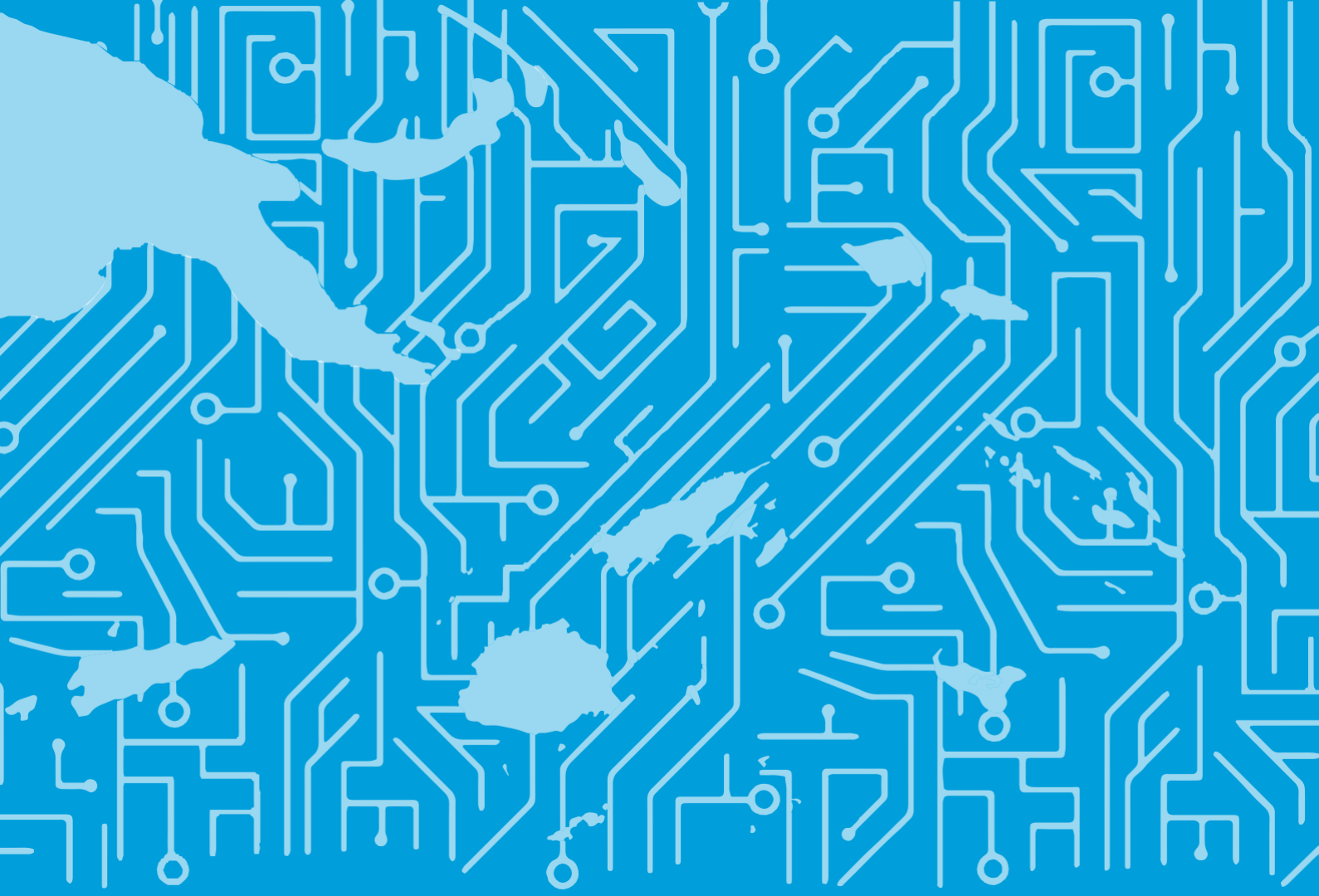
AN INCLUSIVE DIGITAL IDENTITY PLATFORM IN VANUATU

Country diagnostic
January 2021



This publication is brought to you by the Pacific Digital Economy Programme which is jointly administered by the United Nations Capital Development Fund (UNCDF), United Nations Development Programme (UNDP) and United Nations Conference on Trade and Development (UNCTAD). The programme receives funding from the Australian Government.

This research was conducted and written by the Centre for Financial Regulation and Inclusion's (Cenfri) Barry Cooper, Antonia Esser, Fabrice Gatwabuyege, Kinyanjui Mungai, Vera Neugebauer, Laura Muñoz Perez, Roland Banya, with contributions from Ajay Jaganath, Financial Inclusion Specialist and Bram Peters, Regional Digital Lead at UNCDF in the Pacific.

For this piece, UNCDF and the authors would like to thank all stakeholders across the public and private sectors in Vanuatu who took part in qualitative interviews for their contributions to this assessment.

January 2021

UNITED NATIONS
UNCTAD

UNDP

UNCDF
Unlocking Public and Private Finance for the Poor

Contents

List of tables

List of figures

List of boxes

Acronyms

2G	Second generation
3G	Third generation
4G	Fourth generation
ADB	Asian Development Bank
AML-CFT	Anti-money laundering and combatting the financing of terrorism
ASPI	Australian strategic policy institute
BVN	Bank verification number
CB	Central bank
CDD	Customer due diligence
CDR	Consumer data right
DFS	Digital financial services
ETA	Electronic transactions act 2000
ESCAP	Economic and social commission for Asia and Pacific
EU	European Union
e-commerce	Electronic commerce
e-government	Electronic government
e-money	Electronic money
FATCA	Foreign account tax compliance act
FATF	Financial action task force
FIU	Financial intelligence unit
FSP	Financial service provider
FW	Framework
G2P	Government to person
GDP	Gross domestic product
GDPR	General data protection regulation
GSM	Global system for mobile communication
GSMA	Global system for mobile communication association
ID	Identity document
IT	Information technology
KYC	Know-your-customer
MNO	Mobile network operator
MTO	Money transfer operator
NFC	Near-field communication
NGO	Non-governmental organisation
NSS	National security strategy
NZ	New Zealand
PEP	Politically exposed persons
PIFP	Pacific Islands financial inclusion programme
PPP	Public-private partnership
QR	Quick response
RBA	Risk-based approach
RBV	Reserve Bank of Vanuatu
SDGs	Sustainable Development Goals
SIM	Subscriber Identity Module
UNICEF	United Nations Children's Fund
USSD	Unstructured supplementary service data
VEO	Vanuatu electoral office
VNPF	Vanuatu national provident fund

Executive summary

An inclusive digital identity platform that meets the economic and social needs of the population while adding efficiency and safety to government and the private sector is a powerful tool to achieve large-scale inclusion. The following considerations would be useful to take into account during a design process:

		Systemically important, centralised digital ID platform	
Competitive advantage over existing ID databases	Remote, robust and secure verification of an individual's identity	Real-time identity information updates through centralised ledger	Third-party identity verification access, supported by ID proxies
For transaction scale and to meet national priorities (use cases)	Close the foundational ID gap; integrate all existing ID databases	Integrate e-commerce and G2P payments, MTO CDD and e-money/financial account opening	SIM registration crucial to enable digital service expansion
To implement widely accessible ID proxies	Biometric photos are quality-checked; voice templates are added	FIU guidance on remote verification is issued	SIMs are registered and verified phone numbers are linked
To provide the appropriate safeguards	Establish robust data privacy, protection and cybersecurity law	Targeted awareness campaigns	Clear governance and participation rules of platform
To ease access for individuals	Bislama, English and French-enabled services; voice access crucial for illiterates	USSD/voice channel access on top of 4G connections	Enable wide range of ID proxies
To ensure solid governance, inclusivity and financial sustainability	Regional integration crucial, otherwise risk of abandonment	Set up and integration costs supported by NGOs/development partners	Contractually bind stakeholders to contribute based on cost savings

Current identity landscape

- A digital ID platform can offer a future-proof template for the onboarding of the approximately 20% of people in Vanuatu who currently do not have access to an ID. However, it may be too costly to onboard hard-to-reach individuals who could be added over time, if and when they would need (digital) identity services. Narrowing this gap will be crucial to enable higher transaction scale and ensure inclusivity.
- The national ID database lends itself to be integrated with a digital ID platform first but approximately 40% of the population are not yet included in that database. In order to close this gap, information from other identity databases could be utilised and digital ID utility could serve as a portal to upload and verify/create unique/robust identities across the excluded population. All five current identity databases (birth registry, national ID database, passport, driving licence and provident fund registry) have considerable overlap in the information they collect and store.
- A digital ID platform could solve issues with inconsistencies in the details of a person stored in the different identity databases by serving as a central utility that consolidates identity data from different identity sources into one single robust identity per individual.
- A digital ID platform would address the challenge of third-party verification of identity information, which currently entails high costs of compliance and the need for face-to-face interactions, especially in the financial sector. If no third-party verification is enabled, it could undermine the value-add of a digital ID platform.
- National ID already includes a proxy ID in the form of a QR code. Facial biometrics show great potential as ID proxies as they are widely collected by identity providers in Vanuatu. However the quality of the captured biometric information would need to go through quality control to ensure robustness. Mobile numbers can also be a powerful proxy given their prevalence, but a robust SIM registration process would need to be implemented to enable phone numbers as an ID proxy.
- A combination of SIM and voice biometrics, when compared to SIM plus fingerprint and/or facial recognition, would likely be universally accessible on the MNO networks in Vanuatu due to the pervasiveness of basic/feature phones in the country when compared to smartphones.

Current digital ecosystem

- Mobile phones present the obvious instrument to reach the majority of individuals with a digital ID platform. The digital ID platform should accommodate voice and USSD access on top of 2G channels given that 74% of people in Vanuatu currently do not access the internet via any device and feature/basic handsets dominate over smartphones.
- Large gaps in electricity coverage, particularly in rural and remote areas could impact quality to run and usage of platform.
- Use of mobile digital services nascent and fragile with low current uptake, limiting their ability to drive considerable uptake of the digital ID platform.
- Bislama, English and French should ideally be accommodated in a digital ID interface to allow usage by majority of country's population. To include those comfortable in other languages, as well as the 12% of the population who are illiterate, a voice service could be embedded into the digital ID platform.
- As mobile internet and social media use is limited, trust still needs to be established for the majority of the population. Fit-for-purpose awareness and usage campaigns around digital services and digital ID use would have to be factored into the set up costs to drive uptake.
- Mobile money is used very little by the people of Vanuatu. More use cases around its usage would need to be created to promote usage and population would need to be educated and trained on how to utilise online services.
- Legislation governing data privacy is in place in the telecommunications sector which could provide a framework for developing national broad-based consumer data privacy legislation.
- A new Cybercrime Act is under consideration and expected to address threats including misuse of identity and data. Data protection frameworks are important to build security and trust in the digital identity system.
- There is a need for a robust national cybersecurity framework to be developed. A draft Cybercrime Act is under consideration that outlines actions against computer related offences such as unlawful access to computer systems and communications networks. If adopted, this would represent a positive step in safeguarding against cybersecurity risks.
- Vanuatu's AML-CFT regulation lacks clarity on what constitutes a "document" for CDD purposes and there is therefore a need for the FIU to issue sufficient guidance in this regard in order to judge the applicability of the digital ID solution to fulfil this function.

Use cases

- While there is a significant number of use cases that could benefit from a digital ID utility in Vanuatu, the likely monthly transactions that could be generated by most of these use cases may not make it financially viable to integrate a large share of them. Regional integration will be key.
- Given the size and different owners of the current databases, once-off integration and consolidation of existing information will require considerable effort before revenue can be generated, but is absolutely crucial to bring inclusivity, efficiency and longer-term cost savings to the market.
- Financial transactions (e-commerce payments, G2P payments, MTO CDD and e-money/financial account opening) are expected to contribute the largest share of transactions now and in future and are also a national priority. Including financial stakeholder will therefore be important.
- In terms of national priority, closing the foundational identity gap will be vital in narrowing the digital divide and in developing an inclusive economy. The platform can give the template for onboarding and it will be crucial to bring more people into the formal system to generate scale and improve inclusion.
- Utilising the digital platform for SIM registration would have several benefits, ranging from streamlined e-money account opening to enabling ID proxies. This use case should ideally be integrated to bring value to a range of stakeholders as well as aiding in meeting national objectives.
- Several systems for electronic service delivery already exist, especially across civil use cases such as school enrolment, driving licence renewal and birth, death and marriage registrations, but to a varying degree of efficiency. This puts these existing services at a lower priority for integration with the platform from a stakeholder perspective and it will require significant efforts to get stakeholder buy-in in that space.

Governance/finance considerations

- The facility needs to be regionally integrated as Vanuatu on its own is unlikely to create enough scale in a digital ID platform. The more Pacific Islands are integrated, the higher the chance of financial viability. But regional integration requires strong, harmonised regulatory frameworks, which increases the range of stakeholders that have to be accommodated.
- The platform should ideally serve as a cross-cutting utility to drive scale and achieve national policy objectives and hence both private sector and public entities (in addition to the Reserve Bank) should be involved in design and governance. The aim is to create systemically important infrastructure.
- Private sector entities signal interest in the utility but there are no clear signs that an entirely privately operated utility is preferred by any stakeholder.
- A government-led, private sector-owned and operated approach could be suitable for the region if collaboration and buy-in can be ensured and if the initial funding for the set up can be secured.
- NGOs and development partners are well-placed to assist with the set up costs if the utility is aimed at inclusivity instead of profit maximisation. For the continuous financing of operational costs, however, stakeholders should be contractually bound to contribute to costs based on their respective efficiency cost savings, in addition to viable transaction fees and system integration costs. The aim of an NGO-led financial model would be to sustainably balance revenue and utility.
- The utility could eventually also enable a real-time retail payments switch that can route transactions with high accuracy, which could contribute to the operational costs and overall systemic utility.

1. Introduction

Diagnostic assesses the readiness of Vanuatu for a digital identity platform. This country diagnostic report was commissioned by the United Nations Capital Development Fund (UNCDF) under the Pacific Financial Inclusion Programme (PFIP) and Reserve Bank of Vanuatu (RBV) to understand and assess the use cases and ecosystem requirements for a digital identity (ID) platform in Vanuatu. This platform solution can be understood as a central repository which houses an individual's unique personal data (biographic[1] and biometric[2]) in digital form (World Bank, 2016; World Bank, 2018). The digital ID platform can thus be used to assert and prove an individual's identity as discussed in Box 1 below (FATF, 2020). The ultimate objective of this diagnostic is to recommend if and how the implementation of an inclusive and sustainable digital ID platform solution, tailored to the Vanuatu market, can lead to higher inclusion levels through bringing value to consumers, industry and government.

Digital identity platforms enable a range of services in the digital age and therefore at the centre of a modern, digital economy. A digital ID can serve as a digitalisation catalyst by forming the basis to enable growth in secure online platforms which can be used to participate in economic activity. The implementation of digital ID solutions in emerging economies is stated to have the potential to help unlock economic value of around 6% of GDP by 2030 (McKinsey Global Institute, 2019). Utilising such a solution can boost inclusion by allowing for the identification of individuals reliably and remotely, facilitating access to a variety of digital services across civil society, health, education, employment and finance. Digital ID solutions have, for example, enabled governments across the world to identify vulnerable populations to provide fiscal support packages during the recent COVID-19 pandemic[3], making digital ID solutions an increasingly necessary part of any economy.

