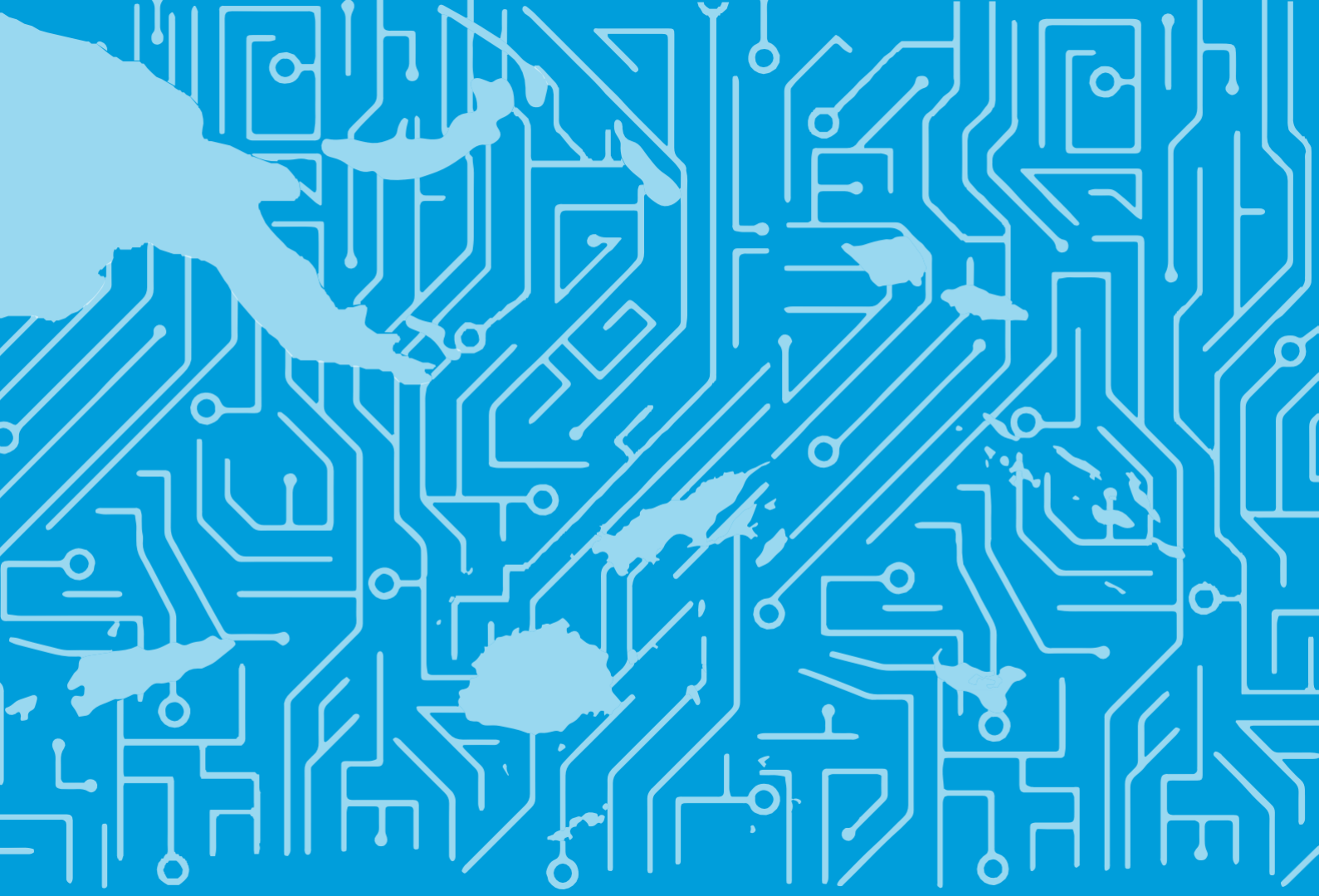
AN INCLUSIVE DIGITAL IDENTITY PLATFORM IN FIJI

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 Fiji 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
EDD	Enhanced due diligence
ESCAP	Economic and Social Commission for Asia and Pacific
EU	European Union
e-commerce	Electronic commerce
e-government	Electronic government
e-money	Electronic money
e-transport	Electronic transport
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FNPF	Fiji National Provident Fund
FRCS	Fiji Revenue and Customs Service
FSP	Financial Service Provider
FTR	Financial Transaction Reporting
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
LTA	Land and Transport Authority
MEHA	Ministry of Education, Heritage and Arts
MNO	Mobile Network Operator
MTO	Money Transfer Operator
NIBSS	Nigeria Inter-Bank Settlement System
NFC	Near-field Communication
NGO	Non-Governmental Organisation
NZ	New Zealand
PEP	Politically Exposed Persons
PFIP	Pacific Financial Inclusion programme
PFMI	Principles for Financial Market Infrastructure
PPP	Public–Private Partnership
QR	Quick Response
RBF	Reserve Bank of Fiji
RBA	Risk-based approach
RGO	Registrar General Office
SDD	Simplified Due Diligence
SDGs	Sustainable Development Goals
SIM	Subscriber Identity Module
TIN	Tax Identification Number
UN	United Nations
UNCDF	United Nations Capital Development Fund
USSD	Unstructured supplementary service data

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	SIM registration is integrated	Financial sector is integrated	Security background checks are integrated
To implement widely accessible ID proxies	Biometric photos, fingerprints are quality-checked; voice templates are added	FIU guidance on remote verification is issued	Verified phone numbers are linked
To provide the appropriate safeguards	Robust data protection and cyber security law	Targeted awareness campaigns	Clear governance and participation rules
To ease access for individuals	English, Fijian and Fiji Hindi-enabled services	USSD and voice channel access on top of 4G connections	Enable wide range of ID proxies
To ensure solid governance, inclusivity and financial sustainability	Set-up and integration costs supported by NGOs and development partners	Contractually binding stakeholders to contribute based on cost savings	Regional integration

Current identity landscape

- A digital ID platform can offer a future-proof template for the onboarding of the 29% of Fijians 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 need (digital) identity services.
- The birth registry, tax identification numter (TIN) and voter ID card have currently the highest coverage and lend themselves well to be integrated with one another via a digital ID platform. This could assist with increasing the robustness of existing identities as well as with duplication of identity information. In addition, the driving licence, passport and national provident fund databases should be integrated as all six databases have considerable overlap in the information they collect and store.
- Information in Fiji's voter database is not always up to date, especially where individuals are not proactive in changing their particulars. The drive to replace Votercard 1.0 with Votercard 2.0 could present an opportunity to update this information. A digital ID platform would help address this issue by being able to register a change in the particulars of individuals centrally and update the ledger for all connected entities in real time, so that all information is up to date across the board.
- 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.
- The planned national ID system and its progress need to be taken into account to avoid duplication efforts, especially around remote data verification capabilities.
- Facial and fingerprint biometrics show great potential as ID proxies as they are widely collected by identity providers in Fiji. 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 in Fiji, but the SIM database would need to be deduped and verified.
- While SIM plus fingerprint and/or facial recognition is more robust, a combination of SIM and voice biometrics would likely be universally accessible on the MNO networks in Fiji due to a high prevalence of basic and feature phones when compared to smartphones.

Current digital ecosystem

- Mobile phones present the obvious instrument to reach the majority of individuals with a digital ID platform given that it makes up 64% of web traffic by device. However, the utility should accommodate voice and USSD access on top of 4G channels, given that 34% of Fijians currently do not access the internet and feature and basic handsets dominate over smartphones.
- Electricity penetration is sufficiently consistent and of a high enough quality to support a digital ID platform.
- Mobile digital services are increasingly available, including e-government services like digitalFIJI, mobile merchant payments via QR codes, e-hailing platforms and food delivery services: the digital ecosystem is developing gradually, creating current future demand for a digital ID platform from a provider perspective.
- Fijians are almost universally literate, reducing the need for a voice-accessible solution suitable for illiterate individuals. Most people either speak English, Fijian or Fiji Hindi, all of which would ideally be accommodated on a digital ID solution. For those more comfortable in other languages, a voice service could be considered.
- Mobile money is rapidly gaining traction but from a low base. The DFS market is nascent and fragile. Creating trust and needs-based services, underpinned by a digital ID platform, can be a powerful driver of uptake if accompanied by awareness and usage campaigns.
- Digital services still need to prove their worth, especially among rural individuals when it comes to convenience, saving time and money. A digital ID platform could use those factors as anchors for awareness and usage campaigns.
- Data protection frameworks (i.e. measures to guard against unauthorised access to data) need further development.
- There is a need for a robust national cyber security framework to be developed. Alternatively, the cyber security standards adopted by the digital ID platform could become the de facto compliance standard and set the tone for a regulatory framework in the country.
- Technically Fiji's AML-CFT regulation allows for the use of electronic documentation in asserting the identity of an individual, suggesting that a digital ID solution could be utilised for CDD purposes. However, in practice, providers insist on paper verification.

Use cases

- There is a significant number of use cases in Fiji that could benefit from a digital ID utility.
- The highest numbers of expected monthly transactions riding on the digital ID platform are generated by financial services rather than civil services. Financial providers including mobile money schemes are therefore crucial to integrate to increase the financial viability of the platform.
- G2P welfare and pension payments (almost 134,000 monthly transactions) as well as receiving remittances via MTOs and their associated CDD practices (64,000 transactions) are both the highest use cases in terms of expected monthly transactions as well as in terms of national priority.
- Initiatives like digitalFIJI have invested significant resources to create an e-government portal to enable the remote access to services. 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.
- Ideally all use cases should be enabled by the utility. However, if prioritisation is necessary, a mix of high transaction scale, as outlined above, and high national priority (criminal background checks, tax and voter identification, marriage, birth and death registries) is possible.
- The upfront once-off integration transactions are higher than the reoccurring transactions, meaning the first step of consolidation of existing databases should not be underestimated in the design phase of the utility.

Governance and finance considerations

- The Reserve Bank of Fiji is well placed to lead the set-up of a digital ID platform given its mandate and the utility the platform would bring to the financial sector.
- However, 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 Fijian context 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.
- There is a risk that transaction scale is not high enough to cover costs in the longer-term and hence regional integration with other Pacific Island states is desirable. Regional integration requires strongly harmonised regulatory frameworks.
- The utility could eventually also enable a real-time retail payment switch that can route transactions with high accuracy and can contribute to the operational costs and overall systemic utility.

1. Introduction

Diagnostic assesses the readiness of the Fijian market 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 the Reserve Bank of Fiji (RBF) to understand and assess the use cases and ecosystem requirements for a digital identity (ID) platform in Fiji. This utility is a central repository, housing individuals' unique personal data (biographic[1] and biometric[2]) in digital form (World Bank, 2016; World Bank, 2018). A digital ID platform can be used to assert and prove an individual's identity, further discussed in Box 1 below (FATF, 2020). The ultimate objective of this diagnostic is to assess if and how the implementation of an inclusive and sustainable digital ID platform solution, tailored to the Fijian 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 are 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 in order 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

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 or linked 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 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 or onto a subsidiary database depending on how the facility is structured. Their identity data can be captured via different secure 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 fingerprints, facial and iris scans plus 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 links to identifiers by which an individual can be uniquely and exclusively 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 or linked digitally either directly on a centralised database or the digital ID platform acts as an integration layer that creates interoperability between existing secure 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).

identifiers (or ID proxies). Different types of ID proxies (such as phone numbers, biometrics, or email addresses) 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 individual's identity over time makes digital ID platforms particularly useful for financial inclusion. Twenty-three percent (23%) of Fiji's adult population (those aged 15 years and above) do not have access to formal financial services (Reserve Bank of Fiji, 2020). According to the most recent financial services demand-side survey, 17% of the unbanked adult population cite a lack of documents as a reason for not having a formal bank account (Reserve Bank of Fiji, 2015). In addition, the usage of digital financial services (DFS), while growing, remains low, with only 24% of adults having an active mobile money account in 2019 (Reserve Bank of Fiji, 2020). 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 by as much as 39%, resulting in frontline staff spending 60% less time on onboarding and ongoing due diligence processes as well as cost savings of 50% with respect to the record-keeping of documents and the storage thereof (Thom et al, 2020). This can therefore 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 Fiji.
- 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 this will determine the value they derive for 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 characterises of its population.

