THE INDEPENDENT STATE OF PAPUA NEW GUINEA

Digital ID Policy 2024

3rd Draft (Version 1.1)
December 2024

Contents

DEFINITIONS

For the purposes of this policy, the following definitions apply:

Term	Definition
Authentication:	The process of verifying the identity of a user or system, ensuring that they are who they claim to be, typically through credentials such as passwords, biometric data, or tokens.
Biometric Data:	Unique physical or behavioral characteristics used to identify individuals, including but not limited to fingerprints, facial recognition, iris scans, and voice patterns.
Cybersecurity:	The practice of protecting systems, networks, and programs from digital attacks, unauthorized access, damage, or data theft.
Digital ID (System):	An electronic identity verification system that allows individuals to prove who they are for the purpose of accessing services, conducting transactions, or engaging in digital interactions.
Digital Identity Service Provider:	An entity responsible for the management, operation, and maintenance of the digital ID system, ensuring secure, efficient, and compliant identity services.
e-KYC (Electronic Know Your Customer):	A digital process for verifying the identity of individuals or entities using electronic methods, ensuring compliance with regulatory requirements. e-KYC streamlines the onboarding process by enabling secure and efficient collection, validation, and authentication of identification data for accessing services across various sectors.
Encryption:	The method by which information is converted into secret code that hides the information's true meaning, ensuring data confidentiality and protection against unauthorized access.
Interoperability:	The ability of different information systems, devices, and applications to communicate, exchange data, and use the information exchanged in a seamless manner.
KYC (Know Your Customer):	A standardized process used to verify the identity of individuals or entities involved in a business relationship and to assess the potential risks of illicit activities, such as money laundering or fraud. The process typically involves collecting and validating information, such as identification documents and other relevant data, to ensure compliance with applicable legal and regulatory requirements.
National ID (NID):	A legally mandated, government-issued identification document used to verify the identity of individuals within a jurisdiction. It serves as an official record for administrative, legal, and regulatory purposes, ensuring compliance with national identification requirements and facilitating access to public and private services.
Open Standards:	Standards that are publicly available and have various rights associated with their use, ensuring that different systems can interact and integrate effectively without proprietary constraints.
Personal Data (or Personal Identity Information):	Any information relating to an identified or identifiable person. This can include data such as names, identification numbers, location data, or other attributes specific to a person’s physical, physiological, or social identity.

Privacy by Design:	An approach to system engineering that takes privacy into account throughout the whole engineering process, ensuring that data protection is built into the system architecture from the outset.
Public-Private Partnership (PPP):	A cooperative arrangement between public and private sectors, aimed at funding, designing, implementing, and operating projects that benefit both parties.
SevisPass:	The official Digital ID system established for Papua New Guinean citizens, designed to provide a secure, reliable, and user-friendly means of verifying identity in digital environments. It facilitates seamless access to public and private services, supports online transactions, and promotes digital inclusion while upholding data protection and privacy standards.
Tier Framework:	A classification system within the Digital ID policy that defines different levels of ID issuance and corresponding identity verification and access, balancing security requirements and financial inclusion.
User Consent:	The informed and voluntary agreement of a person to allow the collection, use, or sharing of their personal data under specified conditions.
Verification:	The process of checking that a digital identity matches the real-world identity it represents, confirming its accuracy and validity.
Vendor Neutrality:	The principle of designing systems that do not rely on a specific vendor's products, ensuring flexibility and avoiding lock-in to proprietary technologies.
Vulnerability Assessment:	The systematic process of identifying, evaluating, and addressing security weaknesses within a system to protect against potential threats.

FOREWORD BY THE MINISTER

In our rapidly evolving digital era, the importance of secure, reliable, and universally accessible identification systems cannot be overstated. The **National Digital ID Policy 2024** for Papua New Guinea marks a significant milestone in our journey towards embracing digital transformation and fostering inclusive growth.

The digital transformation agenda is mandated by the **Digital Government Act of 2022** and other policy initiatives driven under the Ministry of ICT through the efforts of the **Marape-Rosso government**.

Let me affirm that as a nation, we stand at the threshold of a new age where technology will be a pivotal enabler of economic development, social inclusion, and improved governance. The introduction of the **National Digital ID Policy 2024** is a testament to our commitment to harnessing the power of digital technologies to enhance the lives of our citizens, streamline government services, and bolster our economic resilience.

Let me promise the citizens that this policy is designed to provide every Papua New Guinean with a unique digital identity, ensuring that all individuals can participate fully in the digital economy. It will facilitate secure, efficient, and transparent access to government services, financial institutions, healthcare, and various other essential services. Moreover, the implementation of digital signatures will revolutionize our approach to authentication and authorization, reducing fraud and fostering trust in digital transactions.

We recognize that the success of this policy hinges on robust infrastructure, stringent data protection measures, and widespread digital literacy. Therefore, we are committed to investing in the necessary technological infrastructure, enacting comprehensive data protection laws, and launching extensive digital literacy programs to ensure that every citizen can safely and effectively use their digital IDs.