Digital identity platforms enable continuous identity proofing as well as digital identity proxies, which are especially useful for countries with hard-to-reach populations. A digital ID platform can be beneficial in two additional ways. Firstly, it enables continuous identity proofing, i.e. it can be utilised to verify a person's identity on an ongoing basis, rather than once off, to create more robust identity profiles especially for individuals without identity documents (Cooper et al, 2020). A digital ID platform can also facilitate the creation of ID proxy identifiers (or ID proxies). Different types of ID proxies (such as phone numbers, biometrics, or email addresses)

Box 1: Overview of a digital identity platform

A digital identity platform offers a simpler and more secure means to establish and verify an individual's identity. The digital identity platform works by:

1. Capturing data. Identity data tied to an individual is captured/integrated on a centralised database or ledger. Depending on the model of the platform, multiple existing databases that are used to produce physical identifiers, such as passport, ID cards, driving licences etc. are formatted and integrated via a digital ID using a common data standard or format. Those individuals currently not covered by identity databases or those that need to add additional identifiers such as biometrics (e.g. a photograph, fingerprints, iris scans or voice prints) can be newly onboarded directly onto the platform. Their identity data can be captured via different channels, including in-person enrolment stations or remote mobile channels (utilising smart phone technology such as fingerprint scanners and via photographs). India's Aadhaar system, for example, has a flexible evidence requirement in which it collects both fingerprints and/or a variety of basic identity documents predominantly through in-person enrolment stations.

2. Verifying data. After collecting data the identity platform processes the data and verifies the data's authenticity. This happens through a deduplication process that matches, verifies and consolidates conflicting or duplicated information available for an individual, to create one unique and robust identity file per person that contains identifiers by which an individual can be identified digitally. Telefónica Deutschland in Germany, for example, uses a digital identity platform solution offered by Thales which verifies data using facial matching via liveness detection.

3. Digitalisation. The verified data is digitalised and stored digitally either directly on a centralised database or the digital ID platform acts as an integration layer that creates interoperability between existing databases. In case an individual needs to prove their identity or a service provider is required to verify a customer's identity, they can send a digital verification request to the digital ID database via a digital interface and get confirmation (yes, the person is who they say they are) and/or the list of identity details on the individual in real time.

1 Biographic data includes information such as an individual's name, age, gender and residential address.

2 Biometric data includes information such as an individual's fingerprints, scan of their iris and voice prints.

3 For instance, in Chile digital IDs were used to rapidly pre-enrol new beneficiaries into social programmes, while in Thailand the government was able to use its digital ID platform to identify eligible beneficiaries of its social assistance programmes and use it to facilitate direct deposit payments into bank accounts (Pangestu, 2020).

can be linked and utilised to create a unique identity for individuals without any form of identification, as well as be used to enhance the robustness of identities for those that already have a physical form of ID. This therefore gives individuals a convenient and verifiable form of identification that can be used in the place of paper-based documents to access services digitally as well as in person. The concepts of ID proxies and identity proofing are discussed in more detail in Box 2 below.

The ability to access digital services and create or verify an individuals' identity over time make digital ID platforms particularly useful for financial inclusion. In Vanuatu, 63% of adults (those aged 15 years and above) do not have access to formal financial services (Reserve Bank of Vanuatu, 2016). Fifteen percent (15%) of the unbacked adult population cite a lack of documents as a reason for not having a formal bank account (Reserve Bank of Vanuatu, 2016). In addition, the usage of digital financial services (DFS) remains very low, with less than 3% of adults using a mobile money product to send and receive money (Reserve Bank of Vanuatu, 2016). According to the Financial Action Task Force (FATF)[4], digital ID platforms can help promote financial inclusion by providing individuals without traditional paper-based forms of identification with a unique and legal ID to access formal financial services (FATF, 2020). This digital ID would however need to be legally recognised and accepted by financial regulators for know-your-customer (KYC) purposes in order for it to be used to gain access to formal financial services. A digital ID solution can also have cost saving benefits for providers by reducing their cost of compliance. The removal of requirements for paper-based documents at onboarding and use of digital technologies can help institutions reduce their cost of compliance costs with AML-CFT obligations by as much as 39%. It would also result in frontline staff spending 60% less time on onboarding and ongoing due diligence processes as well as lead to cost savings of 50% with respect to the record-keeping of documents and the storage costs thereof (Thom et al, 2020). This can in turn free up staff capacity and budgets for providers to focus on reaching more financially excluded population segments.

Different types of digital ID platform models can be employed. The choice of the model for a digital ID platform depends on country-specific factors such as its digital infrastructure capabilities as well as how the platform will be governed. Box 3 provides an overview of the different governance models that are prevalent in the digital identity space presently.

The feasibility and sustainability of a digital identity platform depends on the use cases, regulatory environment, country context, stakeholder buy-in and choice of technology. For a digital ID platform to be sustainable and feasible, the following should be taken into consideration:

- The combination of **different use cases** to drive scale as each use case can have different usage patterns which can influence the design and sustainability of the digital ID platform. Scale is important from a financial standpoint as typically higher transaction scale leads to lower transaction costs. Furthermore, use cases aligned with the achievement of national and/or policy objectives, or sustainable development goals (SDGs) are particularly powerful for macro developmental impact. Therefore, use cases need to be assessed taking both perspectives into account, especially given the smaller population size in Vanuatu.
- The **governance scheme** of the platform affects the future sustainability of the platform. The optimal governance scheme is dependent on the use cases.
- A **comprehensive legal framework** underpinned by policies, laws and regulations that govern how data is managed and to mitigate abuse via sound data privacy and cybersecurity. These factors are important as a digital ID platform entails the collection and storage of large amounts of personal data and it is therefore essential that safeguards are in place to ensure data and its owners are protected. This in turn can help build trust and promote usage of the platform.
- Design of the platform should take into consideration the **digital ecosystem** of the country and **local demand-side factors**. A country's digital infrastructure can impact the system design and operations of a digital ID platform as well as the scale of transactions going through the platform. It is also important to understand the extent to which a population is familiar and ready for digital technologies as it will determine the value they derive from a digital ID platform, its usage and ultimately viability. Overall, the utility should provide value for actors across the public and private sectors by helping them address challenges in the provision of services to individuals. This will be essential in determining the platform's use cases, its usage patterns and financial feasibility.
- The choice of **platform technology** should be tailored to the specific usage cases identified in the country by various stakeholders as well as the ecosystem in which it operates by taking into consideration the state of a country's digital infrastructure and unique characteristic of its population. This will ensure it is designed in a way that brings sufficient value for both providers and consumers in the most cost-efficient manner.

4 The Financial Action Task Force is an intergovernmental organisation that sets international standards on anti-money laundering and combatting the financing of terrorism. See more at: https://www.fatf-gafi.org/.

Box 2: Overview of identity proxies and continuous identity proofing

This box provides an overview of the two main additional benefits of a digital identity platform for a modern, digitised economy: ID proxies and continuous identity proofing.

ID proxies

An ID proxy is a form of agreed-upon identifier which can be used as an alternative to paper-based documents to assert the identity of a person (Cooper et al, 2019). As explained in Box 1, the biographic and biometric data of a person that is stored on a digital ID platform can be used to create different kinds of shorthand for identity information – ID proxies. Today ID proxies globally are mostly used in the financial sector to make retail and person-to-person payments. The use of ID proxies eliminates the need for paper-based documents and opens the door for individuals to use identifiers they are familiar with to conduct transactions and access services digitally and remotely.

This can be especially useful in regions such as the Pacific Islands where populations can be scattered across many islands and where the logistics of travelling to different islands to access services can be burdensome and costly

Apart from identity document numbers such as passport number, social security number etc., the most common types of ID proxies (Cooper et al, 2019) are:

Biometrics. A biometric information ID proxy links information based on an individual's physical attributes (fingerprints, iris, voice, facial features) to an identity file or proxy number to verify that individual's identity. Typically, an individual will need to go to an in-person enrolment centre for registration and onboarding. Nigeria's Bank Verification Number (BVN) system, for example, captures all fingerprints, signature and facial recognition which allows for customers to open accounts at financial institutions using their biometric identity. The individual simply scans their fingerprints, iris, shares a photo or provides voice samples to conduct a transaction online or in person.

Phone number. A mobile number ID proxy uses an individual's phone number as an identifier. In some jurisdictions the mobile number and mobile money account number are the same, creating convenience for customers to transact with each other or businesses. To use one's mobile number to initiate payments or utilise other account instructions an individual must register their mobile number with the financial institution and link it to their account. The use of a mobile number as an ID proxy is increasingly common, for example, MTN's Mobile Money (MoMo).

QR code. A Quick Response (QR) code is a two-dimensional, scannable, tokenised image proxy. An individual will be provided with a unique QR code containing their identity information by their bank, online platform, or mobile wallet provider. The code is usually generated via the platform's mobile application which can then be used to make payments. This code is readable with an imaging device such as a point of interaction (POI) device, webcam, or smartphone camera. Mexico's Cobro Directo (CoDi) payment platform generates QR codes to send generated request-to-pay (RTP) via a mobile app or through a web browser.

NFC. Near-field communication (NFC) technology is a wireless technology which allows for a device to collect data from a nearby device or tag that contains an NFC chip. For an NFC payment to be conducted, a physical NFC tag on a mobile phone or an NFC chip integrated in a phone is used to transfer payment instructions from the individual's account or mobile. MTN's MoMoPay, for example, provides its customers in select countries with an NFC tag which is linked to a mobile money wallet. Once a payment is initiated through close contact of the NFC tag and the MTN point of interaction, the payment is validated via a customer's personal pin before it is processed.

Email. An email ID proxy uses a person's email address as the main identifier instead of using the individual's bank account or electronic wallet number. To use an email address as an ID proxy, an individual links it with a financial institution, government agency and/or an online platform that facilitates payments. For example, to transfer money using Google's GPay, an individual needs to link their email address to their debit or credit card and then enter the email address when initiating a transaction. PayPal is also a widely adopted service, using email addresses as proxies.

Often ID proxies are combined or layered to create what is referred to as a "proxy ID stack", for example the India Stack. This stack can serve to strengthen the proxy registration system (Cooper et al, 2019). When considering which ID proxy or combination of ID proxies to adopt it is important to weigh up their benefits and shortcomings regarding accessibility, verifiability and trustworthiness (uniqueness, privacy and customer experience).

Continuous identity proofing

Digital identity proofing systems can increase the robustness of identity information over time as new information gets added to a user. The digital ID system constantly conducts the identification and verification process throughout the lifecycle of an account, which in practice means that it continually adds new information to the ID profile. The platform allows for different information to be collected and consolidated over time. A significant benefit of this process is that it enables and strengthens an identity for individuals who do not have foundational identity documentation. For example, if an individual is not able to provide a foundational ID

(continued on next page)

document, they can start by getting access to limited services to limit the risk to the payment system. As the person uses the service, the institution can collect behaviour patterns and new information to establish a more robust risk profile. The data would be monitored, updated and verified, which means that the ID file itself gets stronger and more robust (Cooper et al., 2020). Eventually this identity would be strong enough to qualify the individual for accounts with less restrictions, as the level of assurance would have increased since the establishment of the original identity, despite the lack of a foundational ID document.

Box 3: Overview of digital identity governance models

Government-led, owned and operated. Here a single or group of public sector entities take responsibility for ownership and implementation of the platform and how it is governed. Under this model, a government-issued digital ID is provided to individuals. Examples of this approach are Estonia's state-issued digital identity and the Aadhaar identity platform.

Private sector-led, owned and operated. Under this model, private sector firms such as banks or mobile network operators (MNOs) take the lead on implementing the digital ID platform and are responsible for its governance. Under this approach, these private sector entities serve as the issuers of a government-recognised digital ID by utilising a foundational ID system as their source of identity (GSMA & World Bank, 2016). Examples of this approach include Singapore's MyInfo and Sweden's Bank ID.

Government-led, private sector-owned and operated. This approach involves the government taking the lead when it comes to the design requirements and operating parameters of the digital ID platform, while the private sector takes responsibility for the implementation and operation of the desired platform. Examples of this include Nigeria's electronic ID card, which is embedded with MasterCard's technology, Nigeria's BVN and Australia's PayID.

NGO-led and government or private sector-owned and implemented. Under this model, individuals have control of how their personal data is housed or linked through the digital ID platform and how it is shared and used, while government and/or the private sector take responsibility for the issuing of the identity credentials. An NGO or trust would be the holder of the facility and have a privacy mandate distinct from commercial entities that link to the facility or provide value-added services. An example of this approach would be a self-sovereign identity and BunkerID.

This diagnostic is divided into six chapters. Given the above, it is essential to the success of a digital identity platform's roll-out that it be informed by a holistic diagnostic study undertaken prior to implementation. This study is therefore divided into the following sections:

- Section 2 provides an overview of the current state of identity coverage in Vanuatu, the quality of existing identity databases in the country and challenges experienced in the use of these databases that a digital ID platform could help solve.
- Section 3 assesses the state of the digital infrastructure in Vanuatu, the regulatory environment as well as consumer considerations that can influence the implementation of a digital ID platform.
- Section 4 provides a scope of the use cases for a digital ID platform in the country.
- Section 5 looks at the potential governance and financial models of a digital ID platform.
- Section 6 concludes and provides recommendations.

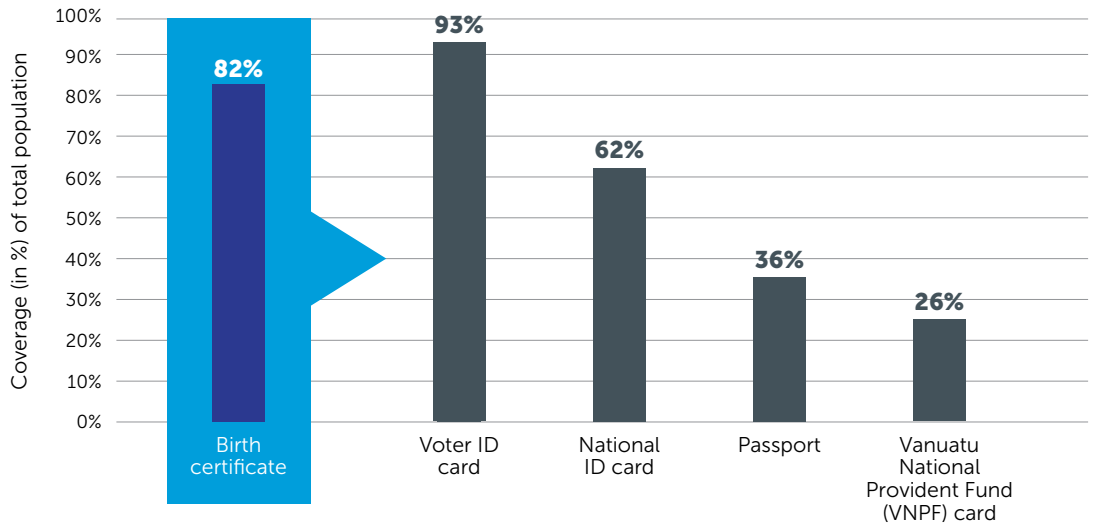
2. Current ID systems in Vanuatu

This section provides an overview of the current state of identity coverage in Vanuatu, the quality of existing identity databases in the country and challenges in the use of these databases that a digital ID platform could help solve. It is important to understand the identity ecosystem, as the extent of the benefits and the design of a digital ID platform is influenced by the prevalence, format and quality of information housed in identity databases in the economy.

Close to 20% of people in Vanuatu lack access to a birth certificate, which forms the basis for five additional legal identity documents. The birth registry is the main foundational identity[5] in Vanuatu and covers 82% of the population (around 254,000 people) as shown in Figure 1 below (UNICEF, 2017). With a birth certificate, people in Vanuatu can then access five additional, legally recognised, identities[6], namely a voter ID card, a national ID card, a Vanuatu National Provident Fund (VNPF) card, a driving licence and a passport. All six identity documents, either in combination or individually depending on the use case, are typically accepted forms of identification to access most services in the country. This means that legally 18% of Vanuatu's population is currently excluded from such services and will also struggle to access any of the additional five identities[7]. To prevent a growing digital divide in the access to services for the excluded population, this gap needs to be narrowed as much as possible. A legally recognised digital ID platform can offer a future-proof template for the onboarding of people without an official ID document and/or will be able to create a robust identity over time, as outlined in Box 2. This identity can then be used to access core services such as healthcare, education and formal financial accounts.