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, shows a photo or provides voice samples in addition to an identity reference in order 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, see 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 government, 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 transaction or payment to be conducted, a physical NFC tag on a card or adhered to 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 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 processes 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.

(continued on next page)

For example, if an individual is not able to provide a foundational ID document, they can start by getting access to limited services to limit the risk to the financial system or government service. 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 or services 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 platform. Examples of this include Nigeria's electronic ID card, 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 a 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 links to the facility or provides value-added services. An example of this approach would be a self-sovereign identity and BunkerID.

This will ensure it is designed in a way that brings sufficient value for both providers and consumers in the most cost-efficient manner. Technology should ideally be chosen only once all needs, specifications and the governance model have been established.

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 Fiji, the quality of existing identity databases in the county 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 Fiji, 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 Fiji

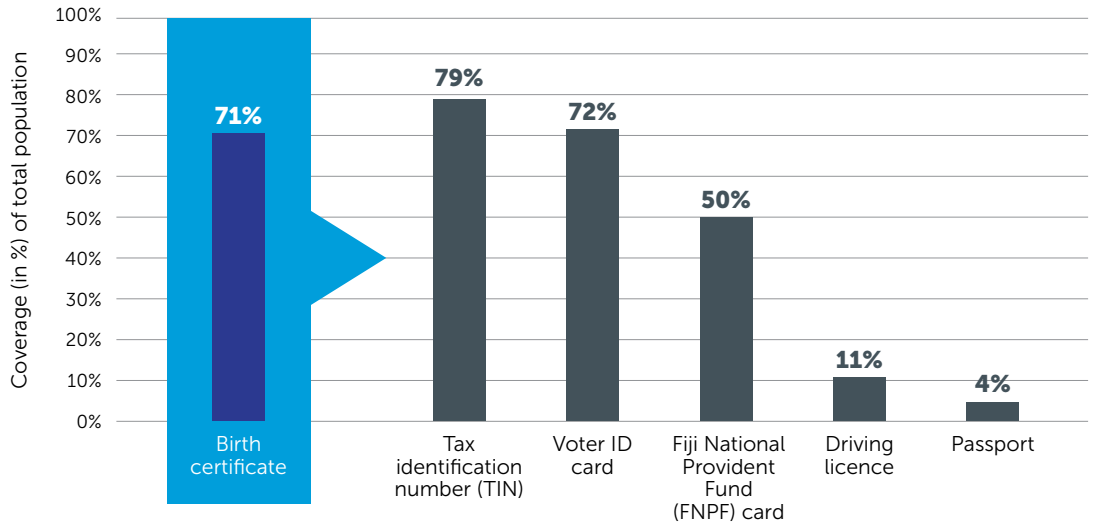
This section provides an overview of the current state of identity coverage in Fiji, the quality of existing identity databases in the country and challenges experienced in the use of these databases that a digital ID platform could help solve. It is important to understand the identity ecosystem, as 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.

Almost 30% of Fijians 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 Fiji and covers 71% of the population (around 632,000 people) as shown in Figure 1 below (Fiji Bureau of Statistics, 2017). With a birth certificate, Fijians can then access five additional, legally recognised identities[6], namely a tax identification number (TIN), a voter ID card, a Fiji National Provident Fund (FNPF) card, a driving licence as well as a passport, as shown in Figure 1. All six identity documents, either in combination with each other or individually depending on the use case, are typically accepted forms of identification to access most services in the country. This means that, legally, 29% of Fijians are currently excluded from such services and will also struggle to access any of the additional five identities[7]. In order 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 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.

The required effort to close the foundational identity coverage gap depends on the location of the excluded individuals. Approximately 87% of the population lives on the two major islands of Viti Levu and Vanua Levu (ASPI, 2020). It should be determined how many individuals that currently do not have access to a birth certificate live on these two islands as the effort to onboard them onto the platform, which is only necessary once, is relatively low compared to those individuals that live on harder-to-reach islands. 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 have as many people onboarded 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.

Considerable overlap in collected information across databases; robustness challenges exist. As Figure 1 shows, 79% and 72% of the Fijian population currently have a TIN and/or voter ID card, respectively, making these two databases the most complete in terms of coverage, apart from the birth registry, which is owned and managed by the Ministry of Justice. All five databases collect name, date of birth, address and a photo of the individual, creating substantial overlap in information, as

Figure 1. Current coverage of ID documents in Fiji



Sources: Election guide (2019), Fiji Bureau of Statistics (2017), Fiji National Provident Fund (n.d.), FRCS (2013), Land Transport Authority of Fiji (2020), Facebook (2020), Xinhuanet (2020)

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 birth certificate 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 Fijians to access services on an ad hoc basis, it presents a barrier in accessing digital services.

shown in Table 1. This overlap translates into onboarding costs for the database host that could be reduced by creating a central depository 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:

- **Duplication and inconsistencies of identity information.** Stakeholder interviews revealed a lack of linkages between the different identity databases and the duplication of information that is collected by identity providers. The information of individuals stored in these different ID databases can also be inconsistent. For example, a person can have a different name in the birth registry when compared to the driving licence database. This undermines the trustworthiness of the identifier. A digital ID platform could solve this issue by serving as a central trusted utility that consolidates identity data, which is uploaded once and updated on the central ledger. This can help create one single, robust identity per individual, which can then be easily verified either in person or remotely.
- **Lower robustness of voter ID card database.** Information in Fiji's voter database is not always up to date, especially where individuals are not proactive in changing their particulars. The drive to replace Votercard 1.0 with Votercard 2.0 could present an opportunity to update this information. A digital ID platform would help address this issue by being able to register a change in the particulars of individuals centrally and update the ledger for all connected entities in real time, so that all information is up to date across the board.
- **Third-party verification capabilities lacking.** All current identity databases in Fiji 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 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.

Birth registry, TIN and voter ID card databases to serve as starting point for digital ID platform integration due to highest coverage. The combination of birth registry, TIN and voter ID card databases would serve as a good starting point for integration with the digital ID platform. This would require collaboration between the Fiji Revenue and Customs Authority (FRCS), the Electoral Commission and Office of the Register General (RGO) in the Ministry of Justice, as hosts of the respective databases. The identity information from the FNPF database (same host as TIN), driving licence and passport can then also be used to verify the information and/or fill gaps. In addition, both the voter ID card as well as the passport databases currently contain fingerprint information that offer an important security layer in terms of biometric identification; the TIN and FNPF databases also store mobile phone numbers and email addresses, useful as ID proxies.

However, biometric information and phone numbers will likely need initial verification process to increase robustness. For biometrics 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 and

Table 1. Fiji identity database details

	TIN	Voter ID card	FNPF card	Driving licence	Passport
Stored information (overlaps)	• Full name • Date of birth • Address • Photo				
Additional useful information	• Email address • Phone number	• Fingerprint	• Email address • Phone number		• Fingerprint
Database owner	Fiji Revenue and Customs Authority (FRCS)	Electoral Commission	Fiji Revenue and Customs Authority (FRCS)	Land Transport Authority of Fiji (LTA)	Immigration Department, Government of Fiji

Sources: Bank of Baroda (n.d.) FRCS (n.d.), Immigration Fiji (n.d.), Institute for Democracy and Electoral Assistance (2017) , Naidu et al (2013), South Pacific Bank (n.d.), Stakeholder interviews (2020), UNCDF (n.d.)

fingerprint biometric templates stored in identity databases in Fiji suffer from quality issues which renders them not machine readable. In addition, given the less than robust SIM registration process, phone numbers and the identities they are linked to would have to be re-checked as explained in Box 4.

National ID including biometrics under construction; synergies need to be explored. Fiji's government has been planning a new national identification system secured by facial recognition and other biometrics since 2019, with the aim to consolidate the existing overlapping identity schemes in the country. While the status and progress of this project is unknown at present, media reports suggest it is aimed at the financial sector. It will be important to understand the planned set-up, governance and integrated use cases in detail to create synergies between the two projects and avoid duplication efforts. In particular, the digital verification possibilities of national ID information should be investigated and pushed from the Reserve Bank side to make the national ID useful for remote transactions.

Summarised insights from current identity coverage in Fiji

1. A digital ID platform can offer a future-proof template for the onboarding of the 29% of Fijians 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.
2. The TIN, voter card, FNPF, driving licence and passport databases all collect name, date of birth, address and a photo 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 depository of information in the form of a digital ID platform that every stakeholder with permission could draw on.
3. The birth registry, TIN and voter ID card databases currently have the highest coverage and lend themselves well to be integrated with one another via a digital ID platform, which could assist with increasing the robustness of existing identities as well as with deduplication of identity information.
4. Information in Fiji's voter database is not always up to date, especially where individuals are not proactive in changing their particulars. The drive to replace Votercard 1.0 with Votercard 2.0 could present an opportunity to update this information. A digital ID platform would help address this issue by being able to register a change in the particulars of individuals centrally and update the ledger for all connected entities in real time, so that all information is up to date across the board. 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.
5. The planned national ID system and its progress need to be taken into account to avoid duplication efforts, especially around remote data verification capabilities.
6. Facial and fingerprint biometrics show great potential as ID proxies as they are widely collected by identity providers in Fiji. However, 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 the SIM database would need to be deduped and verified.

Box 4: The potential of ID proxies and identity proofing in Fiji

Facial recognition, fingerprints 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. 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. Fingerprints are also widely collected and their robustness would need to be verified to ensure uniqueness. Lastly, 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[8]. Other than biometric ID proxies, mobile numbers in Fiji can be a powerful proxy given their prevalence. However, the SIM databases would need to still be deduped and verified[9]. Email addresses in Fiji are currently not linked to financial services and would first need to be verified before serving as an ID proxy.

Availability of different types of ID proxies depends on prevalence of basic and feature phones and use of voice and USSD channels. A high prevalence of basic and 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 Fiji. 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 Fiji 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 29% in Fiji 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, 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 service interactions and biometric identifiers added or linked (photos, fingerprints, voice identification templates). Voice biometrics have been identified as more important in Fiji 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. In addition, the digital ID platform could eventually be used to route payments to the appropriate channel to enable channel and instrument interoperability, i.e. link to electronic payment switch routing functionality, which could be particularly useful for a smaller economy such as Fiji and its neighbours.

