform
		Maxis	<ul style="list-style-type: none"> Telco providers will be ready to adopt NDID in the next 2-3 years. However, this is subject to technology integration and cost considerations
		Telekom Malaysia	<ul style="list-style-type: none"> Adoption of NDID is dependent on various factors such as system procurement, establishment of new process, infrastructure and cost
		Telekom Malaysia	<ul style="list-style-type: none"> Has to be legally binding. Only comfortable to adopt when regulations are amended

Table 1. FGD – Telco

5.2.2.E-commerce

#	Areas	Organisation	Key points
1.	Potential uses of National Digital ID in your organisation/ sector	Pos Digicert	<ul style="list-style-type: none"> • NDID can be used as part of Proof of Delivery (PoD). Current process requires physical signature of recipient. Due to the pandemic, recipients are to provide their last 4-digit numbers of the MyKad • Consider inclusion of non-citizens/ other eligible residents as they constitute a large customer base for Pos Malaysia
2.	ID verification/ authentication practices (how is it being done currently, technology used, authentication costs, how can NDID be adopted)	Pos Digicert	<ul style="list-style-type: none"> • Current authentication process during delivery (PoD) is done at 0 cost. Since there is a charging mechanism to SP to use NDID services, adoption might need to be carefully evaluated. Additionally, certain customer authentication costs are shared with their partners (i.e. Western Union) • 1,000 touchpoints depend on the services the customer want to do, cost is shared together with service providers (e.g. Western Union). Still premature to discuss the appropriate pricing mechanism for authentication services
		Lazada	<ul style="list-style-type: none"> • Onboarding of customer - Currently there are a lot of cases of identity forging by customers (i.e. creation of ghost accounts). Similar issues faced with individual sellers, registered businesses Proof of Delivery - Done manually • Additional cost per acquisition will be a setback to the commercial team
3.	Potential adoption of National Digital ID (key considerations/ readiness to adopt etc.)	Lazada	<ul style="list-style-type: none"> • Technology wise, the company might be ready to adopt National Digital ID. However, an assessment needs to be done to ensure adoption is aligned to the overall business strategy
		Pos Digicert	<ul style="list-style-type: none"> • Should the government decide to enrol citizens for NDID next year, JPN can leverage on Pos Malaysia counters all over Malaysia
4.	Legal & regulatory considerations to enable adoption of NDID? (Existing restrictions/ any amendments required)	N/A	<ul style="list-style-type: none"> • To check if there are any legal restrictions in the Postal Act 2012

Table 2. FGD – E-commerce

5.2.3.Banks

#	Areas	Organisation	Key points
1.	Potential uses of National Digital ID in your organisation/ sector	N/A	<ul style="list-style-type: none"> No response provided
2.	ID verification/ authentication practices (how is it being done currently, technology used, authentication costs, how can NDID be adopted)	N/A	<ul style="list-style-type: none"> No response provided
3.	Potential adoption of National Digital ID (key considerations / readiness to adopt etc.)	Maybank	<ul style="list-style-type: none"> Given that they are bound by AML/ CFT requirements, certain aspects of e-KYC might not allow usage of NDID. Given the main focus has always been customer experience, if NDID will significantly improve this, Banks will consider adopting

Table 3. FGD – Banks

5.2.4.E-Wallet

#	Areas	Organisation	Key points
1.	Potential uses of National Digital ID in your organisation/ sector	Grab Pay	<ul style="list-style-type: none"> Linkage to credit bureau or perform credit assessment - more seamless and real time to extract data Potentially be used for on-going Due Diligence
2.	ID verification/ authentication practices (how is it being done currently, technology used, authentication costs, how can NDID be adopted)	TnG	<ul style="list-style-type: none"> TnG is already doing identity verification digitally. Users are already educated on this sort of onboarding process. NDID to further help in improving overall customer experience
		Grab Pay	<ul style="list-style-type: none"> Grab Pay is already investing on facial recognition and liveness technology to perform ID verification
		Grab Pay	<ul style="list-style-type: none"> Will it be linked to the blacklist database?
3.	Potential adoption of National Digital ID (key considerations/ readiness to adopt etc.)	Grab Pay	<ul style="list-style-type: none"> Highly dependent on cost to maintain 2 system (to cater for users with NDID vs users without NDID) and take up rate of citizen of Malaysia
		Grab Pay	<ul style="list-style-type: none"> Independent app for the NDID? host-to-host connection Any solution on e-KYC using biometrics on phone, rather than face-to-face? (Their current technology) What are the SDK required?