The required effort to close the foundational identity coverage gap depends on the location of the excluded individuals. Approximately 25% of the population of Vanuatu lives in the cities of Port Villa (the capital) and Luganville (the second largest city in the country) (ASPI, 2020). This means that a large majority of the population is scattered across the country's four major islands and more than 80 smaller islands (ASPI, 2020). The distance between the islands can be large, with the distance between north to southern outermost islands being around 1,300 kilometres (UNDP, 2015). It is therefore important to determine how many individuals without a birth certificate are scattered across the islands, as the effort to onboard them onto the platform could be high. The enrolment of new users on the system can be phased and opportunistic, i.e. combined with census or other data collection initiatives. For the financial viability of a digital ID platform it is desirable to onboard as many people as possible to create transaction scale, yet the costs of onboarding need to be weighed against the needs of the population: an individual who is leading a remote and self-sufficient life may not have a great need for a digital identity as a priority.

Figure 1. Current coverage of ID documents in Vanuatu



Sources: Election guide (2020), Daily Post (2019), UNICEF (2017), UNCDF (2020), VNPF (2019)

5 A foundational identity is a general-purpose form of identity credentials provided to the population of a country that can be used to access a wide variety of public and private sector transactions, services and platforms. Examples of this include national IDs and civil registries (GSMA 2019; World Bank, 2018).

6 A legally recognised identity is referenced in regulation.

7 Stakeholder interviews revealed that in the case where a person cannot provide a voter ID card or any of the other ID types, an identity can be established through a trusted witness or figure of authority who needs to sign a letter confirming a person's identity. While this is good practice to enable more Ni-Vanuatu to access services on an ad-hoc basis, it presents a barrier in accessing digital services.

Opportunity for digital ID platform to expand on more robust national ID database. As Figure 1 shows, 93% of adults in Vanuatu have a voter card compared to 82% of the population that has access to a birth certificate (Election guide, 2020; UNICEF, 2017). The higher number of people that have a voter card compared to a birth certificate should technically not be possible as a birth certificate is required to attain a voter card. This indicates issues with duplication in the voter system. The Vanuatu National ID was created as a way to deal with this issue and dedupe the voter database and is also based on the information in the voter registry. The process of deduplication is currently ongoing and is predicted to be completed in 2021 (Stakeholder interviews, 2020). After finalisation, one robust national ID database is expected to be in place, which could be expanded via a digital ID platform by integrating the other forms of ID as well as onboarding new individuals.

Considerable overlap in collected information across databases could be solved by digital ID platform. Table 1 shows that all five databases collect name, date of birth and address of the individual, creating substantial overlap in information. This overlap translates into onboarding costs for the database host that could be reduced by creating a central repository of information in the form of a digital ID platform that every stakeholder with permission could draw on. In addition to this inefficiency, stakeholders raised three challenges that could be overcome with a digital ID platform:

- **Aftermath of natural disasters leads to duplication in voter databases.** Stakeholder interviews revealed that natural disasters have led to duplicates being generated in the voter ID database[8] (Stakeholder interviews, 2020). This is due to the fact that the voter ID database captures the residential address of an individual as outlined in Table 1. As a result of natural disasters, people move from one island to another where they re-register onto the voter ID database with a new address due to their voter ID cards being lost or damaged. Although the deduplication efforts on the voter system are still underway to create a robust national ID database as previously mentioned, stakeholder interviews revealed that there are still issues of duplicates in the national ID system (Stakeholder interviews, 2020). A digital ID platform could be utilised to register changes in the particulars of an individual in one central utility, allowing for the easy identification and removal of duplicates and enabling this information to be accessible to all connected entities on the platform in real time.
- **Inconsistency in details captured in different identity databases.** Stakeholder interviews revealed that there can be inconsistencies in the details of a person stored in the different identity databases in Vanuatu (for example, a person's name can be spelled differently in the birth registry and VNPF database) (Stakeholder interviews, 2020). As a result, it can be difficult to validate a person's identity when they try to get access to services such as opening a bank account. A digital ID platform would serve as a central utility that consolidates identity data from different identity sources into one single robust identity per individual, which can then be easily verified either in person or remotely.
- **Third-party verification capabilities lacking.** All current identity databases in Vanuatu lack third-party electronic verification capabilities when it comes to accessing services. This means that providers that rely on these forms of identity, such as financial service

Table 1. Vanuatu identity database details

	National ID	Voter ID card	VNPF card	Driving licence	Passport
Stored information (overlaps)	• Full name • Date of birth • Address				
Additional useful information	• Photo • Email address • Phone number		• Photo • Email address • Phone number	• Photo	• Photo • Phone number
Database owner	Department of Civil Registry and Vital Statistics	Vanuatu Electoral Office (VEO)* and Department of Civil Registry and Vital Statistics	Vanuatu National Provident Fund	Department of Customs and Inland Revenue	Department of Immigration and Passport Services

* National ID database access by VEO governed by memorandum of understanding.
Sources: Election guide (2020), Daily Post (2019), UNICEF (2016), UNCDF (2020), VNPF (2019)

8 Stakeholder interviews revealed that there could be as many as 20,000 duplicates in the database.

providers (FSPs), have no means of electronically verifying the authenticity of an identity document or its information. This incentivises providers to create their own customer databases against which the documents are checked. This requires face-to-face validation of credentials each time, incurring immense operational costs for providers as well as consumers. A digital ID platform could provide individuals with robust and easily verifiable credentials which could be accessed by third parties with permission to enable remote verification as well as authenticate information in face-to-face interactions.

National ID database could serve as starting point for digital ID platform integration due to stakeholder trust in it. The national ID database lends itself to being integrated with a digital ID platform first as stakeholder interviews suggest it is a trusted database (Stakeholder interviews, 2020). Given that approximately 62% of the population has been included so far, further onboarding would be required to grant equal access to the digital ID platform. This could be done by consolidating the information from the birth registry, VNPF, voter, driving licence and passport databases to fill in and/or verify gaps in the national ID system and using the digital ID platform as a portal to upload and verify or create unique, robust identities across the excluded population. This process would require collaboration between the Civil Registry Office of the Ministry of Internal Affairs, the Department of Civil Registry and Vital Statistics, the Vanuatu Electoral Office, the VNPF, the Department of Immigration and Passport Service and Department of Customs and Inland Revenue.

MNO database potentially powerful addition to existing registries. The rising number of mobile users in Vanuatu over the coming years (discussed in Chapter 3) means that MNO databases could also serve to create unique, robust identities when overlaid with existing information in identity databases as outlined in Box 4. This, however, can only be possible if the SIM database is linked to a robust identity to increase reliability and trust among stakeholders as KYC checks are currently not mandatory for SIM card purchases (GSMA, 2020).

Biometric information, email addresses and phone numbers likely to need initial verification process to increase robustness. In order for biometrics, email addresses and phone numbers to be integrated into the digital ID platform and used as potential ID proxies as outlined in Box 4 below, they would need to be verified to ensure their robustness. Stakeholder interviews revealed that the photo biometric templates stored in identity databases in Vanuatu suffer from quality issues which can render them not machine readable. In addition, given the lack of a SIM registration process, phone numbers and the identities they are linked to would have to be re-checked as explained in Box 4.

Summarised insights from current identity coverage in Vanuatu

1. A digital ID platform can offer a future-proof template for the onboarding of the 18% of people in Vanuatu who currently do not have access to an ID. This will be important from an inclusivity and scale point of view. However, it may be too costly to onboard hard-to-reach individuals who could be added over time, if and when they would need (digital) identity services.
2. The national ID database lends itself to be integrated with a digital ID platform first but approximately 40% of the population do not have a National ID card yet. To close this gap, information from other identity databases could be utilised and digital ID utility could serve as a portal to upload and verify or create unique, robust identities across the excluded population.
3. MNO databases could also serve to create unique, robust identities when overlaid with the existing information, once rigorous SIM registration regulation is finalised and implemented. A digital ID platform can provide this link, making MNOs key stakeholders to target with and involve in the design of a utility.
4. A digital ID platform could solve issues with inconsistencies in the details of a person stored in the different identity databases by serving as a central utility that consolidates identity data from different identity sources into one single robust identity per individual.
5. A digital ID platform would address the challenge of third-party verification of identity information, which currently entails high costs of compliance and the need for face-to-face interactions, especially in the financial sector. This need, if unaddressed, undermines the value-add a digital ID platform could provide.
6. National ID already includes a proxy ID in the form of a QR code. Facial biometrics show great potential as ID proxies as they are widely collected by identity providers in Vanuatu. However, the quality of the captured biometric information would need to go through quality control to ensure robustness. Mobile numbers can also be a powerful proxy given their prevalence, but a robust SIM registration process would need to be implemented to enable phone numbers as an ID proxy.
7. A combination of SIM and voice biometrics, when compared to SIM plus fingerprint and/or facial recognition, would likely be universally accessible on the MNO networks in Vanuatu due to the pervasiveness of basic and feature phones in the country when compared to smartphones.

Box 4: The potential of ID proxies in Vanuatu

Facial recognition and voice prints show most promise for biometric ID proxies; mobile numbers can create scale. Table 2 shows the different ID proxies that could currently be developed based on the existing identity databases in Vanuatu. The national ID card already includes an ID proxy in the form of a quick response (QR) code which is being utilised to gain access to a variety of services, such as in the financial sector (ASPI, 2020). Given the predominance of photographs, facial recognition seems to be the most promising in terms of reaching scale. However, facial recognition software and hardware can be expensive. Furthermore, stakeholders mention that not all photographs are currently stored in high enough definition to be uniquely identifiable. Given the increasing prevalence of mobile phones, linking identities to voice prints can allow a voice proxy to be created and used. This practice is gaining increasing traction globally as onboarding can be done remotely[9]. Other than biometric ID proxies, mobile numbers in Vanuatu can be a powerful proxy given their prevalence. However, SIM card registrations are not mandated in Vanuatu and therefore a robust SIM registration process would need to be implemented to enable phone numbers as an ID proxy[10] (GSMA, 2020). Email addresses in the country are currently not linked to financial services and would first need to be verified before serving as an ID proxy.

Combination of SIM and voice biometrics would have greater reach in Vanuatu. A high prevalence of basic or feature phones, as further discussed in Section 3.1, plus use of voice and USSD channels as a baseline can determine the kind of ID proxies that can become universally available in Vanuatu. While SIM plus fingerprint and/or facial recognition is more robust, a combination of SIM and voice biometric would likely be universally accessible on the MNO networks in Vanuatu due to high prevalence of basic and feature phones when compared to smartphones.

Continuous identity proofing, an open gateway to economic inclusion. Identity proofing is a risk-aligned digital process whereby those people that have limited or no foundational identity credentials on file are still able to engage in financial and civil services which are appropriate to their needs and in accordance with any risk posed by such consumers. This would be most appropriate for those within the 18% in Vanuatu with limited foundational ID credentials and particularly for those in more remote locales that would have difficulties in utilising their physical credentials on a digital platform. In time and with further database links or consumer interactions, a digital identity becomes more robust. The proofing process involves the accumulation of more identifiers and ID proxies, including SIM cards, phone numbers, email, location data, civil services interactions and biometric identifiers added or linked (photos, fingerprints, voice identification templates). Voice biometrics have been identified as more important in Vanuatu for identity proofing purposes. The process of identity proofing can also guard against potential identity theft or abuse through detection of changes in activity or patterns and links to other identities hence promoting quality assurance of the digital identity system overall.

Enabling payment channel and instrument interoperability. The digital ID platform could eventually be used to route payments to the appropriate channel to enable channel and instrument interoperability, i.e. serve as an electronic payments switch, which could be particularly useful for a smaller economy such as Vanuatu and its neighbours.

Table 2. Potential ID proxies

	National ID	Voter ID card	VNPF card	Driving licence	Passport
Potential ID proxies	ID in combination with: • Facial recognition *or* • Phone number *or* • Email address *or* • QR code *or* • Voice print	Voter ID number	VNPF number in combination with: • Facial recognition *or* • Phone number *or* • Email address *or* • Voice print	Driving licence in combination with: • Facial recognition	Passport number in combination with: • Facial recognition *or* • Phone number *or* • Voice print

Sources: Election guide (2020), Daily Post (2019), UNICEF (2016), UNCDF (2020), VNPF (2019)

9 Biometric considerations: A lack of good quality cameras may limit usability of facial recognition for remote verification of individuals. In the context of voice biometrics, the veracity of the voice identification software is another key factor that needs to be assessed.

10 Stakeholder interviews revealed that the telecommunications regulator is working on SIM registration regulation to make this compulsory.

3. Current ecosystem to establish a digital ID platform

A digital ID system works as well as the ecosystem in which it operates. The platform could be well designed from a technology standpoint but if the country context is not taken into account, it runs the risk of not adding sufficient value to both providers and consumers, leading to an underutilised facility. This chapter assesses the state of the digital infrastructure in Vanuatu, the regulatory environment and consumer considerations that can impact the usage patterns of a digital ID platform.

3.1. State of digital infrastructure

The digital infrastructure in a country underpins any digital service in the economy and at a minimum relates to the quality, penetration and affordability of mobile networks, as well as electricity. These elements not only directly impact the operations and set up of a digital ID platform but also affect the scale of transactions going through the platform, i.e. influence the financial viability of the facility.

Over half of the population has access to mobile phones currently; most widely adopted digital instrument. According to the Global System for Mobile Communication Association (GSMA), Vanuatu had 163,000 unique mobile subscribers[11] (representing 57% of the total population) in 2018 (GSMA, 2019). However, as established in Section 2, SIM registration is not mandatory in the country, meaning individuals can purchase a SIM card without going through any KYC checks. This makes it difficult to assess the true mobile phone coverage across the population and thus the share of individuals who connect to voice or data services could potentially be higher or lower than 57%. Regardless, the mobile phone is the most widely adopted digital instrument in Vanuatu through which a digital ID facility and its services could be accessed by individuals. The share of individuals accessing a mobile phone is predicted to increase to 64% by 2025 (GSMA, 2019). This still leaves 36% of the population excluded, impacting inclusivity and financial viability of the platform.

Data-only digital ID platform unfeasible, voice and USSD channels more appropriate. With limited and largely unaffordable fixed line connectivity in the Pacific region, mobile technology (complemented by satellite) is the only realistic solution to connect to the internet. According to World Bank data, 26% of Vanuatu's population had access to the internet in 2019[12] (World Bank, n.d). Mobile phones are the most used device when it comes to accessing the internet, making up 60% of web traffic by device in December 2019, compared to 36% for laptops and desktops and 4% for tablet computers (DataReportal, 2020). Of those using mobile data services, the majority is covered by 2G (56%), compared to 3G (27%) and 4G (17%). Access to high-speed mobile internet is expected to grow over the coming years, to 38% (3G) and 54% (4G) of total connections by 2025 (GSMA, 2019). Despite this growth, a 3G or 4G only digital ID solution would still leave a significant number of people unconnected and therefore a design embedding voice and USSD channels should be prioritised first. In addition, challenges to data service connectivity would need to be addressed, as evidenced by the country's score of 36.6 out of 100 for network performance[13] on GSMA's Mobile Connectivity Index, only above Solomon Islands and Tonga among countries assessed in the Pacific Islands (GSMA, 2020). Stakeholder interviews revealed that limited access to reliable electricity connections can make it difficult to maintain mobile data service networks in remote areas. A digital ID platform in Vanuatu based purely on data services would therefore exclude a large number of the population.

High mobile signal coverage creates opportunity to embed voice and USSD channels into digital ID platform. Despite the challenges facing large segments of the population in accessing data services, 92% of people in Vanuatu are within reach of a mobile network signal (Standards Australia, 2020). There is therefore a possibility to include those individuals without data access via voice and unstructured supplementary service data (USSD) channels in a digital ID solution.