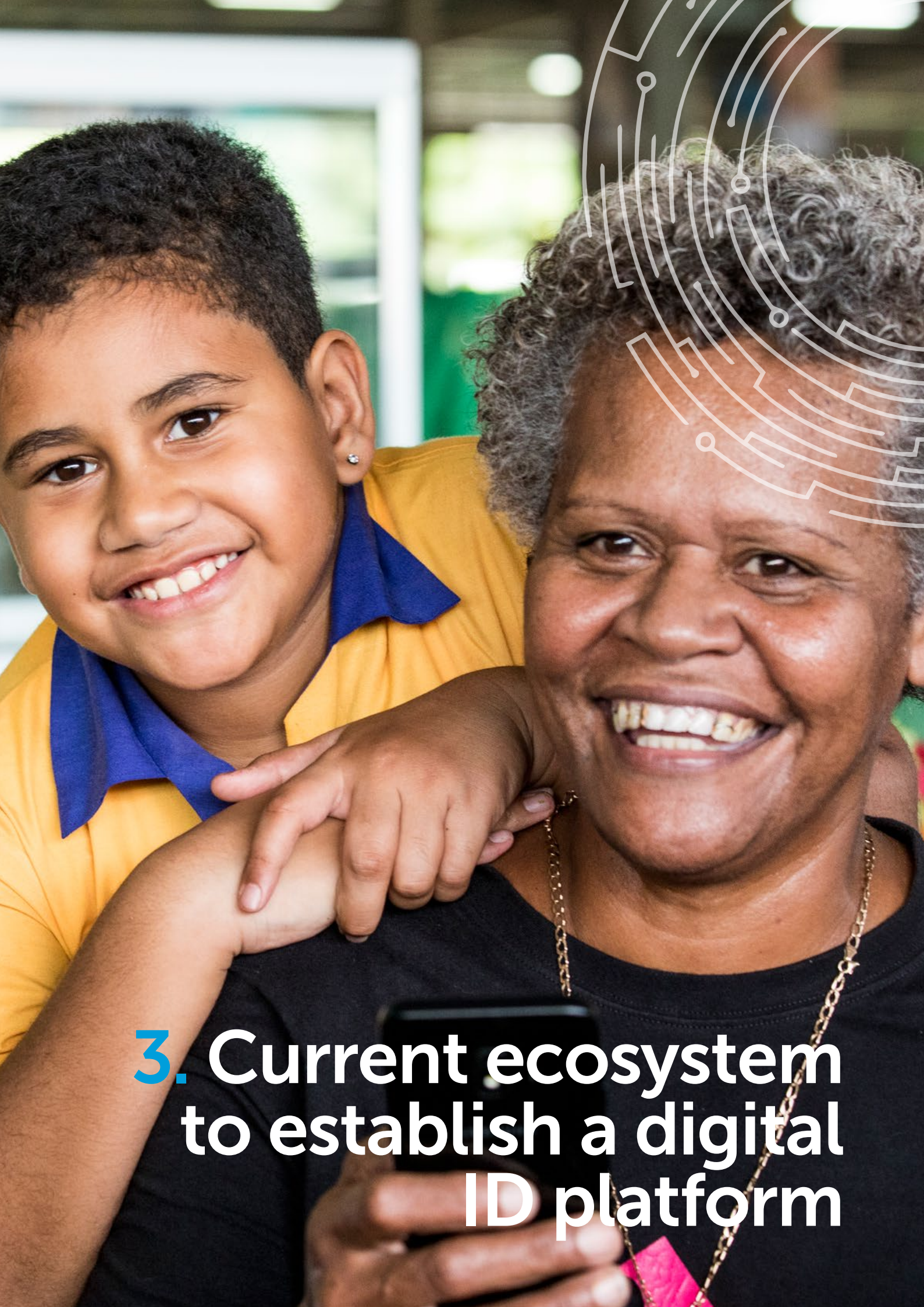
Table 2. Potential ID proxies

	TIN	Voter ID card	FNPF card	Driving licence	Passport
Potential ID proxies	TIN in combination with: • Facial recognition *or* • Phone number *or* • Email address *or* • Voice print	Voter ID card in combination with: • Fingerprint *or* • Facial recognition	FNPF 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* • Fingerprint

Sources: Bank of Baroda (n.d.), FRCS (n.d.), Immigration Fiji (n.d.), Institute for Democracy and Electoral Assistance (2017), Naidu et al (2013), South Pacific Bank (n.d.), Stakeholder interviews (2020), UNCDF (n.d.)

8 Biometric considerations: Capturing 4-4-2 fingerprints (10 fingers) as opposed to a single thumbprint is more robust. Photographs need to clearly show facial features. A lack of good quality camera 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.

9 While know-your-customer (KYC) requirements are in place for SIM registrations in Fiji and a typical customer can have two mobile numbers, stakeholder interviews revealed there is no dynamic link between a SIM card, phone number and official identity proxy. This means that SIM cards are not tied back to one central identity (i.e. each number could result in a different identity). A digital ID platform provides the opportunity to create a more robust SIM registration system by providing individuals with a unique verifiable form of ID to use during the onboarding process. This can lead to phone numbers being used as a more robust proxy ID than facial recognition and thumbprints, as the quality of these templates tend to be poorer.



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 Fiji, 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.

Fiji is the regional leader in mobile subscribers: great opportunity for scale of transactions. With 84% of subscriber penetration (770,000 unique mobile subscribers[10]), the Fijian population is the leader across all the Pacific Islands when it comes to using mobile services by a large margin (GSMA, 2019). However, as established in Section 2, individuals are currently able to use different identity documents which can contain different identity information to obtain more than the maximum two allowed SIM cards. Therefore, the share of individuals who connect to voice or data services is likely to be significantly lower than 84% of the total population[11]. Nevertheless, the high share of the population who currently access mobile services makes the mobile phone the obvious instrument to reach the majority of individuals with a digital ID platform. In addition, the high subscriber base puts Fiji at the forefront of viability of the utility given the opportunity to scale transactions quicker than its neighbours (if mobile products are well designed and meet the population's needs)[12].

Just under two-thirds of the population currently access the internet via mobile, mostly covered by 3G and 4G. 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 for the majority of the population. Sixty-six percent (66%) of Fiji's population has access to the internet (DigitalReportal, 2020). Mobile phones are the most used device when it comes to accessing the internet, making up 64% of web traffic by device in December 2019, compared to 33% for laptops and desktops and 2.6% for tablet computers (DigitalReportal, 2020). Most of those who access the internet via mobile phone are covered by 3G and 4G services (81%) with the aim to increase this to 100% 4G coverage by 2025. The prevalence of 4G connections provide service providers building products for the mobile network with sufficiently developed infrastructure to ensure a minimum quality of service[13]. Stakeholder interviews revealed, however, that connectivity can be patchy, especially in rural areas. In order to include the 50% of Fijians without access to the internet and those whose internet coverage is unreliable; a digital ID platform solution needs to be accessible by voice and unstructured supplementary service data (USSD) as well.

Smartphone penetration rising rapidly yet feature phones still dominate. Basic and feature phones still dominate even though Fiji has the second highest smartphone adoption rate in the Pacific Islands (after French Polynesia), with 43% of total connections made up of smartphones. This share is predicted to increase to 72% of connections by 2025 (GSMA, 2019). First indications suggest that the rate has accelerated during the COVID-19 pandemic and shows that mobile services running via smartphones are likely to grow over the next four years and beyond. This is likely to drive demand for digital ID solutions by both providers and consumers at similar rates, to increase value propositions and uptake. However, 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.

High electricity penetration and quality to run and access a digital ID platform. Fiji has near universal electricity coverage, with 99.6% of its population having access to electricity in 2018, well above the Pacific Island small states average of 86% (World Bank, 2020)[14].

10 Defined as a single individual 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).

11 The extent of this discrepancy could be determined once the SIM registration process is part of the digital ID platform and the identities are consolidated. It is important to have up-to-date data on the number of unique subscribers in order to understand how many people are able to directly access the information stored on the digital ID system, or indirectly through a provider's service that links to the digital ID platform. This is especially relevant in the case of self-sovereign identity models.

12 However, the subscriber base is predicted to grow by a modest 3% by 2025, highlighting the infrastructure challenges MNOs face in providing mobile services to the entire population. The currently excluded and hard-to-reach population faces being left behind (GSMA, 2019).

13 Fiji currently scores 67.7 out of 100 for network performance on GSMA's Mobile Connectivity Index, slightly above the East Asia and Pacific average of 64.4. While the latency of connections is low, meaning that the delay in the connection between signal and transmission of information is small, the relatively slow download speeds in Fiji impact negatively on the score.

14 Of the country's total population, around 80% are connected to the national grid, with the remainder utilising off-grid solutions such as diesel generators to produce electricity (Dornan, 2014; Fijian Government, 2019). The grid is relatively stable with less than 10 power outages per year, compared to an average of 134 for Papua New Guinea (World Bank, 2017).

This bodes well for consistent system functionality of a digital ID platform and ensures consumers can reliably charge their digital devices to use the platform. It also gives providers the ability to reliably integrate their databases without the risk of losing information due to systems going offline.

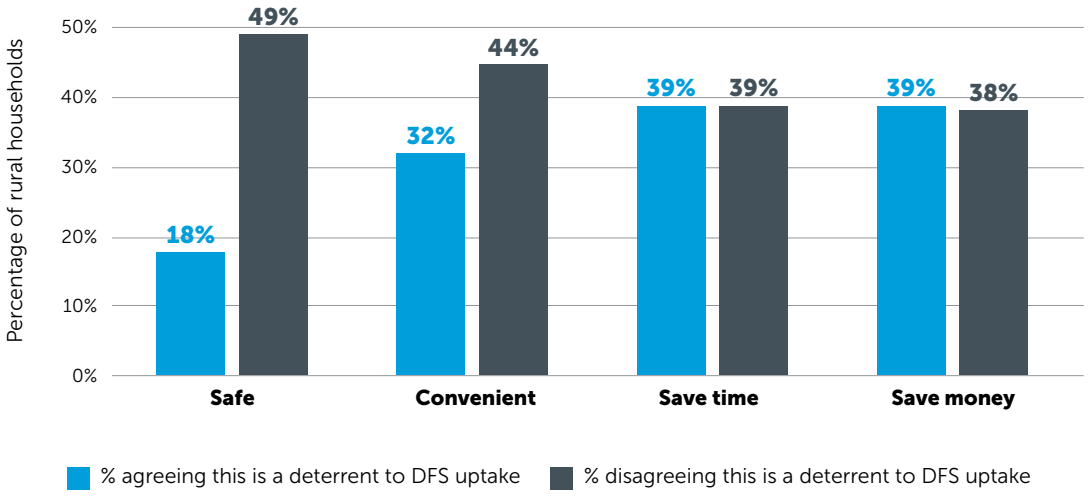
Nascent yet rapidly growing digital mobile services: potential for digital ID platform to drive uptake. The use of digital channels to access and pay for services, while still nascent, is growing rapidly in Fiji. This has been aided by the government's digitalFIJI programme, where Fijians can use a mobile app to access and pay for government services, like birth certificates, registering a business, as well as submitting feedback directly to government. Other digital channels that have seen robust growth include the use of the electronic transport (e-transport) cards to pay for public bus rides, with 1.4 million permanent cards issued since their introduction in 2017 (Nasiga, 2020). There has also been a rise in the use of QR codes to facilitate mobile retail payments, with 82 businesses and 520 outlets across the country using this channel (Ali, 2020). This indicates that the digital ecosystem is developing gradually, especially in the mobile services space, which creates an increasing number of services that could benefit from a digital ID solution. Such use cases will be discussed in more detail in Section 4.