Forthwith, I extend my gratitude to all stakeholders, including government agencies, private sector partners, and international allies, for their invaluable contributions to the formulation of this policy. Your collaboration and support are vital as we embark on this transformative journey.

The **National Digital ID policy 2024** is not just a technological advancement; it is a significant step towards realizing our vision of a digitally inclusive society where every Papua New Guinean can thrive. Together, let us embrace this digital future and work towards building a more prosperous, equitable, and connected Papua New Guinea.

Sincerely,

HON. TIMOTHY MASIU, MP
Minister for Information and Communications Technology
Member for South Bougainville

STATEMENT BY THE SECRETARY

I am pleased to introduce the Digital ID Policy for Papua New Guinea, which serves as a cornerstone for the Implementation of ServisPass, Papua New Guinea's new and innovative digital identity system. The trajectory in our digital journey will achieve sustainability, scalability, and inclusivity with the inclusion of the Digital ID Policy.

SevisPass is designed to provide every citizen with a secure, reliable, and universally accepted digital identity. This initiative is a testament to our commitment to enhancing public service delivery, fostering economic growth, and ensuring the inclusion of all Papua New Guineans in the digital economy.

I am pleased to introduce the **Digital ID Policy** for Papua New Guinea, which serves as a cornerstone for the implementation of **ServisPass**, Papua New Guinea's new and innovative digital identity system. The trajectory in our digital journey will achieve sustainability, scalability, and inclusivity with the inclusion of the **Digital ID Policy**. **ServisPass** is designed to provide every citizen with a secure, reliable, and universally accepted digital identity. This initiative is a testament to our commitment to enhancing public service delivery, fostering economic growth, and ensuring the inclusion of all Papua New Guineans in the digital economy.

The **Digital ID Policy** outlines the framework for the deployment and management of **ServisPass**, ensuring that it adheres to the highest standards of security, privacy, and accessibility. Our vision is to deliver seamless service delivery to the citizens, with **Digital ID** as an important **Digital Public Infrastructure**. We focus on improving the quality of services to make them more transparent, easily accessible, faster, and scalable to every citizen.

We are committed to ensuring collaborative governance with other government agencies and partners by strengthening cooperation in delivering **ServisPass**. With increased participation from all stakeholders, we are certain to coordinate and implement the digital government agenda as mandated by the **Digital Government Act 2022**, achieving the Medium-Term Development Goals in the space of Information and Communications Technology (ICT). We believe the **Digital ID Infrastructure** will enhance security and privacy, promote digital inclusion, support economic development, foster financial inclusion, and improve access to services.

I want to reiterate that the successful implementation of **ServisPass** will require the collaboration of various stakeholders, including government agencies, private sector partners, and civil society. We are committed to working together to ensure that **ServisPass** becomes a trusted and integral part of our national infrastructure.

I encourage all citizens to embrace **ServisPass** and take advantage of the opportunities it offers. Together, we can build a more connected, secure, and prosperous Papua New Guinea.

Thank you.

STEVEN MATAINAHO
Secretary

1. POLICY INTENT

The policy intents to establish a comprehensive framework for the creation, implementation, and sustainability of a secure, inclusive, and interoperable Digital ID system.

The system will serve as a foundational digital public infrastructure (DPI), designed to be reusable across multiple applications and platforms. The Digital ID system will support Papua New Guinea's ongoing digital transformation efforts, driving economic growth, enhancing financial inclusion, and improving the efficiency of service delivery in both public and private sectors. Additionally, it will strengthen national security, promote trust in digital interactions, and ensure accessibility for all citizens while adhering to global best practices for data protection and privacy.

2. INTRODUCTION

Many countries across the world are embracing digital transformation, leveraging on digital technologies to accelerate their economic growth and transform their public administration for better service delivery. The establishment and implementation of a digital identity (ID) system is a critical enabler for digital transformation. As business processes are automated and citizens transitioned towards online interaction with government and service providers the identifying, verifying, and authenticating persons online for purposes of access to services becomes paramount.

Electronic know your customer (e-KYC) processes is one of the major aspects of digital ID. e-KYC process ideally leverage on a digital ID with the advantages of increasing efficiency, cost savings, and accelerated financial inclusion in many countries.

Papua New Guinea has adopted a Digital Transformation Policy of 2020 that prioritizes and encourages use of digital technologies towards sustainably growing the digital economy, transforming the public sector through the digital government initiatives, and encouraging greater citizens participation through information exchange and dissemination on digital platforms.

There are current practices within the banking sector in PNG and in the public sector on collection and managing identity of customers for purposes of facilitating online transactions and services. In the banking sector, each bank has historically been responsible for collecting and managing the identity of its own customers.