Basic and feature phones dominating over smartphones. Basic and feature phones dominate in Vanuatu. Vanuatu's smartphone adoption rate is the second lowest (ahead of Papua New Guinea) among the Pacific Islands, with only 26% of total connections made up of smartphones (GSMA, 2019). While this share is predicted to increase to 66% of connections by 2025 (GSMA, 2019), the relatively low share of smartphones hampers mobile service and product providers in their ability to create viable business cases. This in turn impacts the use cases for a digital ID platform until more mobile services are available and taken up. The current widespread adoption of basic and feature phones further underpins the need for a digital ID solution that can be accessed via voice and USSD, as discussed above. This is necessary to build enough transaction scale in the utility and to prevent the increase of a digital divide within the population.

11 Defined as a single individual who is subscribed to mobile services at the end of the period, with that person being able to hold multiple mobile connections (i.e. SIM cards) (GSMA, 2015)

12 This includes internet access via a computer, mobile phone, personal digital assistant, games machine, digital TV etc. (World Bank, n.d)

13 Indicates the quality of mobile service measured by download speeds, upload speeds and latencies. In Vanuatu, high latency of connections (i.e. the connection between signal and transmission of information can be high) as well as slow upload and download speeds of mobile services impact negatively on the score (GSMA, 2020).

Large gaps in electricity coverage could impact ability to run and usage of platform. In Vanuatu, 62% of the population have access to electricity, well below the Pacific Island small states average of 86%. In rural areas, only 51% of people have access to electricity compared to 94% of people living in urban areas (World Bank, 2020). As a result of a lack of connection to the country's electricity grid, about one in six households in rural areas tend to use various forms of self-generated electricity, mainly by using fossil fuels (UNDP, 2015). Stakeholder interviews revealed that those living in remote areas also rely on solar power for electricity. Gaps in access to reliable electricity connections, particularly in remote areas, could hamper the ability of individuals to use the digital ID platform if they face difficulty in being able to charge their digital devices, which could mean that such a solution is outside their reach. As mentioned previously, unreliable electricity supply can also impact mobile network reliability in these areas, which could undermine system functionality and usage of the digital ID facility.

Usage of digital mobile services limited: potential for digital ID platform to drive uptake. Financial transactions in Vanuatu are mostly conducted using cash or cheque, with less than 3% of adults using a mobile payment channel to send and receive money or pay bills (Reserve Bank of Vanuatu, 2016). While a digital ID platform could help drive the uptake of DFS in Vanuatu by creating a robust SIM registration process and enable a more streamlined approach to opening of mobile wallets, the low adoption currently indicates a larger barrier in terms of trust and use cases that would first need to be overcome. Remote financial transactions using a digital ID are therefore not likely to generate sufficient transaction scale. In the shorter term, the value-add to the digital ecosystem is in the ability to electronically verify identity information during face-to-face engagements until transactions in mobile DFS scale further. DFS as a use case for the platform is discussed further in Section 4.

3.2. Demand side considerations: is the population of Vanuatu ready for a digital ID platform?

Vanuatu has an estimated population size of close to 310,000. Sixty-five percent (65%) of the population is under the age of 30 and the country has a median age of 21.1 (UN, 2020). This section seeks to provide an understanding to what extent Vanuatu's youthful population is familiar with mobile digital services, their digital readiness in terms of literacy, trust as well as attitude. These factors impact the usage and ultimate viability of the identity utility.

High levels of language diversity need to be incorporated into digital ID platform. In Vanuatu, there are more than 100 native languages on top of the three official languages English, Bislama and French (Chepkemoi, 2017). Eighty-eight percent (88%) of the country's adult population (aged 15 years and older) are literate, with 81% comfortable with reading and writing in Bislama and 50% comfortable in English (DigitalReportal, 2020; Reserve Bank of Vanuatu, 2016). At a minimum, English and Bislama should therefore be incorporated into the digital ID platform to enable its use by the majority of the country's population, while French is also desirable. A voice system would need to be considered to accommodate the 12% of the population that is illiterate and those segments of the population using other languages.

Digital platform would need clear value propositions given most of the population not familiar with online technologies. The population of Vanuatu has a small online footprint, with only 26% of people having access to the internet. Of those who are active online, only 31% are active social media users (DigitalReportal, 2020). There would therefore be the need to demonstrate clear use cases for the digital ID platform for the vast majority of the population that is not familiar with benefits of interacting through digital channels. Building trust and consumer protection mechanisms will also be important to increase usage of digital channels for a population not familiar with sharing their personal information online. This will be discussed further in Section 3.3.

Awareness, education and assistance for onboarding required given lack of experience with digital channels. Given the large population size that is not familiar with digital channels, awareness and education initiatives would need to be implemented to get them accustomed to utilising these channels. This would likely require face-to-face instruction to encourage people to try accessing remote services that are underpinned by a digital ID solution, which could highlight the value-add this kind of utility could bring to their daily lives. These considerations need to be taken into account when budgeting for the set-up of and enrolment into a digital ID platform.

3.3. Regulatory and policy environment

This section investigates the policy and regulatory environment in Vanuatu that would underpin a digital ID utility. This will help in identifying gaps that would need to be addressed to facilitate the implementation and adoption of an inclusive, transparent and safe digital ID platform in the country.

3.3.1. Concept of identity

Concept of identity in legislation could allow for innovation in fields of identification. The concept of identity is referred to in Vanuatu's Electronic Transactions Act 2000 (ETA). The definition of an "identifiable individual" in this piece of legislation refers to someone "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physiological, mental, economic, cultural or social identity" (TRR, 2000). The definition is appropriate and useful in that there is no specification for the identification number to be issued in the form of a paper-based document. Further, it does not restrict innovation by enabling the use of biometrics or ID proxies linked to an ID number to be utilised by individuals. The concept of identity therefore enables access to services remotely without the need to carry around physical documents to prove identity. This concept would need to be harmonised across all legislation, regulation and de facto implementations to ensure the use of a digital ID across all sectors of the economy.

3.3.2. Data privacy and security

A digital ID solution entails the collection and storage of large amounts of personal data and it is therefore important that there are frameworks in place to ensure this data is kept private and is protected.

Sectoral regulation governing data privacy could provide framework for regulation covering digital ID platform. While Vanuatu does not have comprehensive laws relating to data privacy, its Telecommunications and Radiocommunications Regulation Act 2009 stipulates that consent is required for services providers in the telecommunications sector to collect or disclose customer data, except under specific circumstances[14], thus providing individuals a certain degree of control over their data. This indicates that there is legislation in place that could serve as a reference point to be used in composing a national broad-based consumer data privacy framework to ensure strict privacy measures around information housed on a digital ID platform. If a digital ID solution is introduced without strong control measures aimed at data privacy, it could lead to the misuse of data by requesting parties, which could undermine trust and usage of the platform.

Data protection regulation undeveloped in light of implementation of digital ID platform. While Vanuatu's ETA allows for the Minister responsible for telecommunications and electronic commerce to enact regulation on data protection standards[15], these have yet to be developed (Bali Process, 2015). There is therefore a need to establish robust national frameworks detailing legal requirements and standards on data protection. A new Cybercrime Act is under consideration and expected to address threats including misuse of identity and data[16]. This is important to safeguard against data breaches and misuse of information housed on a digital ID platform to prevent risks such as identity theft. Data protection controls and standards that could be introduced and mandated under the country's legal frameworks could include requirements to encrypt and/or anonymise personal data (World Bank, 2019). In addition, penalties for unauthorised access, use or alteration to personal data should also be included in legislation and regulation (World Bank, 2019). These could be developed in line with international standards on data protection such as the European Union's General Data Protection Regulation (GPDR)[17]. Putting in place adequate safeguards can help promote user trust and help facilitate adoption of a digital ID solution.

Cybersecurity frameworks under development. Vanuatu does not currently have a national cybersecurity framework in place but progress is being steadily made on legislation related to issues of cybersecurity (RNZ, 2020). There is recognition by government of the risks of cybersecurity facing the country, evidenced by the launch of a National Security Strategy (NSS) in 2019, which included 10 pillars of focus for the country's national security of which cybersecurity was one (Government of Vanuatu, n.d). Existing legislation covering issues related to cybersecurity include the Telecommunications Act 2006[18] and ETA. These frameworks, however, do not put in place legal standards for information technology (IT) security which would be required under a digital ID platform (World Bank, 2019). There is therefore the need for a robust national cybersecurity framework to be in place before launch of a digital ID platform. The draft Cybercrime Act that is under consideration outlines actions against computer related offences such as unlawful access to computer systems and communications networks. If adopted, this would represent a positive step in safeguarding

14 Section 40 of the Act provides that a service provider must not, without the consent of the end user, or unless required by law or authorised by warrant or by the telecommunications regulator: (a) divulge any personal end user information to any person who is not an agent or employee of the service provider; or (b) collect any personal end user information not reasonably required for the provision of any telecommunications service to an end user. https://www.trbr.vu/attachments/article/195/Telecommunications_and_Radiocommunications_Regulation_Act_2009.pdf

15 Section 25 of the ETA, stipulates that the Minister may make orders prescribing standards for the processing of personal data, whether or not the personal data originates inside Vanuatu. Available at: https://www.vfsc.vu/wp-content/uploads/2015/12/Electronic-Transactions-Act-No.-24-of-2000.pdf

16 Part 3 of the Bill for Cybercrime Act stipulates offences for identity related crimes and misuse of data. Available at: https://parliament.gov.vu/images/Bills/2020/2nd_Ordinary/English/Bill_for_the_Cybercrime_Act_No_of_2020.pdf

17 GDPR is a regulation that requires businesses to protect the personal data of EU citizens from misuse and exploitation for transactions that occur within EU member states. Available at: https://gdpr.eu/

18 Telecommunications (Amendment) Act 2007 stipulates penalties and offences for interactions or misuse of telecommunication transmissions or messages and the latter dealing with misuse of information in an electronic record (WIPO, n.d)

against cybersecurity risks[19]. Alternatively, the standards adopted by the digital ID platform could become the de facto compliance standards and set the tone for a regulatory framework in the country. If no standards are implemented, there is a risk that the platform would fail to comply with a subsequent standard. Addressing these risks would prevent the digital ID platform from becoming susceptible to hacks targeted at stealing identity data or destabilising the functionality of the platform.

3.3.3. AML-CFT regulation

Given that financial services are likely a key driver of the platform, it is particularly important to assess how the existing anti-money laundering and combatting the financing of terrorism (AML-CFT) regulation and guidelines would impact the functioning of the utility.

Need for clarity on what constitutes a "document" for customer due diligence (CDD) purposes in AML-CFT regulation. Vanuatu's AML-CFT regulatory frameworks[20], issued by the country's Financial Intelligence Unit (FIU), require regulated entities to use "official or other identifying documents" to identify their customers (Reserve Bank of Vanuatu, 2015). Regulation, however, does not give a clear definition of what constitutes a "document" (i.e. whether it has to be a in physical form or whether it can be in an electronic format). This lack of a clear definition of what a document is, is being conservatively interpreted by institutions to mean physical paper-based documents[21]. The listing of different combinations of physical documents[22] to assert and verify identity using a risk-based approach (RBA)[23] in regulation is further reinforcing this approach. Institutions are therefore constrained in their ability to innovate, as it is implied that they undertake customer due diligence (CDD) using physical documents, regardless of the risk of the customers or level of assurance provided by this identification and verification method. This creates a barrier to the use of a digital ID and erodes the potential value-add such a solution could bring in terms of providing a more robust and easily verifiable form of identification that can be used for remote onboarding. To accommodate a digital ID platform, the country's FIU would need to issue sufficient guidance to institutions that clarify the interpretation of AML-CFT regulation and whether electronic forms of documentation could be appropriate for CDD purposes.

Digital ID platform should meet foreign regulations to capture passport information and understand a person's nationality. For expats and citizens of other countries, the digital ID should also be able to facilitate and meet their home jurisdiction requirements, for example the ability to facilitate GDPR and US regulations such as Foreign Account Tax Compliance Act (FATCA)[24]. This is important when it comes to handling foreign passport information (such as biographic and biometric data) to be able to adequately identify and note the nationality of people in line with accepted international systems, formats and standards in place.

19 Part 2 of the Bill for Cybercrime Act stipulates computer related offences: Available at: https://parliament.gov.vu/images/Bills/2020/2nd_Ordinary/English/Bill_for_the_Cybercrime_Act_No_of_2020.pdf

20 Framework comprises of the Anti-Money Laundering and Counter-Terrorism Financing Act No.13 of 2014 and the Anti-Money Laundering Counter Terrorism Financing Regulation Order No. 122 of 2014. Available at: https://fiu.gov.vu/

21 Stakeholder interviews revealed a focus on the presentation of paper-based documents such as birth certificates, driving licences or the VNPF card when onboarding new clients.

22 As outlined in Table B of Schedule 2 of Anti-Money Laundering Counter Terrorism Financing Regulation Order No. 122 of 2014.

23 The FATF requires countries and institutions to use a risk-based approach when implementing AML-CFT controls. Practically, this means aligning the number of resources applied with the level of money laundering risk. Institutions implementing a risk-based approach would, for example, apply greater resources, monitoring and CDD obligations towards higher risk customers and vice versa for lower risk customers. This is supposed to enhance the financial system's ability to combat crime, improve efficiency of processes and reduce the amount of red tape that lower risk individuals are exposed to in customer onboarding processes (FATF, 2007).

24 FATCA requires foreign financial institutions and certain other non-financial foreign entities to report information to their local Tax Authority about foreign assets that are held by their US taxpayers and entities. Available at: https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca

Summarised insights from current ecosystem in Vanuatu

Digital ecosystem

1. The majority of the population can be reached via a mobile phone. A digital ID platform should accommodate voice and USSD access on top of 2G channels given that 74% of people in Vanuatu currently do not access the internet via any device and feature and basic handsets dominate over smartphones.
2. Large gaps in electricity coverage, particularly in rural and remote areas could impact quality to run and usage of platform.
3. Use of mobile digital services nascent and fragile with low current uptake, limiting their ability to drive considerable uptake of the digital ID platform.

Demand-side considerations

4. Bislama, English and French should ideally be accommodated in a digital ID interface to allow usage by majority of country's population. To include those comfortable in other languages as well as the 12% of the population who are illiterate, a voice service could be embedded into the digital ID platform. Given the extremely diverse set of languages across Vanuatu, this requires careful consideration to avoid exclusion.
5. As mobile internet and social media use is limited, trust still needs to be established for the majority of the population. Fit-for-purpose awareness and usage campaigns around digital services and digital ID use would have to be factored into the set-up costs to drive uptake.
6. Mobile money is seldom used by the people of Vanuatu. More use cases around its usage would need to be created to promote usage and the population would need to be educated and trained on how to utilise online services.

Regulatory environment

7. Legislation governing data privacy is in place in the telecommunications sector which could provide a framework for developing national broad-based consumer data privacy legislation.
8. A new Cybercrime Act is under consideration and expected to address threats including misuse of identity and data. Data protection frameworks are important to build security and trust in the digital identity system.
9. A draft Cybercrime Act is under consideration that outlines actions against computer related offences such as unlawful access to computer systems and communications networks. If adopted, this would represent a positive step in safeguarding against cybersecurity risks. Alternatively, the standards adopted by the digital ID platform could become the de facto compliance standards and set the tone for a regulatory framework in the country. This is important as having legal standards for IT security in place before a digital ID platform is launched could prevent it from becoming susceptible to data breaches.
10. Vanuatu's AML-CFT regulation lacks clarity on what constitutes a "document" for CDD purposes and whether remote CDD is legal. There is therefore a need for the FIU to issue sufficient guidance to the market in this regard to not undermine the utility of the platform.