3.2. Demand-side considerations: Are Fijians ready for a digital ID platform?

Fiji is comprised of 332 islands, of which 110 are inhabited (FAO, 2016). The country has an estimated population size of around 890,000; the second most populous in the Pacific region behind Papua New Guinea. The majority of the population (60%) is under the age of 40 (UN, 2020). This section seeks to provide an understanding of the extent Fiji's population are familiar with mobile digital services, their digital readiness in terms of literacy, trust and attitude. These factors impact the usage and ultimate viability of the identity utility.

English, Fijian and Fiji Hindi should be accommodated by a digital ID platform. Fiji has three official languages: English, Fijian and Fiji Hindi[15]. Ninety-nine percent (99%) of the country's adult population (population aged 15 years and older) are literate (DigitalReportal, 2020). Seventy-two percent (72%) of adults in Fiji are comfortable with reading and writing in English, while 77% are comfortable in a native language (Reserve Bank of Fiji, 2015). English, Fijian and Fiji Hindi should therefore be incorporated into the digital ID platform to enable its use by the majority of the country's population. A voice system embedded in the digital ID platform could be considered as it could accommodate other native languages.

Figure 2. Perceptions of main benefits of digital financial services



Source: (Finau et al, 2016)

15 There are also a number of other languages such as Rotuman, but these are used by a minority of the country's population (Nag, 2019).

Growing number of Fijians using digital channels which bodes well for ID platform uptake and usage; nascent market will need agent force to support further growth. Just under two-thirds of Fiji's population is familiar with engaging online, with 63% being active social media users (DigitalReportal, 2020). In addition to this, the use of mobile DFS has shown growth, with 24% of the adult population (those 15 years and older) having an active mobile money account in 2019, up from just 3.3% in 2018 (Reserve Bank of Fiji, 2020). This is an impressive growth rate but shows that the Fijian DFS market is nascent and hence fragile. The COVID-19 pandemic has also helped to drive growth in the use of DFS in Fiji. For example, inward remittances through mobile money platforms increased by 279% to USD50.4 million in the first ten months of 2020 compared to the same period in 2019 (RBF, 2020). Trust and consumer protection go hand in hand and it is therefore vital to increase trust in digital channels by providing a safe online identity for each person. A digital ID platform could serve as a driver of uptake of mobile services by the growing number of individuals who are already comfortable sharing their personal information online (with the adequate safeguards in place, further detailed in Section 3.3). However, providing a digital identity to those who are not yet familiar with digital services alone will likely not be enough to drive uptake. Targeted awareness campaigns linked to use cases that actually meet people's needs are necessary, which should be carried out by face-to-face agents close to the target market.

Trust as an important driver of uptake. A digital ID platform could assist with increasing the perception that using services remotely is safe and convenient if it is governed by clear consumer protection principles and data privacy laws to minimise abuse. Stakeholder interviews revealed there had been issues of trust with digital channels in Fiji in the past[16]. These incidences can have a lasting impact on people and therefore it is important to implement robust consumer protection legislation around a digital ID platform to help foster trust and facilitate adoption.

Digital ID utility would need to demonstrate to consumers increased safety and convenience, while reducing cost and saving time. Figure 2 below shows the main drivers and deterrents of DFS uptake in rural areas in Fiji. While almost 50% of rural households see the benefits of DFS when it comes to safety of transactions and accounts, other benefits common in other markets are not as clear cut. Almost a third of respondents feel DFS is inconvenient and opinions are equally divided when it comes to saving money and time via DFS (Finau et al, 2016). This shows that mobile digital services in rural areas are not yet meeting people's needs to the extent that they are convinced by its value proposition. As an example of work being done in Fiji to demonstrate the value proposition for digital services in remote areas, UNCDF has been working with Vodafone Fiji through an innovation lab focusing on improving usage and use cases for M-PAiSA (a mobile wallet) since 2017. By using M-PAiSA, people in remote areas have been able to gain access to basic financial services (for example, buying electricity, paying utility bills and topping up their e-transport card), without the need to travel to major urban centres to conduct transactions (PFIP, 2020). The value proposition of a digital ID platform therefore has to be carefully assessed to understand how awareness campaigns could be structured and to which digital service to link the utility. It would be important to emphasise how engaging online with the use of a digital ID could help individuals with regard to safety, time saving, convenience and cost during awareness campaigns.

3.3. Regulatory and policy environment

This section investigates the policy and regulatory environment in Fiji 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

Ideally define concept of identity in legislation and regulation. The concept of identity is not well defined in legislation or regulation, including norms and standards across the state and those applied within the private sector in respect of regulatory compliance. The advantage of the current approach is that innovation in the fields of identification can be readily adopted. However, the lack of harmonised approaches can lead to a proliferation of proprietary parallel systems and incompatible approaches. A diversity of approaches reduces the feasibility of integrated and interoperable unique identities that can achieve the required scale and utility to be sustainable in a smaller population. Regulated access to source codes and images could become a critical element to render biometric identifiers compatible and interoperable outside of proprietary systems that are guarded with vendor lock-in contractual clauses. Ideally the cross-cutting concept of identity, including digital identity could be framed in principle in legislation and further specified in regulation to enable innovation but maintain compatibility, utility and sustainability of identity approaches.

16 For example, there have been allegations of customer credit on electronic money (e-money) schemes and airtime balances disappearing. In addition, interviews highlighted that Fijians had negative experiences with e-commerce where money was taken but services not delivered, without an adequate mechanisms for redress.

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 protected.

Right to data privacy covered in existing legislation which could be leveraged to build a broader national framework to protection of information on a digital ID platform. Fiji's constitution provides for the right to privacy for individuals, which includes the right to confidentiality of personal information and communications (Fiji Government, 2013; United Nations ESCAP, 2016). The country's Information Act 2018[17] also deals with issues relating to the confidentiality of personal information and there are sectoral laws such as the Telecommunications Promulgation 2008[18] outlining obligations for telecommunication service providers regarding customer data privacy and consent requirements (OneTrust DataGuidance, 2020). These pieces of legislation govern how personal data is being collected, shared and used. They could serve as reference points to be used in composing national broad-based consumer data privacy frameworks to ensure strict privacy measures around information housed on a digital ID platform. If the platform is introduced without strong measures on 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 would need to be developed in light of implementation of a digital ID platform. While there is some legislation covering data privacy as mentioned above, data protection frameworks (i.e. measures to guard against unauthorised access to data) remain undeveloped (Standards Australia, 2020; ASPI, 2020). Implementing legal requirements and standards on data protection is important to safeguard against data breaches and misuse of information housed on a digital ID platform and to mitigate 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)[19], the Australian Competition and Consumer Data Right (CDR) Rules 2020[20] or more appropriate developing market examples. Putting in place adequate safeguards can help promote user trust and help facilitate adoption of a digital ID solution.

Cybersecurity frameworks under development. Fiji does not have national or sector-specific cybersecurity legislation in place; however, stakeholder interviews reveal that draft regulation on cybersecurity issues is under development[21] (Standards Australia, 2020). Existing legislation covering issues related to cybersecurity include the Crime Decree 2009[22] and Online Safety Act 2018[23]. These frameworks 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. 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 any 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.

AML-CFT regulation accommodative of a digital ID for identification purposes. Fiji's key AML-CFT law is the Financial Transactions Reporting (FTR) Act of 2004.

17 The Information Act 2018 gives individuals the right to access, make corrections to or delete incorrect personal information held by public entities. Available at: https://www.laws.gov.fj/Acts/DisplayAct/2460#.

18 This law stipulates that services providers must keep consumer information confidential and only divulge information to the "extent necessary to publish any public telecommunications directory, enable billing of the consumer or to address fraud or bad debt". Under this law, even with the consent of the customer, the disclosure of information is not permitted. Available at: http://www.taf.org.fj/getattachment/Publications/Laws---Regulations/tp2008.pdf.aspx.

19 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/.

20 This legislation was introduced to give consumers greater control over their data, which includes being able to share this data securely with a trusted third-party. It was introduced in the banking sector in July 2020, allowing consumers to choose to share their banking data in order to gain access to personalised financial products and services. Available at: https://www.legislation.gov.au/Details/F2020L00094.

21 The development of a cyber security policy and framework is stated as one of the government's goals in its national development plan. Available at: https://www.fiji.gov.fj/getattachment/15b0ba03-825e-47f7-bf69-094ad33004dd/5-Year-20-Year-NATIONAL-DEVELOPMENT-PLAN.aspx.

22 Division 6 from section 336 to 351 stipulates penalties for misuse of data held on computers. Available at: https://www.steptoe.com/images/content/2/3/v1/2393/3984.pdf.

23 The Act establishes the Online Safety Commission and is intended to promote online safety, deter harmful electronic communications including cyber-bullying and outlines criminal offences for causing harm by posting electronic communication or intimate visual recording. Available at: http://www.parliament.gov.fj/wp-content/uploads/2018/03/Bill-7-Online-Safety-.pdf.

This Act stipulates that financial institutions should use "any official or other identifying document" to identify a customer (Fiji Financial Intelligence Unit, n.d.). The definition of a "document" in the regulation specifies that this can include an electronic document (Fiji Financial Intelligence Unit, n.d.). This therefore suggests no explicit requirement for physical documents to be used for customer due diligence (CDD) by institutions and a digital ID could be used to fulfil this function and even facilitate remote onboarding.

However, specification of documents in issued guidance has led to misinterpretation: need for clarity that digital identity solutions are appropriate for CDD purposes. In practice, financial institutions are only using physical documents to identify and verify consumers. This is because AML-CFT guidelines on customer identification and verification[24] issued by Fiji's Financial Intelligence Unit (FIU) outline the specific options that financial institutions have when asserting and verifying the identity of customers, all of which are specific paper-based documents[25]. This leads to misinterpretations as to what is allowed by the FTR Act, what is outlined in guidance and what is happening in practice. There is therefore a need by regulators to issue clear guidance to institutions highlighting that digital identity solutions are appropriate for CDD under current AML-CFT regulation so long as the levels of assurance of the digital ID are proportionate to the level of risk of the customer, product or context. There is still risk that, in an effort to be conservative and avoid potential penalties, institutions will still rely on traditional documents even where digital alternatives are available and allowed. As such, buy-in from the regulator (and ideally formal acknowledgement of the digital identity for CDD) is crucial.

Summarised insights from current ecosystem in Fiji

Digital ecosystem

1. Mobile phones present the obvious instrument to reach the majority of individuals with a digital ID platform given that they make up 64% of web traffic by device. However, the utility should accommodate voice and USSD access on top of 4G channels, given that 34% of Fijians currently do not access the internet and feature and basic handsets dominate over smartphones.
2. Electricity penetration is consistent and of high quality to support a digital ID platform.
3. Mobile digital services are increasingly available, including e-government services like digitalFIJI, mobile merchant payments via QR codes, e-hailing platforms and food delivery services. The digital ecosystem is developing gradually, creating current future demand for a digital ID platform from a provider perspective.

Demand-side considerations

4. Fijians are almost universally literate, reducing the need for a voice-accessible solution suitable for illiterate individuals. Most people either speak English, Fijian and Fiji Hindi, all of which would ideally be accommodated on a digital ID solution. For those more comfortable in other languages, a voice service could be considered.
5. Mobile money is rapidly gaining traction but from a low base. The DFS market is nascent and fragile. Creating trust and needs-based services underpinned by a digital ID platform can be a powerful driver of uptake if accompanied by fit-for-purpose awareness and usage campaigns.
6. Digital services still need to prove their worth, especially among rural individuals, with regard to convenience, saving time and money. A digital ID platform could use those factors as anchors for awareness and usage campaigns.