Table 4. FGD – E-Wallet

5.2.5.PIDM

#	Areas	Organisation	Key points
1.	Potential uses of National Digital ID in your organisation/ sector	N/A	<ul style="list-style-type: none"> • Reimbursement • Reimbursement - Know who to pay, but don't know where to pay to (bank accounts) Wish to have a microsite - (e-KYC linked to JPN) to confirm the true depositor, then take the instruction from the depositor on where to pay to
2.	ID verification/ authentication practices (how is it being done currently, technology used, authentication costs, how can NDID be adopted)	N/A	<ul style="list-style-type: none"> • Wish to be able to perform authentication without being at the premises itself
3.	Potential adoption of National Digital ID (key considerations/ readiness to adopt etc.)	N/A	<ul style="list-style-type: none"> • Dependant on financial services industry, NDID good to have

Table 5. FGD – PIDM

5.3. List of Respondents' Representation

5.3.1. Ministries and Government Agencies

#	Name of Ministries / Government Agencies
1.	Agensi Pengangkutan Awam Darat
2.	Jabatan Kemajuan Islam Malaysia (JAKIM)
3.	Jabatan Perdana Menteri
4.	Jabatan Ketua Menteri Melaka
5.	Jabatan Kewangan dan Perbendaharaan Negeri Melaka
6.	Jabatan Perlindungan Data Peribadi (JPDP)
7.	Kementerian Dalam Negeri (KDN)
8.	Kem Pelancongan Seni Dan Budaya
9.	Kementerian Kewangan Negeri Sabah
10.	Kementerian Pembangunan Luar Bandar
11.	Kementerian Pendidikan Malaysia
12.	Kementerian Pengajian Tinggi
13.	Kementerian Komunikasi dan Multimedia Malaysia (KKMM)
14.	Kolej Universiti Antarabangsa PICOMS
15.	Kolej Universiti Islam Pahang Sultan Ahmad Shah
16.	Keretapi Tanah Melayu Berhad (KTMB)
17.	Lembaga Hasil Dalam Negeri Malaysia
18.	Lembaga Pembangunan Pelaburan Malaysia
19.	Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)

20.	Malaysia Digital Economy Corporation (MDEC)
21.	Malaysian Investment Development Authority (MIDA)
22.	MIMOS Berhad
23.	Kementerian Pengangkutan Malaysia
24.	Malaysia Competition Commission (MyCC)
25.	National Cyber Security Agency
26.	Pejabat SUK Terengganu
27.	Pejabat Daerah Dan Tanah Melaka Tengah
28.	Pejabat Setiausaha Kerajaan Negeri Perlis
29.	Pejabat Tanah dan Galian Melaka
30.	Perpustakaan Negara Malaysia
31.	Polis Diraja Malaysia
32.	Prasarana Malaysia Berhad
33.	Sarawak Multimedia Authority
34.	Suruhanjaya Koperasi Malaysia
35.	Suruhanjaya Pencegahan Rasuah Malaysia (SPRM)
36.	Suruhanjaya Perkhidmatan Pelajaran
37.	Suruhanjaya Pilihan Raya
38.	Unit Hasil Jabatan Kewangan Negeri Melaka
39.	Universiti Kebangsaan Malaysia
40.	Universiti Malaya
41.	Universiti Pertahanan Nasional Malaysia

42.	Universiti Sains Islam Malaysia (USIM)
43.	Universiti Tun Hussein Onn Malaysia (UTHM)

Table 6. FGD – List of ministries and government agencies

5.3.2. Private Organisations

#	Name of the company
1.	Affin Bank Berhad
2.	Affin Hwang Asset Management
3.	Alliance Bank Malaysia Berhad
4.	Ambank group
5.	Asia E-University
6.	Asia Pacific University of Technology & Innovation (APU)
7.	Association of Banks in Malaysia (ABM)
8.	Augmented Technology Sdn Bhd
9.	Bangkok Bank Berhad
10.	Bank of China (Malaysia) Berhad
11.	Cardcom
12.	Celcom Axiata Berhad
13.	CGS-CIMB Securities Sdn Bhd
14.	Cloudaron Group Berhad
15.	Credit Bureau Malaysia
16.	Curtin University Malaysia
17.	Digi Telecommunications Sdn Bhd

18.	FAOM-Fintech Association of Malaysia
19.	HELP University
20.	Hong Leong Bank Berhad
21.	ICBC Malaysia
22.	India International Bank (Malaysia) Bhd
23.	Industrial and Commercial Bank of China (Malaysia) Bhd
24.	IRIS Corporation Bhd
25.	Jumio Corp.
26.	Kelantan ICT Gateway Sdn Bhd
27.	Kolej Universiti Islam Antarabangsa Selangor
28.	Malayan Banking Berhad
29.	Malaysia Rail Link Sdn Bhd
30.	Maxis Broadband Sdn Bhd
31.	Mizuho Bank Malaysia
32.	MUFG Bank (Malaysia) Bhd
33.	OCBC Bank (M) Bhd
34.	Pos Digicert Sdn Bhd
35.	Prince Court Medical Centre
36.	Public Bank Bhd
37.	Public Mutual Bhd
38.	Raffcomm Technologies Sdn Bhd
39.	Smart Selangor Delivery Unit
40.	Standard Chartered Bank Malaysia Bhd