4. Use case analysis

This section analyses the different use cases for a digital ID in the country. Use cases in this context are the most prominent services in Vanuatu that currently require an identity document to be presented or verified and that would have use for a digital ID utility. The civil and financial services use cases are explained in the country context and how challenges could be addressed by a digital ID platform. After this overview, the use cases are ranked based on their transaction scale as well as their relative importance in terms of meeting stakeholders' objectives, taking the local context into account.

4.1. Overview of civil and financial service use cases

Table 3 and Table 4 list all major applicable use cases in the civil and financial space, respectively, in Vanuatu. This information is based on literature and stakeholder engagements and includes the most prominent needs in the Vanuatu context.

4.2. Use case ranking

Two ranking lenses are applied in this exercise: transaction scale as well as national stakeholder objectives, to assess the extent of demand for such a platform in the local context.

Use cases provide transaction scale for a digital ID platform. The current number of users in the respective sectors serve as a first proxy to understand how much scale in transactions the platform could possibly generate. This is important to inform the governance and financial model discussed in Section 5. Ideally all use cases would be integrated to create the maximum scale on the platform. As it is not practical to integrate all use cases at once, however, the ranking based on transaction scale gives an indication of priority of integration. Box 5 outlines the methodology behind this analysis lens.

Stakeholder objectives and national policies will drive stakeholder buy-in in practice. The transaction scale ranking is important to understand the demand for a platform in the absence of existing digital solutions. Vanuatu has limited digital solutions for a number of use cases and hence it will be important to reflect how that influences the likelihood of buy-in for use case development to be supported by the new system. Different agendas and objectives ultimately need to be met by the platform to make the utility useful for the public and private sector – in some cases these are driven by national or regional policies, in other cases by profit. Stakeholder interviews, literature and national policies influenced the priority ranking in the national objectives lens. Box 6 provides further information on the approach behind this parameter.

High-priority use cases

Financial use cases highest priority; SIM registration key. High transaction use cases, shown in Figure 2, are services that we estimate to have more than 4,000 potential monthly requests to verify an individual's identity

Table 3. Civil service use cases for a digital ID platform in Vanuatu

Use case	Challenge the digital ID platform could address
Enable unique and up-to-date voter identification	The current voting database has issues with duplicates as well as containing outdated data. **Solution:** A digital ID platform would centralise detail/information changes such as changes in address, civil status, deaths etc. to ensure up-to-date, robust information on the voter database.
Enable replacement of birth certificates and centralised birth registration	Loss of documents, especially after disasters is common. **Solution:** A digital identity platform would enable remote access to a digital birth certificate and could reduce the cost of access when needing to use a birth certificate as an identifier. It would also enable a standardised format to onboard or register new births.
Improve marriage and death registration and data sharing	Data sharing between agencies on death and marriage status information is often delayed and prone to errors, thus increasing the potential for fraud and identity theft. **Solution:** A digital ID platform would facilitate data sharing and allow for registration of civil matters to be centralised and unique. It would also enable remote access to individual's status to enable further remote services.
Accessible title deed registration and verification	The electronic database for title deeds is currently not linked to other identity databases. The information is not easily accessible by third parties. **Solution:** A digital ID platform that includes title deed information would pull through title deed information changes for third-party providers and allow for remote verification of title deeds.

(continued on next page)

Use case	Challenge the digital ID platform could address
Enable centralised and remote criminal background check	Processes around criminal background checks are currently manual and time-consuming. Criminal background checks are conducted in case of crimes, for enhanced due diligence of politically exposed persons (PEP), for individuals on sanctions lists as well as for visa purposes and employment, among others. **Solution:** A digital ID platform would enable authorities, employers, FSPs and others to have the most up-to-date information on the criminal history of individuals, if linked to a unique identity. Moreover, the waiting period for police clearance could be eliminated through real-time verification.
Enable more seamless remote school enrolment	Students need to present their birth certificate when registering for school and the process is done face-to-face. **Solution:** Information can be directly accessed through the digital ID platform, so that the birth certificate does not need to be presented anymore. School enrolment can be planned and facilitated with a more comprehensive database of prospective student cadres per area.
Allow for remote driving licence renewal and registration	Current driving licence renewal is done face-to-face and requires a paper identity document. **Solution:** A digital ID platform would centralise driver identity information to allow for remote renewal and would make the registration process more seamless due to the ability to verify an individual's identity information.
Emergency assistance and disaster recovery	The occurrence of natural disasters causes displacement of people on a frequent basis. It is not easy to identify individuals in need of assistance after an emergency and enable swift relocation to a safer location. **Solution:** A digital ID would enable swifter relocation services such as change of address as well as help to identify people in need of financial or humanitarian support in conjunction with satellite imagery that can be compared to population information on the platform.
Allow for quicker hospital admissions	Hospital admissions and health service access involve many time-consuming forms and the need for identification could impact an individual's ability to access urgent healthcare. **Solution:** A digital ID platform would allow for quick identification of patient and related health records, if electronic document storage is linked to the platform.

Source: Authors' own based on literature and stakeholder interviews

Table 4. Financial service use cases for a digital ID platform in Vanuatu

Use case	Challenge the digital ID platform could address
Enable remote opening and verification of financial accounts	Currently accounts are opened with hard copy documents and in person only. There is no shared digital verification system to allow third parties to verify account information or document authenticity. Limitations in effective risk-based approaches cause an acute focus on compliance risk mitigation instead of focusing on mitigating AML-CFT risks. This limits overall risk management effectiveness and can drive de-risking decisions. **Solution:** A digital ID platform would decrease the need for hard copies and aid remote onboarding and verification through centralised information. The employment of an identity proofing approach combined with an enhanced ability to cross-reference multiple digital identifiers and risk factors can enhance compliance risk management capabilities, reduce the risk of exclusion as well as provide better levels of sectoral overarching assurance which influence international de-risking decisions[25].
Enable SIM card registration and verification and e-money registration	Ni-Vanuatu as well as non-locals can currently obtain multiple SIM cards without identity documents, which leads to financial risks in mobile money services and an increased threat of fraudulent activity. **Solution:** A digital ID platform would link an identity to a SIM card, not an identity document, to allow for robust verification of mobile money transactions and SIM card ownership.
Minimise misdirection of G2P welfare payments and improve natural disaster assistance	Given the duplications due to allowing multiple IDs for sign up there is leakage in the system. Natural disaster assistance requires a quick and efficient pay-out to affected individuals. **Solution:** A digital ID platform would uniquely identify individuals eligible for G2P welfare payments and it would also provide a de facto routing of welfare payments, even for those without accounts, to enable collection via the most appropriate instrument. A digital ID platform will also enable authorities to identify affected individuals quickly and efficiently by accessing different databases and hence channel the required support with minimal delay.

(continued on next page)

25 The underlying digital identity datasets create opportunities for regtech and suptech solutions that can enable exceptionally high levels of risk detection as well as more proportionate consumer approaches with broader economic inclusion possibilities.

Use case	Challenge the digital ID platform could address
Enable remote customer due diligence (CDD) for money transfer operators (MTOs)	Face-to-face interactions with agents to collect cash remittances is expensive and requires a wide agent network. Additionally, customers must bring physical identification documents every time they collect cash remittances. **Solution:** A digital ID platform and its related proxy identities would enable remote collection of digital remittances. This would alleviate the difficulty of having to physically travel to MTO branches with physical documents. Robustly verifying the identity of recipients can impact the risk profile of institutions in respect of correspondent banking and thus encourage increased international ratings and access.
Enable the development of e-commerce payments	E-commerce is currently nascent in Vanuatu. One of the key barriers to new entrants participating in the e-commerce space in Vanuatu is the lack of mechanisms to accept payments online from customers (UNCTAD, 2018). **Solution:** A digital ID platform would enable real-time payments by aiding effective customer and vendor identification but also driving more e-commerce solutions. In addition, it could be an important first step to encouraging fintechs to develop payments solutions for e-commerce in Vanuatu as the digital ID platform can be used to route payments linked to customer identities.
Enable remote utility payments	The low level of financial inclusion and a recent emergence of mobile money in Vanuatu suggests that while the Utilities Regulatory Authority accepts digital payments, they are more likely to transact a considerable proportion of their payments through cheque or cash. **Solution:** A digital ID platform would enable more users of the service as they can take advantage of identity verification and proxy identities to pay. It would also enable the Utilities Regulatory Authority to accept remote digital payments without having the need to first register the customer.
Enable remote credit reporting and history access	Accessing credit history is vital to enable the extension of credit for both providers and consumers. While Vanuatu has an established credit bureau, Data Bureau Limited, it is currently underutilised. **Solution:** A digital ID platform would enable more coverage from the credit bureau as they can use the identity platform for identity verification and proxy identities. In addition, an individual's identity will be linked to their credit score and credit history, which is available remotely to credit providers for quick verification. It would also allow for better digital credit provision.
Enable remote insurance onboarding and claims verification	Insurance penetration is low and the onboarding processes are costly for providers. Claims pay-out processes are also costly and time-consuming and do not occur remotely. **Solution:** A digital ID platform would enable quicker onboarding through remote identity verification, which can lower CDD costs, making insurance more accessible and affordable. Digital identity linked proxy IDs can be used to route claims pay-outs.

Source: Authors' own based on literature and stakeholder interviews

Box 5: Ranking methodology for transaction scale lens

Transaction scale or number. Transaction scale refers to the number of requests for identity verification or onboarding from individuals and/or service providers (including government) that the platform would perform.

High, moderate, low priority. The ranking is divided into high, moderate and low priority integration based on the likely number of average recurring transactions per month. Some of these services, such as voter registration, will be performed as needed and not monthly but for comparability we express the likely number of digital ID transactions per month. The annex provides further details on the assumptions behind the calculations.

Once-off transactions. Once-off transactions include the first onboarding of new individuals as well as the consolidation of identity information of each existing digital identity database in Vanuatu. As they are only performed once they are not necessarily a continuous driver for scale but are important to take into account when it comes to estimating the initial cost and governance model of the platform, which is discussed in Section 5.

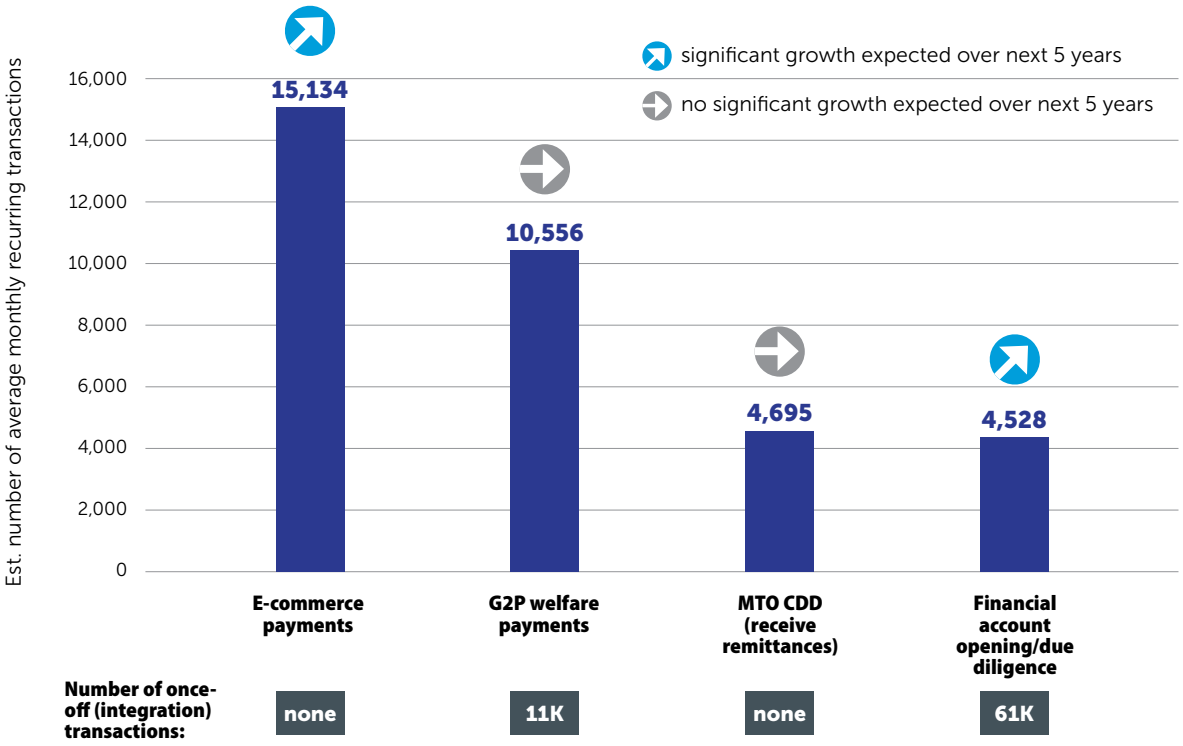
Growth. The growth indicator highlights to what extent the use case in question is likely to grow over the next five years. A high-growth use case suggests that its importance will likely increase over time even though its current demand may be moderate or low. The growth rate is dependent on a number of infrastructure developments, especially in the digital payments space and is only indicative.

Box 6: Ranking methodology for national priority lens

High, moderate, low priority. The ranking is divided into high, moderate and low priority integration based on the composite of several factors. These factors include the extent to which the use case was mentioned in literature or in stakeholder interviews as fulfilling a concrete need. Not every use case listed in Section 4.1 is high in terms of stakeholder interests, either because the use case does not tie neatly to existing national policies, i.e. does not fulfil a priority objective and is hence less likely to be prioritised for integration in practice; or because stakeholders do not see a sufficient case to invest in new infrastructure or have already invested in other infrastructure to meet their needs for identity verification. Hence, use cases with an existing digital infrastructure have been ranked lower priority as the gains from introducing a digital ID platform for them will most likely be lower. Equally where stakeholders indicated a marginal appetite for change. In such cases, especially where transaction scale is high, it will be important to clearly quantify the added benefit (e.g. cost savings or efficiency gains) that integration with the digital ID platform would have, as otherwise stakeholder buy-in could be a challenge. The collected information is based on stakeholder engagements and existing literature.

via the digital ID platform. While the mobile DFS market is still nascent, the ability to conduct remote transactions and verify people's identity in real time with up-to-date information has the highest potential to generate the most transactions. E-commerce payments are expected to grow in line with further digital ecosystem development. However, for this growth to materialise it will be important to prioritise the registration of SIM cards and link them to unique identities via the digital ID platform. This is also a priority in terms of national objectives, as shown in Table 5. Other financial use cases include G2P payments, which also rank highly on the national priorities given Vanuatu's high risk of natural disasters. Financial account opening and MTO CDD rank highly due to their implications for the financial sector. The former is expected to grow within the next five years given the trajectory on the financial inclusion side. For Vanuatu, emergency assistance after natural disasters is priority and hence should be enabled by the ID platform. Once-off, initial integration transactions would only be needed in the case of G2P payments and financial accounts, which is not prohibitive and could be achieved cost effectively, dependent on the quality of the existing databases in the use cases.

Figure 2. High-scale transaction use cases



Source: Authors' own based on literature and stakeholder interviews

Table 5. Use cases with high national priority

National priority lens	
Use case	**Considerations**
Financial account opening and due diligence	The digital ID platform is a high priority for the Reserve Bank of Vanuatu to enable financial inclusion and manage risks to the financial sector and beyond. It also ranks as a high priority to financial service providers to onboard new clients and manage risks linked to current clients.
Closing the foundational ID gap	The digital ID platform is a high priority to the government of Vanuatu to address the gap in foundational ID. A significant share of the population is not registered in any of the current databases. While the national ID rollout is underway, this gap needs to be narrowed substantially to meet national economic and social objectives. Consolidating the multiple ID databases and reaching those without any form of identity will therefore be a top priority for using the platform.
MTO CDD (receive remittances)	The digital ID platform is a high priority to the Reserve Bank in terms of being a significant enabler of remittances and a mechanism for ensuring the integrity of the ML/TF regime in the cross-border remittances space. For money transfer operators a digital platform could alleviate stringent CDD caused by de-risking which is throttling remittance inflows.
SIM and e-money account registration and verification	For the providers and Reserve Bank of Vanuatu, the platform is a high priority because developing a robust SIM registry system is important to mitigate AML-CFT risks arising in e-money. It also allows the expansion of other DFS services and linked ID proxies due to phone number registration.
G2P welfare payments	For the government of Vanuatu, ensuring timely, well-targeted welfare as well as reducing fraud risks around these payments is important to ensure the wellbeing of Vanuatu residents. The digital ID platform will assist the government in offering economic support to impacted families during natural disasters through expeditated welfare payments.
Emergency assistance and disaster recovery	For the government of Vanuatu, natural disaster risk mitigation and recovery is a top priority. The digital ID platform will assist the government of Vanuatu to reach more individuals in times of natural disasters through expeditated emergency assistance payments.