Regulatory environment

7. Ideally define concept of identity in legislation and specify in regulation to create certainty for providers.
8. Data protection frameworks (i.e. measures to guard against unauthorised access to data) remain undeveloped.
9. There is a need for a robust national cybersecurity framework to be developed. Alternatively, the cybersecurity 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.
10. Technically, Fiji's AML-CFT framework is accommodative of utilising a digital ID solution for CDD purposes. However, guidance issued by FIU insisting on physical documentation has led to misinterpretations on what is allowed.

24 This is specified in Guideline 4 on customer identification and verification. Available at: https://www.fijifiu.gov.fj/Pages/Guidelines-and-Policy-Advisories/Guidelines.aspx.

25 This is supported by stakeholder interviews which revealed a focus on the presentation of physical documents such as birth certificates, driving licences or the TIN or FNPF cards when opening bank accounts or accessing mobile money products.

Risk-based approach to CDD in place, but reliance on physical documents hindering innovation. Fiji's guidelines on customer identification and verification further clarify that financial institutions may use a risk-based approach (RBA)[26] to customer due diligence (CDD), including simplified due diligence (SDD) for lower risk customers and enhanced due diligence (EDD) for higher risk customers. In practice, this is translating into the use of a points-based system[27], whereby institutions rate the level of assurance based on the quantity and quality of documents submitted (stakeholder interviews, 2020). While this is evidence of a risk-based approach to CDD (which is required by the FATF), institutions are constrained in their ability to innovate, as they are required to undertake CDD using documents, regardless of the risk of the customers or level of assurance provided by the identification and verification method.

Digital ID platform should also meet foreign regulations in order 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)[28]. This is important when it comes to handling foreign passport information (such as biographic and biometric data) to adequately identify and note the nationality of people in line with accepted international systems, formats and standards in place.

26 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).

27 Most banks in Fiji follow Australian regulations: the Australian Transactions Reports and Analysis Centre (AUSTRAC) guidelines for KYC involve a full 100-point check under the Australian Financial Transactions Reporting Act (FTRA). Points are allocated to types of documents used to prove identity, where an individual needs at least 100 points to be able to open an account (ACCAC, n.d.).

28 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.

4. Use case analysis

This section analyses the different use cases for digital ID in the country. Use cases in this context are the most prominent services in Fiji that currently require an identity document to be presented or verified and that would have use for a digital ID utility. Both civil and financial service use cases are assessed for challenges that 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 and national priorities.

4.1. Overview of civil and financial service use cases

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

4.2. Use case ranking

Two ranking lenses are applied in this exercise: transaction scale and 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. Fiji already has 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 a new system from the perspective of the impacted stakeholders. 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.

Table 3. Civil services use cases for a digital ID platform in Fiji

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 or information changes such as changes in address, civil status, deaths etc. to ensure up-to-date, robust information on the voter database.
Enable tax base identification and remote tax returns	Tax filing can be a time-intensive process for both citizens and tax administration and compliance issues exist both in terms of identifying who needs to pay tax and to actually file the tax return. **Solution:** A digital ID platform could enable direct access to identification documents, so they do not have to be provided by the applicant. A digital ID platform could facilitate tax filing by enabling the connection of different databases across sectors to prepopulate forms and make it easier to enforce compliance.
Enable gig employment via digital platforms	Employment opportunities increase with the expansion of digital channels. However, without digital credentials it is harder to establish a trust relationship between employer and employee, leading to less formalised employment opportunities in the digital space. **Solution:** A digital ID platform could be a catalyst for digital labour market participation by helping to streamline employee authentication, enabling contracting and facilitating employment via digital platforms.
Close foundational ID gap	Over 25% of Fijians currently do not have any form of official identity, excluding this share of the population from accessing both remote and in-person services. **Solution:** A digital identity platform could enable individuals to be onboarded onto the platform and begin the journey of having their identity verified through continuous and progressive identity proofing. Ultimately, this will enable access to services such as voting, financial services and welfare payments.

(continued on next page)

Use case	Challenge the digital ID platform could address
Enable replacement of birth certificates and centralised birth registration	It currently costs FJD10.90 to re-print a birth certificate from the digitalFIJI database and loss of documents is common. Without a birth certificate, individuals are unable to access other forms of identity documents (TIN, voter ID card, FNPF, passport, driving licence) and will be limited partially or completely in accessing basic services. **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 provide a consistent template to onboard and register new births.
Improve marriage and death registration and data sharing	Data sharing between agencies on death and marriage status information is often slow and error-prone, giving rise to the potential for fraud and identity theft. **Solution:** A digital ID platform would facilitate data sharing in real-time and allow for a centralised and unique registration of civil matters. This is crucial for having timely and accurate population information and statistics. It would enable remote access to an individual's status to enable further remote services. This would increase convenience for both consumers and providers.
Title deed registration and verification	Title deed registration and verification services consist of checking birth certificates and police clearances that need to be submitted as a form of identification and background check. **Solution:** A digital platform could enable digital title deed registration and verification services that do not require any police clearance documents or birth certificates to be submitted, as long as the title deeds, police and civil status databases are integrated and consolidated.
Enable centralised and remote criminal background check	Processes around criminal background checks are currently manual and time-consuming. Criminal background checks are conducted in the case of crimes, for enhanced due diligence of politically exposed persons (PEP), for individuals on sanctions lists, 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 a police clearance could be eliminated through real-time verification.
Enable monitoring of school enrolment	Students have to present or upload their birth certificate and their TIN letter to enrol at schools. This process is currently manual. **Solution:** A digital ID platform would allow schools to identify new pupils and allow for seamless enrolment remotely. The platform would also enable the Fiji Ministry of Education, Heritage and Arts (MEHA) to have better oversight on the education system as the platform can be used to monitor progress.
Allow for remote driving licence renewal and registration	The driving licence renewal process requires in-person presence and submissions of physical documents such as medical certificates and passport-sized photos. The additional paperwork adds to the administrative costs of the Land and Transport Authority. **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. The digital platform will also alleviate the administrative costs associated with registrations and renewals.
Link transport credit to proxy identity	The Fijian transport system relies on identity information for issuing permanent cards and requires access to additional information for subsidised cards. **Solution:** A digital ID platform would enable direct access to the information required for issuing new permanent cards and enable regular and efficient checks of subsidised cardholders.

Source: Authors' own based on literature and stakeholder interviews

Table 4. Financial services use cases for a digital ID platform in Fiji

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 and provide better levels of sectoral overarching assurance which influence international de-risking decisions[29].
Enable SIM card registration and verification and e-money registration	Fijians can currently obtain multiple SIM cards with different 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 could also provide a de facto routing of welfare payments, even for those without accounts, to enable collection via the most appropriate instrument. Through using a digital ID platform, authorities can identify affected individuals in a quick and efficient way by referencing different databases and hence channel the required support in a timely way.
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 risk profiles of institutions in respect of correspondent banking and thus encourage increased international ratings and access.
Enable access to e-commerce and expedite e-commerce payments to real-time	There is a challenge of delayed electronic payments on e-commerce platforms. In addition, the e-commerce market is limited to mainly banked customers who have debit or credit cards. **Solution:** A digital ID platform would enable real-time payments by aiding effective customer and vendor identification but also driving more e-commerce solutions. The platform would increase accessibility through allowing ID proxies which would be interoperable across payment instruments and channels to support even more e-money payments.
Enable remote utility payments	Certain utility payments can currently be made on the e-government platform, but uptake is still low. **Solution:** A digital ID platform would encourage more users to the service as they can use the identity platform for identity verification and proxy identities to pay. It would also enable utility companies to accept remote payments without needing 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. The current credit bureau is underutilised. **Solution:** A digital ID platform would allow linking an individual's identity to their credit score and credit history. Having this available to credit providers, including remote access for quick verification, would also allow for better digital credit provision.
Enable remote insurance onboarding and claims verification	Insurance penetration is low and 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

29 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.

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 certainly 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 Fiji. 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

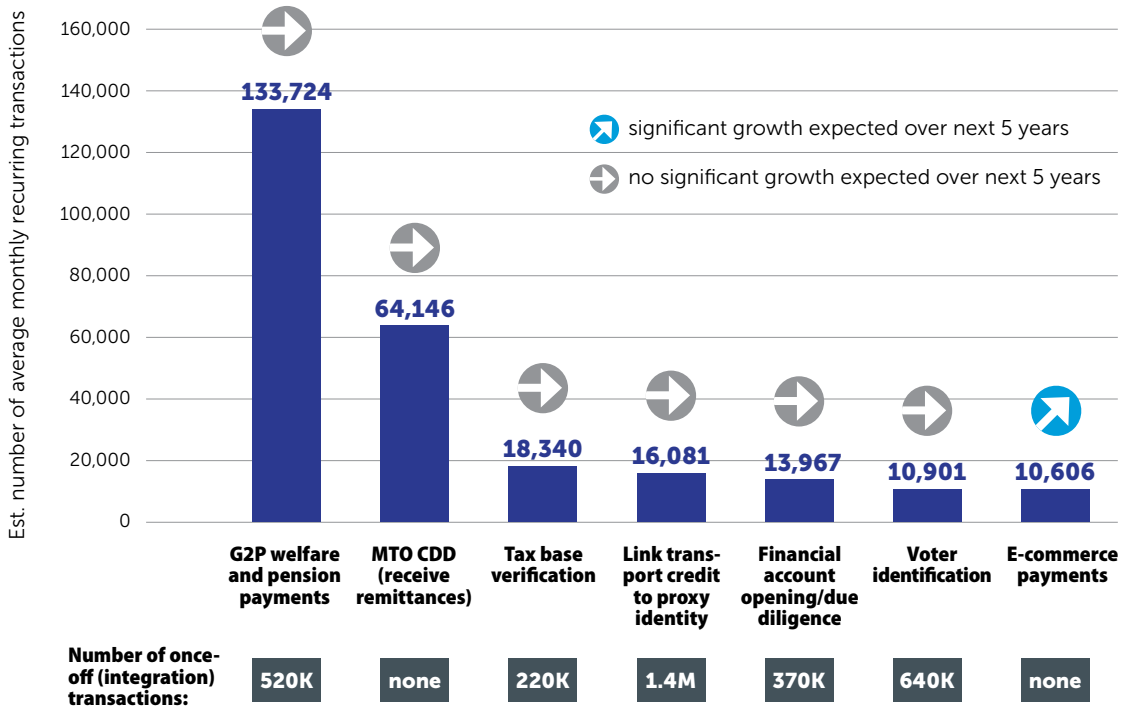
High, moderate, low priority. The ranking is divided into high, moderate and low priority integration based on the composite of several factors. These factors include the extent to which the use case was mentioned in literature or in stakeholder interviews as fulfilling a concrete need. Not every use 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 have already invested in other infrastructure to meet their needs for identity verification. For example, under digitalFIJI, several civil services are already possible digitally. 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. 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.