41.	Taylor's University
42.	U Mobile Sdn Bhd
43.	UCSI University
44.	United Overseas Bank (Malaysia) Bhd
45.	Universiti Tunku Abdul Rahman (UTAR)
46.	Universiti Teknologi Petronas (UTP)

Table 7. List of private organisations

Figure 2. Other areas of concern using NDID

1. Please specify other Digital ID functions/ services that would benefit your ministry / agency / company with the implementation of the NDID programme



- [illegible]

Figure 5. Why NDID should not be adopted in organization

5. Please explain why you do not foresee National Digital ID minimising the overall cost for identity verification processes.

➤ “Not necessarily as there could be certain industries that may need to have new hardware and/or software (including possibly maintenance) to integrate into the new framework unless the full deployment cost is borne or heavily subsidized by the government. Hence, as proposed earlier, in developing the national NDID solution, the mobile phone would be an option to seriously consider as a ‘medium’ or enabler which should effectively somewhat reduce industry impact if there is sufficient collaboration and interoperability between systems, businesses, individuals and with the national platform. As such, NDID user interfaces (UI/UX) should be designed at the onset to be mobile device centric, including the use of apps for smartphones and non-apps for feature phones. In addition, to promote public adoption as well as private sector take-up (e.g. as part of their digitization efforts) of the NDID, it is essential that all elements be kept minimal and NDID operating model should follow a cost-recovery model.”

6. What are the potential regulatory/ legal changes that are required within your ministry / agency / company to facilitate the adoption of NDID?

➤ Possibly PDPA, depending on the security of the system. There will probably be needed to review how the user data is provided and what we should store in future.

➤ Risk evaluation, legal T&C around privacy of data and customer consent, security of connectivity

➤ Legal validation for new work processes

➤ Legal age for online onboarding (e-KYC)

➤ Digital Signature Act

➤ Potential changes with regards to customer privacy and data protection law.

➤ A clear guideline from BNM would be required on the adoption of NDID to establish banking relationship with the Bank.

➤ Understanding the security measured framework in place

➤ Statutory requirements for processes under the National Land Code, the National Land Code (Penang and Malacca Titles) Act

➤ Proper controls, governance and regulations need to be put in place to prevent potential misuse and possible risks elements, for example misuse due to insufficient proper controls akin to dual-use technologies such as social media, GPS; risks already present in digital technologies with large-scale population-level usage such as system failures, cybersecurity, breaches and privacy violations; exposures due to risks found in conventional national ID programs. It is vital that the NDID framework includes principles that enable user-control, privacy, transparency and security based on (or through reformed) current laws and regulations. Another aspect to consider (though not really in relation to regulatory) is technical standards to enable smooth portability and be future-proof as proprietary standards may lead to complexities and vendor lock-in. Celcom would like to humbly request that a working group (both technical and regulatory) be set up for the formulation of the NDID framework so that industry feedback can be considered and incorporated where possible, which will the end of the day benefit all parties.

➤ Regulatory - Customer's written consent has to be obtained in line with s.133/s.145 of FSA/IFSA for banking secrecy requirements.

➤ Legal - Need clarity and details over the scope of application. For example, whether and how this applies to the signing, authentication and filing of powers of attorney and instruments of dealings for land and properties, etc. How and by who will the documents be retained and who are the parties to sign section 90A Evidence Act certificate when adducing evidence in court, etc.

www.pwc.com

PricewaterhouseCoopers ("PwC") has prepared this report for Malaysian Communications and Multimedia Commission ("MCMC"), as part of the deliverables in accordance with the provisioning of consultancy services on the National Digital Identity (ID) Framework for Malaysia. We do not accept or assume any liability or duty of care for any other purpose or to any other person to whom this document is shown or into whose hands it may come save where expressly agreed by our prior consent in writing.

This document contains information obtained or derived from a variety of sources, as indicated within the document. PwC has not sought to establish the reliability of those sources or verified the information so provided. Accordingly, no representation or warranty of any kind (whether express or implied) is given by PwC to any person (except to our client under the relevant terms of Contract) as to the accuracy or completeness of the document.

© 2020 PricewaterhouseCoopers Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Limited, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.