Source: Authors' own based on literature and stakeholder interviews

Modest monthly transactions, closing foundational ID gap and regional integration crucial. The number of use cases that can generate a relatively high number of transactions is low in Vanuatu. This has implications for the financial sustainability of a digital ID platform and its ability to generate enough value for stakeholders. To increase the share of transactions it will be crucial to close the foundational ID gap by onboarding more citizens onto the platform or any of the existing databases to be integrated with the utility. While this can have severe cost implications, the drive to expand the national ID already onboards new people regularly and would just need to be strengthened and prioritised. To increase scale in a utility and meet national objectives, regional integration with other islands in a shared facility would be advisable, further discussed in Section 5.

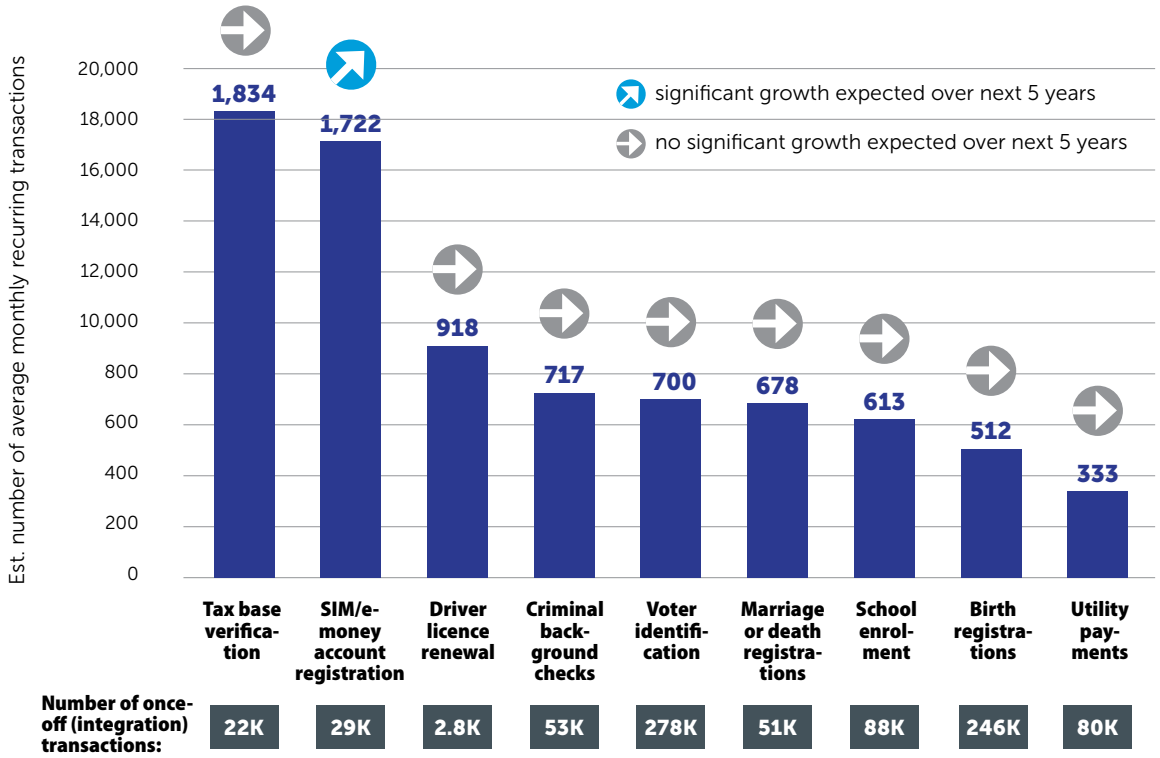
Medium-priority use cases

Low monthly transactions but high gains from once-off integration; stakeholder buy-in crucial. Most use cases in Vanuatu fall in the medium priority list. As shown in Figure 3, nine use cases are estimated to generate between 300 and 2,000 monthly transactions through the platform. Tax identification, e-money account opening, driving licence renewal and criminal background checks fall within this category. E-money accounts are the only use case in this cohort that is expected to grow more than population growth over the next five years and there is potential for it to move to the high priority bucket. Given the overall low number in transactions in this category overall, the value-add may not necessarily lie in the number of reoccurring transactions but rather in the integration (i.e. once-off registration) of existing databases to drive consolidation and efficiency. As a number of the listed use cases already have electronic backend systems, stakeholder buy-in may be lower. It is therefore crucial to prove efficiency gains, market access and cost savings to the stakeholders in question. Table 6 details the efficiency gains that could be achieved if the civil use cases were linked, especially in the case of voter, birth, marriage and death registrations, as well as utility and e-commerce payments, given that this information is kept in fragmented databases. The high number of different stakeholders that would have to agree on specifications of the system, however, runs the risk of delay in establishing the utility, calling for a strong entity to lead this endeavour.

Low-priority use cases

Credit history, title deeds and insurance low on integration list due to more pressing systemic barriers. Lower priority use cases are expected to

Figure 3. Medium-scale transaction use cases



Source: Authors' own based on literature and stakeholder interviews

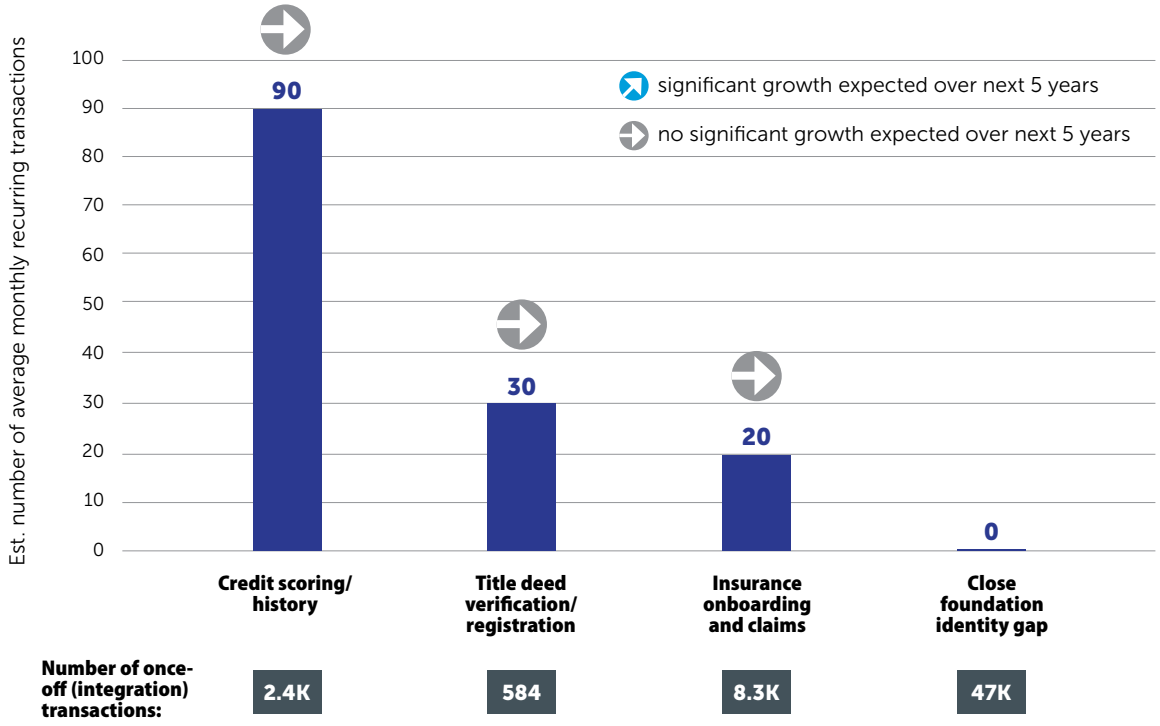
have less than 100 monthly transactions on a digital ID platform, as shown in Figure 4. Credit history access, insurance and title deed verification generate very small numbers of ID verification transactions and will only add marginal value to scale. These are also lower among the national priorities, listed in Table 7, given that the expansion of these financial services across the population is not currently crucially dependent on identity verification but on the removal of systemic barriers in the system. If general access to these services is expanded, monthly transactions in the digital ID system are also likely to grow. Hence it is still advisable to consider integration of the lower-scale use cases to enable future benefits. As discussed above, closing the foundational identity gap may not add any reoccurring transactions but is a crucial step to enable higher scale in all other use cases.

Table 6. Use cases with medium national priority

National priority lens	
Use case	**Considerations**
Birth registration	The National ID roll-out is currently verifying birth certificate information, yet there is still room to close the birth certificate gap. Using the digital ID platform for birth registration is a medium priority as a new National ID system exists.
Voter identification	The infrequency of elections means that using a digital ID platform is not a high priority use case. In addition, the national ID roll-out is already aiming to verify voter information. The voter identification use case is therefore a medium priority.
E-commerce payments	Using a digital ID platform for e-commerce payments is a medium priority as the e-commerce sector is still nascent yet growing. The Vanuatu Government can make use of this developing industry to drive digital payments enabled by a robust digital ID system and hence could create more traction in e-commerce.
Marriage or death registrations	For the Department of Civil Status, the platform will enable them to track marriages as well as deaths more accurately. For the Ministry of Health, the platform enables accurate accounting of deaths. For both, a separate database already exists, hence the medium categorisation.
School enrolment	Using a digital ID platform for school enrolment is a medium priority given the already high rate of enrolment. The Vanuatu Ministry of Education and Training can particularly benefit from being able to account accurately for students enrolled versus school-aged children that are not in school. Stakeholders also indicate that the data on the platform is helpful to the Ministry of Education and Training for budgeting and planning purposes.
Criminal background checks	The Vanuatu Ministry of Justice and Community Services as well as the Vanuatu Police Force will benefit from the digital ID platform by being able to access real-time integrated information. Using the digital ID platform for criminal background checks is a lower priority for Vanuatu given the relatively low crime rate.
Utility payments	Enabling digital utility payments is a medium priority because mobile money utility payments already exist. However, the share of digital utility payments could be increased considerably in line with the expansion of the digital ecosystem, bringing efficiencies to both providers and consumers.

Source: Authors' own based on literature and stakeholder interviews

Figure 4. Low-scale transaction use cases



Source: Authors' own based on literature and stakeholder interviews

Table 7. Use cases with lower national priority

National priority lens	
Use case	**Considerations**
Tax-base verification	In Vanuatu, there is no personal income tax and the tax base is relatively small. TIN has only recently established and hence additional gains from integration for the database may be too small.
Credit scoring and history	Given the existence of an established credit bureau (Data Bureau Limited), that has been around for almost 10 years, the credit scoring and history use cases are a low priority for the digital ID platform. However, due to its low coverage, there could still be some benefit from the bureau accessing the digital ID platform. The inclusion of biometrics and proxy IDs in the platform may also benefit the existing bureau in improving the quality of credit scoring and credit history in Vanuatu.
Title deed registration and verification	The Department and Ministry of Lands has developed a title information system to capture title deeds electronically. The use of a digital platform for title deed verification is therefore a low priority. Customary land and remote land could benefit, however, from the new digital platform, as the platform will streamline the onboard and verification process for the customer.
Insurance onboarding and claims	While a digital ID platform may assist in improving risk management in general, the platform is a low priority use case for insurance given the low uptake of insurance in Vanuatu.

Source: Authors' own based on literature and stakeholder interviews

Summarised insights from use case analysis

1. While there is a significant number of use cases that could benefit from a digital ID utility in Vanuatu, the likely monthly transactions that could be generated by most of these use cases may not make it financially viable to integrate a large share of them. Regional integration will be key.
2. Given the size and different owners of the current databases, once-off integration and consolidation of existing information will require considerable effort before revenue can be generated, but is absolutely crucial to bring inclusivity, efficiency and longer-term cost savings to the market.
3. Financial transactions (e-commerce payments, G2P payments, MTO CDD and e-money and financial account opening) are expected to contribute the largest share of transactions now and in future and are also a national priority. Including financial stakeholders will therefore be important.
4. In terms of national priority, closing the foundational identity gap will be vital in narrowing the digital divide and in developing an inclusive economy. The platform can give the template for onboarding and it will be crucial to bringing more people into the formal system to generate scale and improve inclusion.
5. Utilising the digital platform for SIM registration would have several benefits, ranging from streamlined e-money account opening to enabling ID proxies. This use case should ideally be integrated to bring value to a range of stakeholders as well as aiding in meeting national objectives.
6. Several systems for electronic service delivery already exist, especially across civil use cases such as school enrolment, driving licence renewal and birth, death and marriage registrations, but to a varying degree of efficiency. This puts these existing services at a lower priority for integration with the platform from a stakeholder perspective and it will require significant efforts to get stakeholder buy-in in that space.

5. Governance and financial considerations for a digital ID platform

This section will pull together the insights gathered from the previous sections of the report to assess the essential design features for consideration of the platform, their cost implications as well as the governance structure the solution could employ.

5.1. Governance structure

Designing a fit-for-purpose governance structure for a digital ID platform is crucial to ensuring longevity of the utility and should be assessed carefully. This section provides considerations around an approach to determine the best governance model for the platform in Vanuatu. Table 8 lists the advantages, disadvantages and implications for Vanuatu of each of the four governance models introduced in Box 3.

Public–private partnership and NGO-led model more suitable for Vanuatu but only with regional integration. All four models are technically possible in Vanuatu, yet all four have significant disadvantages that can outweigh the benefits of establishing a national digital ID platform. While the need for a digital ID platform is there, the substantial stakeholder collaboration and funding required to implement and operate such a utility across a wide range of use cases are likely to be major deterrents for Vanuatu. Applying the use case analysis above to governance configurations, financial use cases are projected at 26,000 transactions per month which would realistically be insufficient to support even a lightweight platform and hence not very likely to bring the desired benefits to Vanuatu's national objectives. A lightweight and underfunded platform is likely to remain below its utility potential with a high risk of project abandonment. An NGO or development partner-led model as well as a public–private partnership spearheaded by a dominant government department has a good chance of gaining traction, but only if scale in the utility can be increased through regional integration with multiple other Pacific Island states. If there is no regional integration, the likelihood of sustainability is low.

Regulatory changes can cause delay; need to adjust as soon as possible. Given the lengthy processes required to change regulation, the necessary regulatory amendments need to be initiated as soon as possible to not lose momentum. Given the need for regional integration on the platform, a policy should be developed that includes regional perspectives and calls for harmonised regulatory frameworks that in turn enable Vanuatu's regulatory reforms. It is not incompatible for the facility to be built in parallel with regulatory changes provided such changes clarify the utility's framework norms and standards. If the necessary specifications are known upfront or are compliant with established local and international norms and standards, the regulation can follow the platform establishment.

5.2. Financial model

The financial model of the digital ID utility can be split into the set-up costs of the utility and the operational costs of running the utility once it has been set up. The considerations when conducting a cost-benefit analysis are discussed in this section. In general, the stronger the utility is set up and capacitated from the start, the easier it will be to secure continuous financing to ensure longer-term sustainability.