High-priority use cases

Financial use cases drive highest scale; national priorities overlap only to some extent. High transaction use cases, shown in Figure 3, are services that we estimate to have over 10,000 potential monthly requests to verify an individual's identity via the digital ID platform. Two financial services dwarf all others, namely the provision of G2P welfare and pension payments (almost 134,000 monthly transactions) as well as receiving remittances via MTOs and their associated CDD practices (64,000 transactions per month). In order to drive enough scale on the platform, it will therefore be advisable to integrate those two services, if possible. In terms of national priority, outlined in Table 5, both use cases are also ranked highly given their importance for the financial sector and the wellbeing of Fijians. Other high-scale use cases include tax verification, linking the transport system to ID proxies, voter identification and financial account opening. Criminal background checks and robust SIM registration to increase mobile money uptake are considered high national priorities but add a comparatively lower number of transactions to the platform. Closing the foundational identity gap does not add reoccurring transactions but is a high priority for stakeholders to increase the base for transactions and increase inclusivity.

E-commerce can drive scale in future; integration process requires rigor and proactive stakeholder engagement. In terms of growth over the next five years, only e-commerce payments show potential to increase in scale, emphasising the need to continuously build on the infrastructure to support this use case if the digital ID platform is to grow in scale. The initial number of onboarding transactions to integrate and consolidate records from existing databases are substantial, requiring a rigorous deduplication process, especially in the financial use cases. To ensure AML-CFT and financial risk is adequately mitigated to progressively turn the platform into a systemically important utility that meets

Figure 3. 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 Fiji 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.
MTO CDD (receive remittances)	The digital ID platform is a high priority to the Reserve Bank of Fiji in terms of being a significant enabler of remittances which is an important inflow that supports the welfare of many Fiji citizens. For money transfer operators, a digital platform could alleviate overly 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 Fiji, the platform is a high priority because developing a robust SIM registry system is important to mitigate AML-CFT risks arising in e-money.
G2P welfare and pension payments	For the government of Fiji, ensuring timely, well-targeted welfare and pension payments and reducing fraud risks around these payments, is important to ensure the wellbeing of Fijians.
Close foundational identity gap	The digital ID platform is a high priority to the government of Fiji to address the gap in foundational ID. A significant share of the population is not registered in any of the current databases. This gap needs to be narrowed to meet national economic and social objectives. Ideally this will already be addressed with the rollout of the new national ID that is under construction.
Criminal background checks	Given the persistent crime rate and need for integration of real-time information, the digital ID platform provides a good opportunity to enable many other use cases, especially for the Ministry of Justice.

Source: Authors' own based on literature and stakeholder interviews

national, regional and international security standards, the respective authorities need to be invested in the process and provide dedicated resources to handle the intricacies of this integration.

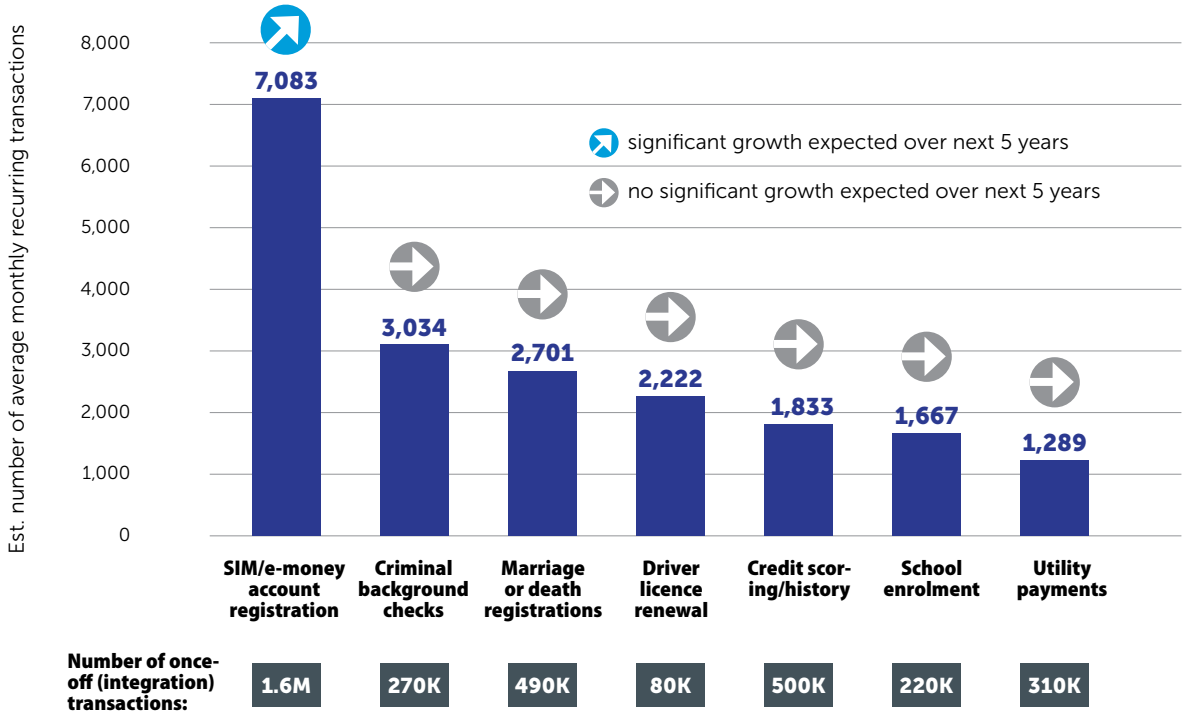
Medium-priority use cases

Civil services dominate; risk of overlap with existing services. Most use cases on the medium transaction scale (between 1,000 and 10,000 transactions) are non-financial and require buy-in from public sector institutions, as shown in Figure 4. Given the significant effort to expand e-government services via digitalFIJI that already accommodates utility payments, for example, a low-effort integration process is most desirable. If such services are not integrated to the platform, however, there is a risk of duplicating services leading to fragmentation in scale. From a financial services perspective, the MNOs would add scale if the SIM registration system could be integrated, mostly for financial services extension in mobile money. We also expect this to be the only growing use case within the next five years in this bucket, given Fiji's mobile money trajectory. Marriage and death registrations as well as school enrolment are medium priorities both from a scale and national priorities' perspective. Centralised birth registrations are vital from a national priority perspective (see Table 6), but given the constant birth rates do not add significant scale to the utility.

Low-priority use cases

Lower buy-in expected from stakeholders where existing systems already well-established. Low-scale use cases are shown in Figure 5 and would contribute less than 1,000 transactions a month to the digital ID utility. Similar to e-commerce payments, digital platform employment is the only growth use case while insurance, birth registrations and title deed verification services are unlikely to grow significantly over the next five years. In the national priority ranking (Table 7), we mostly observe use cases that are already built around an electronic database, such as credit history and the e-transport card system. As these services seem to be working relatively seamlessly, extra effort will be required to convince stakeholders and database owners to integrate with the new utility.

Figure 4. Medium-scale transaction use cases



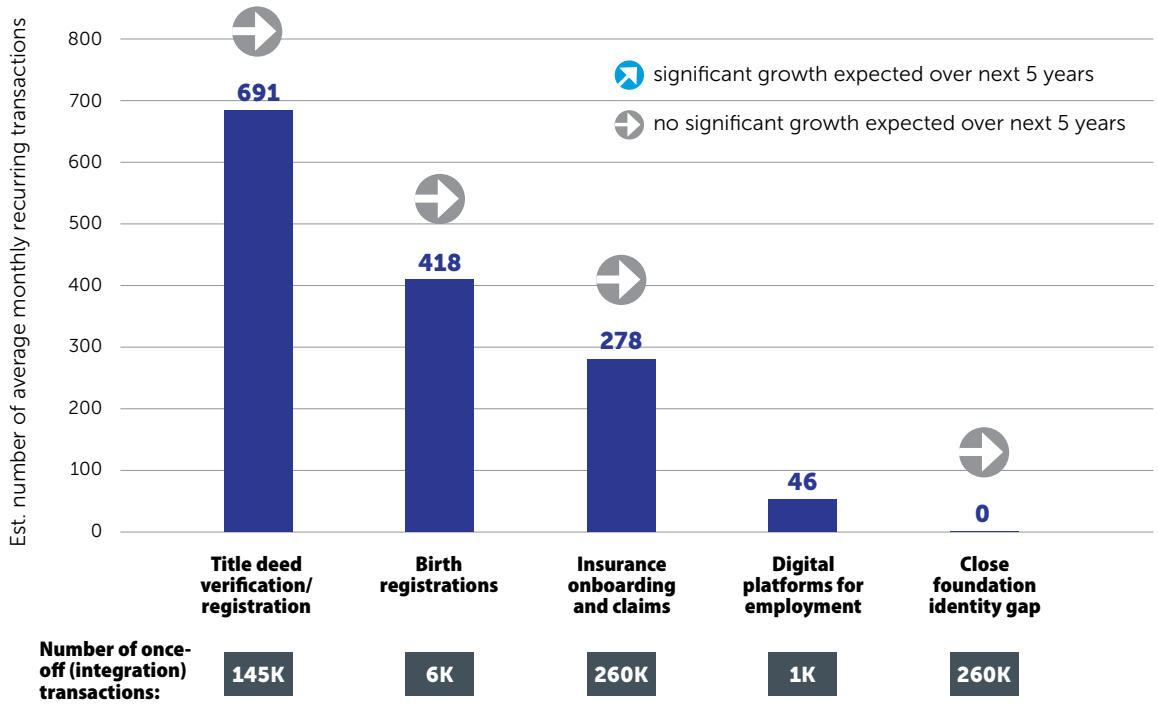
Source: Authors' own based on literature and stakeholder interviews

Table 6. Use cases with medium national priority

National priority lens	
Use case	**Considerations**
Birth registration	Using the digital ID platform for birth registration is a medium priority as a system already exists, but is a value-add to the Fiji Ministry of Justice and Fiji Ministry Health to keep a centralised account of new births that other providers can access. For the Fiji Bureau of Statistics, the platform serves a tool to accurately analyse and estimate population information.
Marriage and death registrations	For the Office of Civil Registry, the platform will 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.
Voter identification	Using a digital ID platform for voter identification is a medium priority given the existing system, but is added-value to the elections office as it ensures a more up-to-date voter registry and reduces the risk of electoral fraud.
Tax base verification	The digital ID platform enables the Fiji Customs and Revenue Authority to maximise tax collection and improve efficiency. There is a system already in place, so would need to get buy-in.
E-commerce payments	Using a digital ID platform for e-commerce payments is a medium priority as the e-commerce sector is still nascent. The Fijian 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.
Digital platforms for employment	Using a digital ID platform for gig employment is a medium priority given the currently low uptake of such a service. However, it is a value-add to Fiji's emerging digital platform economy with growth and employment potential.
School enrolment	Using a digital ID platform for school enrolment is a medium priority given the already high rate of enrolment. The Ministry of Education can particularly benefit from being able to accurately account for enrolled students and school-age children that are not in school. The data on the platform is also helpful to the Ministry of Education for budgeting purposes.

Source: Authors' own based on literature and stakeholder interviews

Figure 5. 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**
Utility payments	Given the high access to water and electricity, enabling utility payments is a low priority. The Fiji Water Authority and Energy Fiji Limited could, however, see long-term benefits from digitised utility payments as a result of the platform.
Credit scoring and history	Given the existence of a credit bureau, credit scoring and history are a low priority for the digital ID platform. The inclusion of biometrics and proxy IDs in the platform may, however, benefit the existing bureau in improving the quality of credit scoring and history in Fiji.
Driving licence renewal	Given the low driving licence uptake and that the licence renewal process is already digital, this use case is a low priority for the digital ID platform.
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 Fiji.
Replace transport cards with ID proxy	Using the digital ID platform for replacing transport cards with ID proxies is a low-priority use case, given that the current system is working well.
Title deed verification and registration	Using the digital ID platform for title deed verification and registration is a low priority, given that this system is already digitised.