Set-up costs

A systemically important utility: set-up to centre around this goal. For an island state like Vanuatu that is fragmented, infrastructure projects regularly compete for budget and need to prove their value-add clearly to warrant attention from authorities. This digital ID platform has the potential to significantly contribute to Vanuatu's ability to build a digital economy if it proves itself as a systemically important service, underpinning most of the digital and even face-to-face interactions that require identification. The set-up costs are therefore driven to a big extent by efforts to align all crucial stakeholders' expectations in terms of functionality and get stakeholder buy-in through targeted efficiency projections per stakeholder. This upfront investment in terms of time, research and advocacy meetings is essential in eventually creating a systemically important utility that is supported by all. Given the need for regional integration, substantial engagements with other central banks, governments and private sector players can be expected.

NGO or donor community to fund set-up costs. As discussed in the previous section, involvement from an NGO or development partner in the financing and governance of the platform could be a suitable option for the region. By its nature, an NGO model would have an efficiency and inclusive agenda instead of a profit imperative, allowing for a considerate and future-looking design of the platform instead of focusing only on the high-transaction scale use cases. The prospect of an inclusive digital platform that allows the majority of the region's population to benefit is significantly easier to advocate to donors than a for-profit utility, especially to cover the set-up costs. These costs are expected to be high as the existing identity information needs to be deduplicated and consolidated, yet they are much lower than creating a new database that includes the onboarding of individuals from scratch. Therefore, as stakeholders will need convincing to buy into the utility and any benefits from the platform will take time before they can be reaped, the funding necessary to design and set up the platform will likely need to be shouldered by donors or grants. The operational costs can then be recovered through the cost savings by integrated stakeholders, discussed in more detail below. As discussed above, regional integration is key to increase financial viability.

Table 8. Governance model assessment

Advantages

Government-led, owned and operated	Private sector-led, owned and operated	Government-led, private sector-owned and operated	NGO-led and government or private sector owned and operated
• Central ownership structure with dedicated resources • Initial funding model aligned with national budgets or budgetary assistance/loans • Regional integration based on national buy-in and regional financing links	• Independent and market-driven utility • Simplified lines of decision-making and procurement • Alignment with commercial interests • Commercial dynamics, competition and efficiency • Some access to advanced external resources, skills and capacity to implement and operate at scale with remote providers • Speed to market	• Alignment between national government policies and regional government strategies • Governance aligned to sovereign states and credible institutions • Ability to create mutual as well as commercially competitive spaces • Harnesses commercial dynamics and competitiveness in a structured marketplace • Potential for hybrid funding models from national budgets/ loans and commercial capital based on clear government backed market structures • Alignment with commercial interests in a strategically structured regime	• Stronger alignment of facility with regional goals and SDGs • Streamlined but consultative structures and objectives • More agile financial model which can be a hybrid between global organisations, donor countries and NGO foundations plus government assistance and commercial funding • Allows for funding to be aligned to a trusted mutual utility concept and also a competitive commercial space that adds value to the consumer • Decisions and funding are not strictly tied to multi-national budgetary processes • Arm's length decisions when it comes to regional viability vs country specific requirements • Less burden on individual government structures and key national institutions but including key institutions in key digital ID utility governance and oversight structures • Stronger alignment with regional and national policy needs but with an underpinning of commercial scale for sustainability

(continued on next page)

Table 8. Governance model assessment (continued)

Disadvantages

Government-led, owned and operated	Private sector-led, owned and operated	Government-led, private sector-owned and operated	NGO-led and government or private sector owned and operated
• Need to build a consortium of different government departments to ensure buy-in, all with different objectives • Potential conflict of interest as platform caters for both public and private sector use cases • Potentially limited buy-in by private sector if not involved in governance • Potentially slower changes to integration of use cases • Continued funding for facility difficult • Lengthy and complex procurement processes which can result in delays, increased costs and compromises in key specifications • Advanced system implementation and operation capacity constraints	• Lack of scale is difficult to sustain in a business case as an investable project • To sustain any business case would require an exclusive focus on key existing commercial use cases with limited or no focus on nascent use cases and use cases of importance to achieve sectoral or national policy objectives • Infrastructure would need to be very lightweight and acutely aimed at very specific use cases with limited ability to reach ubiquity • Key business case focus on included middle- and higher-income consumers with less focus on lower-income and hard-to-reach segments • Competition norms reduce the possibility of a non-competitive sphere and common utility with a unit-cost efficiency incentive as opposed to a profit-optimisation imperative	• Government and private sector objectives and incentives are difficult to align in an effective public–private partnership (PPP) • Structurally different funding and reporting cycles plus differing administrative requirements and timelines can result in inertia or project failure • Lack of clear governance framework, common strategic objectives and lines of control can result in facility paralysis or misdirection • Given local scale, vendor lock-in agreements are inevitable with the risk of suboptimal facility or excessive default cost guarantees • Changes in government policy and commercial considerations need to be proactively managed • High possibility of vendor or private sector abandonment if use cases are slow to be adopted	• NGO funding cycles, types of funding, theory of change and specific goals difficult to manage in the short-to-medium term • NGOs require substantive buy-in and contracting by governments and/or financial and capacity contributions • A high focus on non-commercial use cases can limit scalability and sustainability • NGO strategic funding and support objectives can change in a short period • NGO measurement of results and reporting can be onerous and not always within the frame of reference of governments and the private sector • Potential for vendor lock-in agreements • Potential for government or private sector abandonment • Ultimate transition to self-sustainable regional utility ownership and governance can result in facility paralysis or misdirection

(continued on next page)

Table 8. Governance model assessment (continued)

Suitability for Vanuatu

Government-led, owned and operated	Private sector-led, owned and operated	Government-led, private sector-owned and operated	NGO-led and government or private sector owned and operated
• Can be a significant burden in Vanuatu given the current development demands and the capacity in government • Will be difficult to coordinate between departments and would increase pressure on existing projects	• Vanuatu has access to international institutions that would be capable of implementing and operating such a facility, but they view it as a non-core activity and question scalability • Private sector not very cohesively organised into sectors to accommodate a sector approach, like, for example, in Nigeria • Limited appetite from existing commercial entities to own and control such a facility but high interest in how the facility can impact their internal processes • External or international vendor is more probable but comes with risks in terms of catering to the local context	• Vanuatu government has limited available capacity to coordinate or lead such an approach given the extent of existing policy initiatives and needs • Cross-departmental considerations could be a challenge • Strong governance centres may lack a direct mandate to oversee such a facility. For example, it would require a predominant financial services component to fall within the Reserve Bank mandate • Use case scalability considerations are significant and would point to a regional facility with a governance model that can harmonise requirements that are fit for purpose in both larger developed as well as smaller, less developed markets	• Would need to be a trusted NGO with a long-term commitment across the countries as an honest broker • Amount, type, mix and timing of funding that could be leveraged would be important • Capacity to establish a governance structure locally and possibly between nations • An NGO would be more likely to succeed across different jurisdictions than one single government or a consortium • From the use case scale evaluations, a facility will more readily achieve scale if leveraged across multiple jurisdictions

Source: Authors' own based on literature and stakeholder interviews

Operational costs

Financial contributions to platform to be set out upfront. To reduce the risk of abandonment of the project and to balance the continuous financing of the platform regardless of the initial funding, all providers and government departments that will be using the utility should be contractually bound to budgetary contributions based on their respective savings gained through the platform. This can ensure the recovery of some operational costs in the initial years and prove the systemic value to the stakeholders. If there are no cost savings, then a stakeholder would not have to continuously contribute, other than for the maintenance of their own system integration and links. This system requires clear rules to mitigate for abuse but could present a viable financing model. In practice this means that grant funding could be sought at the start to cover the most essential infrastructure pieces and technical assistance yet ultimately the platform should not be free to use indefinitely[26].

Build for regional integration. As the expected monthly transactions running through the platform in Vanuatu are too low, this has implications for the sustainability of a national platform if operational costs outweigh the costs that can be recovered through charging per transaction. Even if cost savings for stakeholders are significant, they may still not cover the running costs of the utility. From a financial as well as scale perspective it is therefore advisable to extend the reach of the utility to the entire region. Technological advancements make it possible to ringfence the respective data by country but still utilise the infrastructure capabilities for verification from anywhere in the region. This not only harmonises data formats and encourages regional collaboration but can then lead to cost sharing between the countries based on utilisation levels. Regional integration can happen gradually, but it should be aimed for from the onset of establishing the facility to guide the market and especially the necessary regulatory reforms in each jurisdiction. Fiji is an economic leader with the most existing use cases when compared to Vanuatu and other Pacific Island countries. Therefore, Fiji is best placed to also lead a regional integration and set-up discussion.

Retail payment switch potential to subsidise costs and increase efficiency through real-time payments. There is potential to integrate the ID proxy platform with the national payment system through a link with a retail payment switch. The platform and financial switch would together operate as a centralised facility that can route retail payments with a high degree of certainty as it can validate the payments channel in real time using a link to the ID proxies. The capability of the ID platform to act in concert with a financial switch would not need to be decided upfront but if the need arises, the utility can effectively support the independent routing of transactions in the financial sphere with a high level of accuracy. A switch utility could then contribute to covering the operational costs of the digital ID platform not only on direct fees but from potential financial sector efficiency gains.

Summarised insights for the governance and financial model

1. The facility needs to be regionally integrated as Vanuatu on its own is unlikely to create enough scale in a digital ID platform. The more Pacific Islands are integrated, the higher the chance of financial viability. But regional integration requires strong harmonised regulatory frameworks and increases the range of stakeholders that have to be accommodated.
2. The platform should ideally serve as a cross-cutting utility to drive scale and achieve national policy objectives and hence both private sector and public entities in addition to the Reserve Bank should be involved in design and governance. The aim is to create systemically important infrastructure.
3. Private sector entities signal interest in the utility but there are no clear signs that an entirely privately operated utility is preferred by any stakeholder.
4. A government-led, private sector-owned and operated approach could be suitable for the region if collaboration and buy-in can be ensured and if the initial funding for the set-up can be secured.
5. NGOs and development partners are well placed to assist with the set-up costs if the utility is aimed at inclusivity instead of profit maximisation. For the continuous financing of operational costs, however, stakeholders should be contractually bound to contribute to costs based on their respective efficiency cost savings, in addition to viable transaction fees and system integration costs. The aim of an NGO-led financial model would be to sustainably balance revenue and utility.
6. The utility could eventually also enable a real-time retail payment switch that can route transactions with high accuracy, which could contribute to the operational costs and overall systemic utility.

26 Adhaar in India is state-run, similar to a parastatal, i.e. a stand-alone institution. It failed to contractually bind the department responsible for managing the cooking gas subsidy to contribute to the cost of the platform and the significant cost savings reaped by that department were not, even in a small part, applied towards the sustainability of the digital ID system that made such savings possible in perpetuity.

6. Conclusion and recommendations

The objective of this digital identity platform diagnostic for Vanuatu was to establish whether the current identity landscape, the regulatory environment, existing and future use cases as well as consumers would benefit from establishing such a utility, as well as what design considerations need to be taken into account. Vanuatu, together with other Pacific Islands, could certainly benefit from a digital ID platform if its design reflects the realities of the market.

Current identity landscape

There is significant overlap in identity information collected in the five different main identity databases in Vanuatu (birth registry, national ID, driving licence register, passport register and provident fund registry), including biometrics. A clear gap in the Vanuatu identity space is the ability for third parties to verify an identity remotely, which undermines the purpose of a digital identity as it leads to the need for face-to-face validation. This is a clear value proposition of a digital ID platform. In addition, such a utility is best placed to serve as a centralised deduplication and consolidation facility that can create one robust identity for individuals as a basis for ID proxies.

Apart from ID numbers, current suitable ID proxies in Vanuatu include photographs (via facial recognition software) and QR codes embedded in the national ID card. However, significant robustness checks would need to be conducted to increase the quality of the photograph as no other biometrics, like fingerprints, are currently collected.

A big potential for the enablement of ID proxies lies in phone numbers or SIM cards as well as voice templates. SIM cards are currently not registered with an identity document and hence this integration would need to be enabled before phone numbers can be turned into ID proxies. Their potential reach is attractive and therefore this use case is strategic for the ID platform. Voice prints could also be a suitable proxy especially as they can be onboarded remotely and are particularly suitable for remote and less literate populations. Voice templates can be included in the digital ID utility.

There are still 20% of Ni-Vanuatu without access to an identity document. The excluded would need to be onboarded individually onto the platform, which needs to be taken into account when estimating the costs of the platform. Closing this gap is fundamental to the inclusivity of the platform and should be prioritised despite the cost.

Digital infrastructure

The use of mobile phones is growing and so is the digital ecosystem including mobile-accessible services. This not only creates more use cases for a digital ID platform but makes mobile phone solutions the most suitable interface to engage with the utility from a consumer perspective.

However, almost 80% of Ni-Vanuatu do not currently access the internet and hence voice or USSD solutions for identity verification should be considered on top of a 2G-enabled service. The adoption of smartphones is expected to grow over the next five years, yet basic and feature phones will still dominate the market for the foreseeable future. This further underlines the need for USSD or voice access.

Regulatory environment

To ensure trust and protect people's identities, a data protection framework is crucial to underpin a digital ID utility. The national cyber security framework that is under construction needs to be finalised still. Both should be designed with regional integration in mind as well as compliance with international norms and standards. In the absence of such frameworks, the ID platform could start operating with strict safeguards in place that could gradually become de facto compliance standards.

Given the interest and suitability of a digital ID platform for the financial sector in particular, the utility needs to comply with AML-CFT regulation as well as with regional and international norms and recommendations. Vanuatu's AML-CFT regulation lacks clarity on what constitutes a "document" for customer due diligence purposes and whether conducting these checks remotely is legal. The Financial Intelligence Unit therefore needs to issue sufficient guidance to the market in this regard to not undermine the utility of the platform as financial institutions are only using physical documents to identify and verify consumers currently to ensure compliance.

Consumer readiness

The Vanuatu population is mostly literate and is most comfortable in speaking Bislama, English and French. The utility or integration interfaces should be made accessible in all three languages and add a voice service in more languages to increase inclusivity, also for those 12% of illiterate individuals.

The digital service market is still fragile and significant trust and usage barriers still have to be overcome. Therefore, to drive uptake and scale of a digital ID solution, high-profile awareness campaigns need to accompany roll-out and should be anchored in the consumer benefits of the platform to speak to the population's needs.

Use cases

A total of 17 use cases have been identified to benefit from a digital ID platform in Vanuatu, ranging from 20 to over 15,000 estimated monthly transactions. This is a relatively low scale in terms of transactions and further underlines the need for regional integration to create

enough scale. The highest number of transactions are likely to be generated in the financial services sector, which is also high on the national priority list of Vanuatu's policies and objectives. Therefore, financial service providers, including mobile money providers, need to be prioritised for buy-in. Ideally, all use cases should be gradually integrated to create scale and make the platform a systemically important piece of infrastructure with a long lifespan.

Many civil services have already been digitised due to efforts of public authorities. It will be important to clearly show and calculate the value-add for those stakeholders to win their buy-in for integration. Where possible, the benefits of the utility should be expressed as a contributor to national policies to be taken seriously into consideration by stakeholders. Given the ongoing efforts and engagements around the relatively new national ID system, there may be fatigue and lower interest, which needs to be considered when planning stakeholder engagements.

Governance

To drive transactions on the platform and gradually prove the value to the economy, all stakeholders should be involved financially and/or in the governance of the platform. Given the need for regional integration, the Reserve Bank is well placed to lead the conceptualisation of the platform, driving regulatory reforms as well as advocate for it with private and public entities across the region to align with the other central banks. Ultimately, the platform should be run by a private provider to remain impartial as well as due to better technology capabilities, but a mix of private and public sector players should govern the utility. NGOs and development partners can assist with developing a suitable business and governance model for the platform once it has been established. NGOs could also be considered to run the platform, yet there are risks of abandonment if continuous financing cannot be ensured or if the country is locked into vendor agreements.