Source: Authors' own based on literature and stakeholder interviews

Summarised insights from use case analysis

1. There are a significant number of use cases in Fiji that could benefit from a digital ID utility.
2. The highest number of expected monthly transactions riding on the digital ID platform are generated by financial services rather than civil services. Financial providers, including mobile money schemes, are therefore crucial to integrate within the system to increase the financial viability of the platform.
3. G2P welfare and pension payments (almost 134,000 monthly transactions) as well as receiving remittances via MTOs and their associated CDD practices (64,000 transactions) are both the highest use cases in terms of expected monthly transactions as well as in terms of national priority.
4. Initiatives like digitalFIJI have invested significant resources to create an e-government portal to enable remote access to services. 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. Ideally, all use cases should be enabled by the utility. However, if prioritisation is necessary, a mix of high transaction scale and high national priority has the best prospect of success.
6. 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 provide the template for onboarding and it will be crucial to bring more people into the formal system to generate scale and improve inclusion.

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 ensure 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 Fiji. Table 8 lists the advantages, disadvantages and implications for Fiji of each of the four governance models introduced in Box 3.

Public–private partnership and NGO-led model more suitable for Fiji context but risks of abandonment arise. All four models are technically possible in Fiji, yet the advantages outweigh the disadvantages in a government-led but private-sector-owned and operated initiative, as well as the NGO-led model. There are strong signs of buy-in from the Reserve Bank of Fiji given the utility of the platform in the financial sector. Applying the use case analysis above to governance configurations, financial use cases are projected at 90,000 to 100,000 transactions per month which would realistically be insufficient to support a modest platform and hence not very likely to bring the desired benefits to Fiji's national objectives. A limited and underfunded platform is likely to remain below its utility potential, with a risk of abandonment. An NGO or development partner-led model has a good chance of gaining scale through brokering engagements across government service departments as well as across market stakeholders, even across regions, but also runs the risk of abandonment if NGO-based funding is not consistent over the development phase. Their not-for-profit nature ensures that there is no commercial interest that risks excluding segments of the population.

RBF to lead utility in terms of advocacy and governance given high utility in financial sector. The Reserve Bank's role in establishing this utility at the first instance is advocacy. Financial institutions as well as MNOs, other government departments and teams within the Reserve Bank need to be convinced through clear mapping of policies and national objectives and benefits the digital ID platform could bring. The Reserve Bank is well placed to act as an arbiter and governor of the digital ID platform framework. It has the adequate mandate to build the utility in agreement and supervisory interventions so there is real substance behind this endeavour. Depending on the relationship with other regulators and private-sector buy-in, especially from MNOs, a top-down approach in terms of governance led by the Reserve Bank could function well if underpinned by clear participation and governance rules to avoid abuse.

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 maintain momentum. Given the potential 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 Fiji's regulatory reforms, if possible. 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 Fiji 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 transform Fiji's ability towards 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. The Reserve Bank has the analytical capacity to lead such an exercise.

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 Fiji. By its nature, an NGO model would have an

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 and 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 • Access to advanced resources, skills and capacity to implement and operate at scale with remote and/or local 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 and 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 • 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 • Potential 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	• Higher 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 • Key business case focus on included middle and higher-income consumers with less focus on lower-income and hard-to-reach segments • Competition principle can result in competing commercial offerings by multiple platforms, reducing scalability and reach • 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 • High potential for vendor lock-in agreements to suboptimal facility or excessive default cost guarantees • Changes in government policy and commercial considerations need to be proactively managed • Potential for vendor or private sector abandonment	• 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 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 Fiji

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 suitable in Fiji given the current pace of development and the capacity in government • Will be difficult to coordinate between departments and would increase pressure on existing projects	• Fiji has the type and quality of institutions that would be capable of implementing and operating such a facility, but they view it as a non-core activity • 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	• Fijian government has the capacity to co-ordinate or lead such an approach and it could link in with existing policy initiatives • 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 • A model similar to NPS licensing, governance and operation loosely aligned with but not subject to the PFMI principles similar to the BVN run by NIBSS owned by banks in Nigeria and run under the auspices of the Banking Council, including the Central Bank	• 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

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 Fijians 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.

Operational costs

Financial contributions to platform to be set out upfront. In order 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, but the platform should not be free to use indefinitely[30].

Build for regional integration. On their own, the expected monthly transactions running through the platform in Fiji are quite low, despite being in the top across the region. This has implications for the sustainability of the 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 into neighbouring jurisdictions and ideally 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 outset 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 the other two countries in this series, namely Vanuatu and Solomon Islands. 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.

30 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.

Summarised insights for the governance and financial model

1. The Reserve Bank of Fiji is well placed to lead the set-up of a digital ID platform given its mandate and the utility the platform would bring to the financial sector.
2. However, 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 apart from 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 Fijian context 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. There is a risk that transaction scale is not high enough to cover costs in the longer term and hence regional integration with other Pacific Island states is desirable. Regional integration requires strongly harmonised regulatory frameworks.
7. The utility could eventually also enable a real-time retail payment switch that can route transactions with high accuracy and contribute to the operational costs and overall systemic utility.

6. Conclusion and recommendations

The objective of this digital identity platform diagnostic for Fiji was to establish whether the current identity landscape, regulatory environment, existing and future use cases and consumers would benefit from establishing such a utility, as well as what design considerations need to be taken into account. Fiji 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 six main identity databases in Fiji, including biometrics. A clear gap in the Fijian 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 for 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, suitable ID proxies in Fiji include mobile phone numbers as well as fingerprints and facial recognition. However, significant robustness checks would need to be conducted to increase the quality of biometrics as well as phone numbers and SIM cards. Voice templates could also be a suitable proxy, especially as they can be onboarded remotely and are particularly suitable for remote and less literate populations.

While penetration of foundational IDs is widespread, there are still 29% of Fijians without access to an identity document. The excluded people would need to be onboarded individually onto the platform, which needs to be taken into account when estimating the costs of the platform. Given that discussions around a new national ID scheme which includes higher-quality biometrics are under way, it is crucial to align the two projects to create synergies and avoid duplication.

Digital infrastructure

Mobile phones are widely used and given the high 4G coverage across the country, the digital ecosystem is developing gradually at one of the highest paces across the region. This not only creates more use cases for a digital ID platform, but it makes mobile phone solutions the most suitable interface to engage with the utility from a consumer perspective. However, only 40% of Fijians currently access the internet and hence voice and USSD solutions for identity verification should be considered on top of a 4G-enabled service. The adoption of smartphones is expected to grow considerably over the next five years, but basic and feature phones still dominate the market. This further underlines the need for USSD and voice access.

Regulatory environment

To ensure trust and protect people's identities, a data protection framework is crucial to underpin a digital ID utility. In addition, a robust national cybersecurity framework needs to be developed. 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. Fiji's AML-CFT regulation already allows for the use of electronic documentation in asserting the identity of an individual and so technically there is no barrier in allowing providers to conduct remote customer due diligence. In practice, however, financial institutions are only using physical documents to identify and verify consumers to ensure compliance and there is alignment around in-person customer due diligence without reference to any specific risk mitigation. Therefore, it is necessary to have strong buy-in from the FIU to issue guidance on remote customer due diligence without the need for physical document verification.

Consumer readiness

Fijians have a high rate of literacy and are increasingly comfortable with using internet services. Most people either speak English, Fijian or Fiji Hindi. The utility or integration interfaces should be made accessible in all three languages and add a voice service in more languages to increase inclusivity.

Even though digital services such as e-government, e-hailing, e-commerce and mobile money are on the rise, the market is still fragile and building consumer trust is crucial. Rural individuals in particular still need to be convinced by the value proposition of digital services with regard to cost, time savings and convenience. 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 benefits of the platform to speak to the population's needs.

Use cases

A total of 19 use cases have been identified to benefit from a digital ID platform in Fiji, ranging from less than 100 to over 130,000 estimated monthly transactions. The highest number of transactions are likely to be generated in the financial services sector, which is also high on the national priority list in Fiji'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 the 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. The ongoing efforts and engagements around a new national ID system may lead to fatigue and lower interest, which needs to be considered when planning stakeholder engagements.

Governance

In order 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. 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. Ultimately, the platform should be run by a private provider to remain impartial and benefit from 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 or the platform, one which stakeholders can be part of once the utility 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 or development partners if the utility is aimed to be inclusive instead of 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. 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. Regional integration could create the necessary scale, although Fiji would be considered one of the top contributors in terms of transactions. The digital ID platform could eventually also enable a real-time retail payment 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

Ali, F.B., 2020. *Five New Companies Sign Up for M-PaiSA QR Pay*. Available at: https://www.fijivillage.com/news/5-new-companies-sign-up-for-M-PaiSA-QR-Pay-r84xf5/

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

Cava, L., 2020. *Re-registration of Voter IDs: Frustration over FEO's New Move*. Available at: https://www.fijitimes.com/re-registration-of-voter-ids-frustration-over-feos-new-move/

Cooper, B., Ferreira, M., Janse Van Vuuren, L., 2020. *Digital Identity and Financial Inclusion: How Digitising 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 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

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

Dornan, M., 2014. *Access to Electricity in Small Island Developing States of the Pacific: Issues and Challenges*. Renewable and Sustainable Energy Reviews, 31, 726-735

Fiji Bureau of Statistics, 2017. *Provisional Vital Statistics 2010-2014*. Available at: https://www.statsfiji.gov.fj/index.php/latest-releases/vital-statistics/815-provisional-vital-statistics-2010-2014

Fijian Government, 2019. *More Homes Get Connected to the Electricity Grid*. Available at: https://www.fiji.gov.fj/Media-Centre/News/MORE-HOMES-GET-CONNECTED-TO-THE-ELECTRICITY-GRID

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

Food and Agricultural Organisation (FAO), 2016. *Country Profile: Fiji*. Available at: http://www.fao.org/3/ca0385en/CA0385EN.pdf

GSMA, 2015. *New Data Reveals the Pace at which Global Subscribers are Moving to Mobile Data*. Available at: 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: 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: www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Pacific_Islands.pdf

Institute for Democracy and Electoral Assistance, 2017. *Introducing Biometric Technology in Elections*. Available at: www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.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

Mastercard, 2014. *Mastercard-branded National eID Card Launched in Nigeria*. Available at: https://newsroom.mastercard.com/mea/press-releases/mastercard-branded-national-eid-card-launched-nigeria

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

Nag, O.S, 2019. *Languages of Fiji*. Available at: https://www.worldatlas.com/articles/languages-of-fiji.html

Naidu, S., Buttsworth, M. Aumua, A., 2013. *Strengthening Civil Registration and Vital Statistics Systems in the Pacific: The Fiji Experience*. Available at: https://unstats.un.org/unsd/vitalstatkb/KnowledgebaseArticle51023.aspx

Nasiga, L., 2020. *e-Transport Cards in Sufficient Supply*. Available at: https://fijisun.com.fj/2020/02/25/e-transport-cards-in-sufficient-supply/

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

PFIP, 2020. *Managing a Mobile Money Agent Network in Fiji*. Available at: https://www.uncdf.org/managing-a-mobile-money-agent-network-in-fiji