Financial model

The initial set-up costs could be shouldered by NGOs and development partners if the utility is aimed to be inclusive rather than having a purely profit-maximising objective. Therefore, it will be important to specify the objectives of the platform clearly from the start and gain stakeholder buy-in based on these objectives.

The initial set-up costs include the once-off integration, consolidation and deduplication of existing identity platforms, which will require considerable effort and stakeholder engagement that should not be underestimated in the cost calculations.

Entities that make use of the platform should be contractually bound to contribute to the operational costs of running the utility from the outset. This contribution can be proportional to the individual cost savings through the platform for integrated services if and when these cost savings materialise. In other words, stakeholders are expected to contribute only when the platform becomes useful to them to ensure continuous buy-in.

Financial services alone are unlikely to continuously create the necessary scale in the utility to ensure its sustainability, even if integrated regionally. While it is simpler to integrate and collaborate with fewer stakeholders, it is important to consider how to gradually integrate more services outside the financial space if this is not feasible from the outset. The digital ID platform could eventually also enable a real-time retail payments switch that can route transactions with high accuracy through the use of ID proxies. This is another potential avenue to consider in the financial model..

Bibliography

Australia Strategic Policy Institute (ASPI), 2020. *ICT for Development in the Pacific Islands – An assessment of e-government capabilities in Fiji, Papua New Guinea, Samoa, Solomon Islands, Tonga and Vanuatu*. Available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-02/ICT for development in the Pacific islands.pdf

Bali Process, 2015. *Privacy and Data Protection Laws of Bali Process Member States*. Available at: https://www.baliprocess.net/UserFiles/baliprocess/File/Privacy%20and%20data%20protection%20laws%20of%20Bali%20Process%20members%20States.pdf

Chepkemoi, 2017. *What Languages Are Spoken in Vanuatu?* Available at: https://www.worldatlas.com/articles/what-languages-are-spoken-in-vanuatu.html

Cooper, B., Ferreira, M., Janse Van Vuuren, L., 2020. *Digital Identity and Financial Inclusion: How Digitizing Customer Due Diligence Can Strengthen Providers During COVID-19 and Beyond*. Available at: https://nextbillion.net/digital-identity-and-financial-inclusion/

Cooper, B., Perez, L.M., Esser, A., Allen, M., Hlophe, N., Ferreira, M., 2019. *ID Proxy In initiatives Across the Globe: An Analysis*. Available at: https://cenfri.org/wp-content/uploads/An-analysis-of-ID-proxy-initiatives-across-the-globe_Cenfri_BankServAfrica.pdf

Cooper, B., Rusare, M., Ferreira, M., Janse van Vuuren, L., 2020. *Identity Proofing for Covid-19 Recovery: Guidance for Regulators, FSPs and Market Facilitators*. Available at: https://cenfri.org/wp-content/uploads/Identity-proofing-for-COVID-19-recovery.pdf

Daily Post, 2019. *Upgraded Passport Launched*. Available at: https://dailypost.vu/news/upgraded-passport-launched/article_39d32e43-9aa7-5c8d-a26a-992f18d8c29c.html

DigitalReportal, 2020. *Digital 2020: Vanuatu*. Available at: https://datareportal.com/reports/digital-2020-vanuatu

Financial Action Task Force, 2020. *Guidance on Digital Identity*. Available at: http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

Government of Vanuatu, n.d. *Vanuatu National Security Strategy*. Available at: https://www.gov.vu/images/publications/Vanuatu_National_Security_Strategy.pdf

GSMA, 2015. *New Data Reveals the Pace at which Global Subscribers are Moving to Mobile Data*. Available at: https://www.gsma.com/mobilefordevelopment/region/east-asia-and-pacific/new-data-reveals-the-pace-at-which-global-subscribers-are-moving-to-mobile-data.

GSMA, World Bank, 2016. *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. Available at: http://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf

GSMA, 2019. *Overcoming the Know Your Customer hurdle: Innovative Solutions for the Mobile Money Sector*. Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector-1.pdf

GSMA, 2019. *The Mobile Economy Pacific Islands*. Available at: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Pacific_Islands.pdf

GSMA, 2020. *Access to Mobile Services and Proof of Identity 2020: The Undisputed Link*. Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf

López, M.A, 2020. *Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets and Blockchain*. Available at: https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignty-digital-wallets-and-blockchain

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

Pangestu, M.E, 2020. *Harnessing the Power of Digital ID*. Available at: https://blogs.worldbank.org/voices/harnessing-power-digital-id

Reserve Bank of Vanuatu, 2015. *Financial Institutions Prudential Guideline No 9 Customer Due Diligence*. Available at: https://www.rbv.gov.vu/images/Prudential_Guidelines_for_Domestic_Banks/Prudential_Guideline_No9.pdf

Reserve Bank of Vanuatu, 2016. *Financial Services Demand Side Survey Vanuatu*. Available at: http://www.pfip.org/wp-content/uploads/2017/05/VANUATU-DSS.pdf

RNZ, 2020. *Vanuatu Set to Adopt New Cyber Crime Law*. Available at: https://www.rnz.co.nz/international/pacific-news/429717/vanuatu-set-to-adopt-new-cyber-crime-law

Standards Australia, 2020. *Pacific Islands Cyber Security Standards Cooperation Agenda*. Available at: https://www.standards.org.au/getattachment/engagement-events/international/Cyber-Security/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx

Thales, n.d. *Trusted Digital Identity*. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/id-security

Thom, M., Symington, J., Van der Linden, A., 2020. *Inclusive AML-CFT Models in Africa: Lessons from Six Financial Service Providers*. Available at: https://cenfri.org/wp-content/uploads/Inclusive-AML-CFT-models-in-Africa_Nov-2020.pdf

UNCTAD, 2018. *Republic of Vanuatu Rapid eTrade Readiness Assessment*. Available at: https://unctad.org/system/files/official-document/dtlstict2018d5_en.pdf

UNDP, 2015. *NAMA on Rural Electrification in Vanuatu*. Available at: https://www.undp.org/content/undp/en/home/librarypage/environment-energy/mdg-carbon/NAMAs/nama-on-rural-electrification-in-vanuatu.html

UNICEF, 2017. *Situation Analysis of Children in Vanuatu*. Available at: https://www.unicef.org/pacificislands/media/1281/file/Situation-Analysis-of-Children-Vanuatu.pdf

World Bank, 2014. *Digital Identity Toolkit: A guide for Stakeholders in Africa*. Available at: http://documents1.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf

World Bank, 2016. *World Development Report 2016: Digital Dividends*. Available at: https://www.worldbank.org/en/publication/wdr2016

World Bank, 2017. *The Status of Infrastructure Services in East Asia and the Pacific*. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/28954/121466-REVISED-PUBLIC-EAP-Infrastructure-Status-Final-Report.pdf

World Bank, 2018. *G20 Digital Identity Onboarding*. Available at: https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

World Bank, 2019. *ID4D Practitioners Guide*. Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide

Annex: Detailed transaction scale assumptions

High-priority use cases

Transaction scale lens

Rank	Use case	Recurring transactions per month	Once-off transactions	Growth	Assumptions (numbers multiplied to get to total figure)
1	E-commerce payments	No once-off integration	15,134	High	• In 2020, 95,000 internet users in Vanuatu. 18.7% of adults in Vanuatu have a debit card (30,892 adults) and a negligible proportion have credit cards (0.7%) (2016). • There are no internet banking figures for consumers, but since we have 8% of MSME citing they use internet banking, we use this same proportion for customers. *Calculation:* • Recurring transactions: 189,173 adults in 2020 multiplied by 8% equals 15,134 internet banking users which we use as a proxy for e-commerce users. Assuming one payment per month, monthly transactions will be 15,134. • No once-off integration
2	G2P welfare payments	10,556	10,556	Medium	• 146 beneficiaries of Home Island Passage Allowance, 959 beneficiaries of scholarship allowance, 8,159 families meet eligibility criteria for family assistance support programme. Numbers are from 2010 and add up to 9,264. Vanuatu is the world's most at-risk country for natural hazards, according to a UN University World Risk Index. There is very little public sector social assistance in Vanuatu and little that can be regarded as in-kind social assistance. Approximately 9,500 people are affected per year, but this will most likely rise. *Calculation:* • Recurring transactions: 9,264 + (9,500/12) = 10,556 • Once-off integration: 10,556
3	MTO	4,695	No once-off integration	Medium	• Remittance sending excluded, as less than 1% of the adult population send remittances abroad. All calculations below are for receiving. • 8.3% of the adult population (15+ years) receives international remittances. 59.8% of international remittances are received through MTOs. *Calculation:* • No once-off integration • Monthly recurring transactions: 165,196 (adult population) x 0.083 x 0.598 = 8,199 transactions per month in 2015. Adult population has grown by 14.5% from 2015 to 2020. Therefore 189,173 x 0.083 x 0.598 = 9,389 • Important to note that in Vanuatu remittances received from abroad most likely occur either every six months or two to three months. So, assuming the former, 9,389 / 2 = 4,695

4	Financial account opening and due diligence	4,528	61,112	Medium	• 37% of adults in Vanuatu had a bank account in 2015/2016. Multiplied by 165,196 adults in 2015 = 165,196 x 37% = 61,122 adults have a bank account. 14.5% growth in population between 2015 and 2020. That is a 2.9% growth rate each year. New customers are therefore 61,112 x 2.9% = 1,773. Due diligence assumed to occur once every three years = 61,112 / 36 = 1,698. Death rate in Vanuatu is 5.2 / 1,000 people, this is 0.52% of 89,572 = 466 deaths per annum divided by 12 = 39 deaths per month. • 20% of bank accounts not used in past 12 months. 61,112 x 0.2 = 12,222 / 12 = 1,018 *Calculation:* • Once-off integration:165,196 x 37% = 61,112 • Recurring transactions = 1,773 + 1,698 + 39 + 1,018 = 4,528 per month.

Medium-priority use cases

Transaction lens

Rank	Use case	Recurring transactions per month	Once-off transactions	Growth	Assumptions (numbers multiplied to get to total figure)
5	Tax base verification	1,834	22,000	Low	• Labour force was 110,000 in 2012 and only 20% are engaged in formal employment. Assumption: only formally employed individuals pay income tax. • Once-off integration: 110,000 x 0.2 = 22,000 • Recurring transactions: (110,000 x 20%) / 12 = 1,834
6	SIM or e-money account registration or verification	1,722	29,296	Medium	• 349,900 mobile connections in 2020 and an increase by 20,000 between 2019 and 2020 is a growth rate of 6.1%. • e-Money: only launched end of 2019, so assumption that only 1% of population has an account but high growth rates of 40%. *Calculations:* • Once-off integration: (349,900 + (165,196 x 1%)) / 12 = 29,296 • Recurring transactions: (20,000 + (1,652 x 40%)) / 12 = 1,722
7	Driving licence renewal	918	2,754	Low	• No information found. We assume that 20% of the population have a driving licence and that they renew it every three years. *Calculations:* • Once-off integration: (165,196 x 20%) / 12 = 2,754 • Recurring transactions: (165,196 x 20%) / 36 = 918

8	Criminal background checks	717	52,848	Low	• Not found, but we assume that this happens quite infrequently: 3% of the population need a criminal background check once a year. No crime stats found, so let's take Solomon Islands number and adjust for population size: 6,670 / 312,749 x 165,196 = 3,524 *Calculations:* • Once-off integration: 3,524 x 15 = 52,848 • Recurring transactions: 165,196 x 3% / 12 = 413 + 3,524 / 120 = 717
9	Voter identification	700	278,000	Very Low	*Calculations:* • Once-off integration: 278,000 registered voters in Vanuatu and elections occur every 4 years. Population growth is 2.5% and death rates are at 0.52%. • Recurring transactions: 278,000 x 2.5% + 278,000 x 0.52% = 6,950 + 1,446 = 8,396 / 12 = 700
10	Marriage and death registrations	678	50,832	Very Low	• Death rate was 5.27 per 1,000 individuals in 2018. • Marriage data not available, so we adapt Fiji to population size of Vanuatu. *Calculations:* • Marriage: (25,240 / 636,377) x 165,196 = 6,552 • Death: 5.27 x 299,882 = 1,581 • Once-off integration: ((6,552 + 1,581) x 75) / 12 = 50,832 • Recurring transactions: (6,552 + 1,581) / 12 = 678
11	School enrolment	613	88,433	Low	• 7,354 new entrants in Grade 1 in 2014 • Once off-integration: a total of 88,433 students in 2018. • Recurring transactions: 7,354 / 12 = 613
12	Birth registrations	512	245,851	Very Low	• Once-off integration: 245,851 individuals have access to their birth certificate. • Other than new births, the registry will have very few new users per month. • Population growth rate of about 2.5%. • Recurring transactions: The year 1 new users will be 6,146 per annum and 512 new users per month just from births.

13	Utility Payments	333	79,727	Very Low	• 54,985 households in Vanuatu • 45,637 households in Vanuatu with access to water • 34,090 households in Vanuatu with access to electricity • Total 79,727 • We do not assume that they would KYC for each monthly payment. • Assume 5% of base will change yearly. *Calculations:* • Once-off integration: 34,090 + 45,637 = 79,727 • Recurring monthly transactions: (79,727 x 5%) / 12 = 333

Low-priority use cases

Transaction scale lens

Rank	Use case	Recurring transactions per month	Once-off transactions	Growth	Assumptions (numbers multiplied to get to total figure)
14	Credit scoring or credit history	90	2,423	Medium	• 17.6% of adults have a credit report, up from 12.2% in 2018, which is a growth rate of 44.3%. *Calculations:* • Once-off integration: (165,196 x 17.6%) / 12 = 2,423 • Recurring transactions: (2,423 x 44.3%) / 12 = 90
15	Title deed verification and registration	30	584	Very Low	• 7,000 leases, no freehold land • Once-off integration: 7,000 / 12 = 584 • Recurring transactions: Assuming that 5% have changes: 584 x 5% = 30
16	Insurance onboarding and claims	20	8,260	Low	• Only 5% of adults having insurance which would be onboarded during the first year. Let's assume that they have one transaction per year, so onboarding number equals average transaction number. No information on insurance claims. *Calculations:* • Once-off integration: (165,196 x 5%) = 8,260 • Recurring monthly transactions = 8,260 x 2.9% = 240 / 12 = 20
17	Close foundational ID gap	No recurring transactions	46,829	Very Low	• Once-off integration: Total population is 292,680 and individuals with birth certificates is equal to 245,851. Overall, that equates to 292,680 - 245,851 = 46,829 • No recurring transactions

About UNCDF

The UN Capital Development Fund makes public and private finance work for the poor in the world's 46 least developed countries (LDCs).

UNCDF offers "last mile" finance models that unlock public and private resources, especially at the domestic level, to reduce poverty and support local economic development.

UNCDF's financing models work through three channels: (1) inclusive digital economies, which connects individuals, households, and small businesses with financial eco-systems that catalyze participation in the local economy, and provide tools to climb out of poverty and manage financial lives; (2) local development finance, which capacitates localities through fiscal decentralization, innovative municipal finance, and structured project finance to drive local economic expansion and sustainable development; and (3) investment finance, which provides catalytic financial structuring, de-risking, and capital deployment to drive SDG impact and domestic resource mobilization.

About UNDP

UNDP partners with people at all levels of society to help build nations that can withstand crisis, and drive and sustain the kind of growth that improves the quality of life for everyone. The UNDP Pacific Office in Fiji serves 14 countries and territories in the Pacific, as part of the 177-country office UNDP network, and offers global perspective and local insight to help empower lives and build resilient nations. www.pacific.undp.org


UNITED NATIONS
UNCTAD


UNDP


UNCDF
Unlocking Public and Private
Finance for the Poor