Reserve Bank of Fiji, 2015. *Financial Services Demand-Side Survey: Republic of Fiji*. Available at: http://www.pfip.org/wp-content/uploads/2016/08/Fianancial-Services.pdf

Reserve Bank of Fiji, 2020. *2019 Financial Inclusion Report*. Available at: www.rbf.gov.fj/wp-content/uploads/2020/08/Fiji-Financial-Inclusion-Annual-report-2019.pdf

Reserve Bank of Fiji, 2020. *International Remittances and Fiji's Unsung Heroes Abroad*. Available at: https://www.rbf.gov.fj/international-remittances-and-fijis-unsung-heroes-abroad-24-december-2020/

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: 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

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-practitioners-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	G2P welfare and pension payments	133,724	519,175	Low	• Each monthly payment will require KYC verification as a background check via the digital ID platform and number of social welfare payments recipients is 77,512. In addition to these recipients, we also count in natural disaster assistance payments. The Fijian Government identified 71,700 people needing support in 2016 after Cyclone Winston. Assuming a natural disaster like that happens every three years and this requires a once-off check of people in the different databases and on whether they stay in affected regions. • Growth: there has been quite a high growth in number of welfare payment recipients in the past which went up from 42,848 in 2015 to 77,512 in 2020. This will most likely not continue, but natural disaster risk will most likely be increasing due to climate change. *Calculation:* • (71,700 / 36) = 1,992 • Once-off integration: 77,512 • Recurring transactions: 77,512 + (71,700 / 36) = 79,503
2	MTO CDD (receive remittances)	64,146	No once-off integration	Very low	• Remittance sending excluded as less than 1% of the adult population send remittances abroad. All calculations below are for receiving. • 14% of the adult population (15+ years) receive international remittances. 72% of international remittances are received through MTOs. *Calculation:* • 609,366 (adult population) x 0.14 x 0.72 = 61,424 transactions per month in 2015. • Adult population has grown by 4.4% from 2015 to 2020. Therefore, 636,377 x 0.14 x 0.72 = 64,146 people receive remittances. • One transaction per month usually based on the Fiji demand-side data.

3	Tax base verification	18,340	220,080	Low	• Size of labour force is 366,800; tax reports are submitted once a year and assumption is that the number of taxpayers is relatively constant and that each year the persons need to be verified and around 60% of Fiji's workers were in informal employment and not contributing to the Fiji National Provident Fund (FNPF) in 2010/11. The assumption is that only formally employed persons pay income tax. • Growth: There might be a slow increase if the economy becomes more formal. *Calculation:* • Once-off integration: 366,800 x 60% = 220,080 • Recurring transactions: (366,800 x 60%) / 12 = 18,340
4	Link transport credit to proxy identity	16,081	1,400,000	Very low	• So far, 1.4 million permanent e-transport cards have been issued to the public; 61,644 are subsidised for students which would have to be checked regularly (assumption every half a year); also need to estimate how many existing cards get lost and then how many new ones there might be each year. *Calculation:* • Once-off integration: 1,400,000 / 12 = 116,667 • Recurring transactions: 61,644 / 6 = 10,247 for the subsidised ones and then assumption is that 5% of stock gets newly issued each year: 70,000 / 12 = 5,834 which makes 10,247 + 5,834 = 16,081
5	Financial account opening and due diligence	13,967	368,463	Low	• In 2016, there were 368,463 bank accounts in Fiji. In terms of new accounts, we assume a 1% increase in accounts (which is roughly similar to population growth at 0.88%). The crude death rate in Fiji is 0.83% of the population. If this rate applies to the financially included customers, customer death is equivalent to: 368,463 x 0.83% = 3,058 / 12 = 255. Customer churn in Fiji is around 3-6% on SIM cards per month. Assuming this does not mean that these customers necessarily inform the bank of phone number changes and it is possible that main phone numbers are maintained while back-up numbers are recycled. We therefore do not take this into account. We do double the initial onboard transactions to account for at least 1 information change per customer. • Once-off integration: 368,463: once-off integration of existing database into digital ID platform • Recurring monthly transactions: STR = 459 / 12 = 138; new accounts = 368,463 x 1% = 368; deaths = 368,463 x 0.83% = 255; due diligence = 368,463 / 36 = 10,235; 12% of Fijians used to have an account. Assuming a 10% customer churn = (368,463 x 10%) / 12 = 307, so: 138 + 368 + 255 + 10235 + 3071 = 13,967 recurring account openings per month
6	Voter identification	10,901	637,527	Very low	• Once every four years the voters' details will be required. In the previous elections there were 637,527 registered voters. Assuming the same voters vote and new voter growth is in line with population growth. Population growth among adults was 4.4% between 2015 and 2020. So, assuming the voter population grows by 0.88% each year for four years, the voter numbers will be 658,174. Divide by 12 to get the monthly average = 54,848. Assuming Year 1 is a voting year, they will onboard 658,174 and after that, there won't be any transactions. • Once-off integration: 637,527 • Recurring monthly transactions: 637,527 x 0.83% death rate = 5,291 + 5,610 (new voters – 637,527 x 0.88%) = 10,901

7	E-commerce payments	10,606	No once-off integration	High	• 586,000 internet users in Fiji. 47.% of the Fiji population are debit card users (287,620 adults). Internet banking transactions in 2019 amounted to 1.8 million transactions per annum. 2015/2016 figures indicate that internet banking is used by 8.10% of the adult population (49,359 adults in 2015/2016). Assuming that the % of adults using internet banking is around 10% in Year 1. We can say that 10% of 636,377 (adult population in 2020) is 63,638 (internet banking users). Divide 1.8 million transactions by internet banking users (63,638) and divide by 12 is 2.333 which is between 2-3 transactions per month (using 2 as our conservative estimate). • Growth: We saw a 13% growth in volumes between 2017 and 2018. Growth should be 10% to 15%, we take the conservative 10%. • Recurring monthly transactions: Taking the number of internet banking users 63,638 multiply by 2 transactions divided by 12 to get monthly and we have 10,606 potential monthly e-commerce transactions.

Medium-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)
8	SIM and e-money account registration	7,083	1,585,332	Moderate	SIM cards: 770,000 unique subscribers in 2018 and 1.24 million mobile connections in 2020. • Growth: The number of mobile connections in Fiji increased by 47,000 (+4.0%) between January 2019 and January 2020. *Calculation:* • Once-off integration: 1,240,000 / 12 = 103,334 • Recurring transactions: 47,000 / 12 = 3,917 • Growth in e-money accounts: there were 345,323 registered mobile money accounts in 2019 • Growth: growth rate is 11% *Calculation:* • Once-off integration: 345,323 / 12 = 28,777 • Recurring transactions: (345,323 x 11%) / 12 = 3,166
9	Criminal background checks	3,034	271,920	Low	• Assuming that 3% of the population need a criminal record once a year. 18,128 crimes in 2017 would require background checks and then assuming that 3% of the population need a criminal background check once a year. *Calculation:* • Once-off integration: 18,128 x 15 = 271,920 (accumulation of records over the past 15 years) • Recurring transactions: (18,128) / 12 + (609,366 x 3%) / 12 = 3,034

10	Marriage and death registrations	2,701	486,135	Very low	• Average death rate from 2015-2017 was 7,169 and there have been 25,240 new registered marriages in 2013. Assumption is that this does not really change over time, so just adding up these two numbers and dividing them by 12. Then for the first year, there will be a once-off integration of existing records into the digital ID platform. *Calculation:* • Once-off integration: ((25,240 + 7169) x 15) = 486,135 (calculation of stock that accumulated over last 15 years) • Recurring transactions: (25,240 + 7,169) / 12 = 2,701
11	Driving licence renewal	80,000	2,222	Very low	• Currently over 80,000 people have registered, renewal is every 1-5 years, assuming on average every three years. *Calculation:* • Once-off integration: 80,000 / 12 = 6,667 • Recurring transactions: 80,000 / 36 = 2,222
12	Credit scoring and history	499,681	1,833	Low	• 82.4% of the adult population have a credit record, up from 78.9% • Growth rate in credit information is 4.4% and growth in credit is unlikely to be high as this would require significant changes in the credit landscape. *Calculation:* • Once-off integration: 609,366 x 82.4% = 499,681 • Recurring transactions: 502,118 x 4.4% = 1,833
13	School enrolment	216,553	1,667	Low	• In Year 1, the initial total to onboard would be 146,975 registered primary school students and 69,578 registered high school students in 2016. Adding the two gives us 216,553. In 2016, there were 20,404 new first graders in Fiji. Between 2015 to 2020 there was no growth in the age 6–9 group in Fiji. • Once-off integration: 216,553 • Recurring transactions: We assume that that new school entrants will be roughly 20,000 per year divided by 12 = 1,667 average monthly transactions.

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)
15	Title deed verification and registration	691	144,677	Very low	• Once-off integration: 18,000 state land parcels captured. • According to the 2017 census, 35,797 people had freehold land; 26,164 are leasing from the government; 38,502 are leasing from the iTaukei land trust board (TLTB); • 31,939 and 20,985 people occupy land through the traditional village tenure and through traditional ownership (Mataqali Tokatoka Yavus) respectively. • Recurring transactions: Total number of leases, approval notice of lease, tenancy at will, variation of lease, re-entry, licences prepared: 4,470; consent to transfer, mortgage, sub-letting, caveat, subdivision, build, legal proceedings, evict, connect, water meter, connect electricity, re-zoning: 3,816 *Calculation:* • Once-off integration: (18,000 + 35,797 + 38,502 + 31,393 + 20,985) = 144,677 • Recurring transactions: (4,470 + 3,816) / 12 = 691
16	Birth registrations	418	627,272	Very low	• 627,272 have birth certificates. Other than new births, the birth registry will have very few new users per month. Population growth rate of about 0.8%. The Year 1 new users will be 5,018 per annum and 418 new users per month just from births. In Year 2, 421 new users per month from births. *Calculation:* • Once-off integration = 627,272 • Recurring transactions: 627,272 x 0.8% = 5,018 / 12 = 418
17	Insurance onboarding and claims	287	260,914	Low	• In 2018, there were 837 insurance claims. In 2019, 41% of adults have insurance which is equivalent to 260,914 adults. Since there was initial growth between 2017 (19.75%) and 2018 (42%) and a decline in insurance coverage between 2018 and 2019 (41%), we assume that coverage at a minimum will conservatively increase by 1% each year since no clear pattern on growth can be indicated through the information by the RBF. This is 2,609 new clients per annum and 217 new clients per month (we give a 200-300 range). In terms of insurance claims, we assume that claims would remain at a similar rate each year in the short-term unless a natural disaster hits. Claims will be around 70 per month. • Once-off integration: 260,914 • Reoccurring transactions. 217 + 70 = 287

18	Digital platforms for employment	46	750	Moderate	• Fiji Eats, Fiji Cabs, Vodo Fiji and CyberFoods have a combined number of app installations ranging from 15,000-25,000. This is the estimated number of clients. • Employees will require their identity verified. Assuming it requires less than 10% of the minimum customer base (1,500). It is plausible that the number of employees is between 500-1000. We take the average of 750. • Once-off integration: 1,000 + 500 = 1,500 / 2 = 750 • Recurring transactions: 750 x 5% = 38 new employees, plus 750 x 1% = 8 employees leaving = 38 + 8 = 46
19	Close foundational identity gap	No recurring transactions	256,211	Very low	• Once-off integration: 883,483 (Fiji population) • 627,272 with birth certificates. 883,483 - 627,272 = 256,211

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