Few public organizations are providing services online and these organizations have in place systems to identify, verify, and authenticate citizens. These are efforts implemented at organizational levels specific to functional requirements. In contrast, a digital identity as a digital public infrastructure will offer digital ID as a service to public and private sector service providers.

3. POLICY ALIGNMENT

The policy aligns with PNG's Digital Transformation Policy of 2020 and other national strategies, including:

- The National Cyber Security Policy 2021
- The Data Governance and Protection Policy 2024
- The Government Cloud Policy 2023
- The Digital Government Act 2022

The Digital ID system is recognized as a critical Digital Public Infrastructure (DPI) within the Government's Technology Stack. It facilitates secure, efficient, and scalable digital services, enabling interoperability across systems. By doing so, it supports the delivery of integrated services, strengthens financial and social inclusion, and underpins the broader digital transformation agenda in both public and private sectors.

4. GUIDING PRINCIPLES

The Digital ID Policy is underpinned by the following key principles to ensure that the system is robust, inclusive, secure, and sustainable:

Principle 1: Governance and Protection

The design, development, and implementation of the Digital ID System will prioritize the governance and protection of personal data. This includes careful consideration of the collection, storage, management, and use of identity information. Security measures will be integrated into the technology and systems used, ensuring that they meet the highest standards of protection. Additionally, the privacy and confidentiality of all data collected will be maintained, adhering to best practices in data protection and compliance with relevant legal frameworks.

Principle 2: Inclusion

The Digital ID System will be designed to ensure that all citizens of Papua New Guinea—regardless of their location, whether in urban, rural, or unserved areas—have the opportunity to obtain a Digital ID. The process of collecting and verifying personal data will be simplified and tailored to reflect the diverse cultural and societal norms across the country. Special consideration will be given to ensuring that everyone, including marginalized and remote communities, can access digital services and engage in the digital economy.

Principle 3: Appropriateness of Design

The Digital ID System will be designed to balance security with usability.
This include:

- Ensuring data security is maintained throughout the entire Digital ID lifecycle.
- Building the system with scalability in mind to accommodate growing user numbers and demand for services.
- Designing with flexibility to facilitate future integration with other services and innovations.
- Ensuring universal access, particularly for citizens in rural and unserved areas, enabling them to register and obtain a Digital ID.

- Promoting open standards to ensure interoperability and compatibility across different technologies and platforms, while also ensuring vendor and technology neutrality.
- Incorporating privacy by design, ensuring that user privacy is embedded into the system from its inception.
- Ensuring the financial and operational sustainability of the system, making it resilient and capable of supporting long-term digital services and infrastructure.

5. MISSION

To establish a secure, efficient, and inclusive Digital ID System that prioritizes the protection of privacy and personal data, while enabling interoperability across both the public and private sectors. This system will be a catalyst for financial inclusion and enhance citizen access to a wide range of digital services, empowering individuals and supporting the country's ongoing digital transformation.

6. OBJECTIVES

Culminating from the guiding principles and mission, the Policy is focused on the following key objectives:

- Establishing SevisPass as the National Digital ID System: To formally recognize and deploy SevisPass as the standard platform for all digital identification purposes, providing a secure and universally accessible system for citizens.
- Developing Institutional Capacity: To build the necessary governance structures and institutional capacity to effectively manage, oversee, and ensure the integrity of the Digital ID system across public and private sectors.
- Introducing Legislation, Regulations, Standards, Rules, and Procedures: To create and implement a comprehensive legal and regulatory framework that will support the management, operation, and enforcement of Digital ID systems, ensuring compliance and security.
- Ensuring Sustainability: To guarantee the long-term viability and growth of the Digital ID system through the establishment of strategic financial models and operational frameworks, promoting continuous innovation, scalability, and resilience.

7. POLICY FOCUS AREAS

FOCUS AREA 1: ESTABLISHING DIGITAL ID AS A DIGITAL PUBLIC INFRASTRUCTURE (DPI)

The Digital ID system, known as SevisPass, will be established as a key component of Papua New Guinea's digital public infrastructure (DPI). The system will be designed to facilitate secure, efficient, and inclusive access to public and private services for all citizens. The Digital ID system will consist of the following components:

- Registration: The process of registering individuals will involve collecting personal and biometric data. A tiered framework will be used to categorize individuals according to different levels of identification, ensuring flexibility and scalability in the system. This process will be designed to accommodate diverse demographics, including urban, rural, and unserved populations.
- Issuance: Digital credentials, including biometric verification, will be issued to citizens and individuals. These credentials will ensure secure access to services by providing a verified identity that is universally accepted for both public and private sector engagements.
- Use: SevisPass will serve as the primary means for citizens and individuals to access a wide range of services across both the public and private sectors. This includes services such as government welfare programs, health services, financial transactions, and other essential digital services.
- Management: A designated institution will be responsible for the ongoing management of the Digital ID System. This includes overseeing technology adoption, ensuring interoperability between public and private sector platforms, providing continuous maintenance, and managing grievance redressal processes to address any issues related to the system's operation.

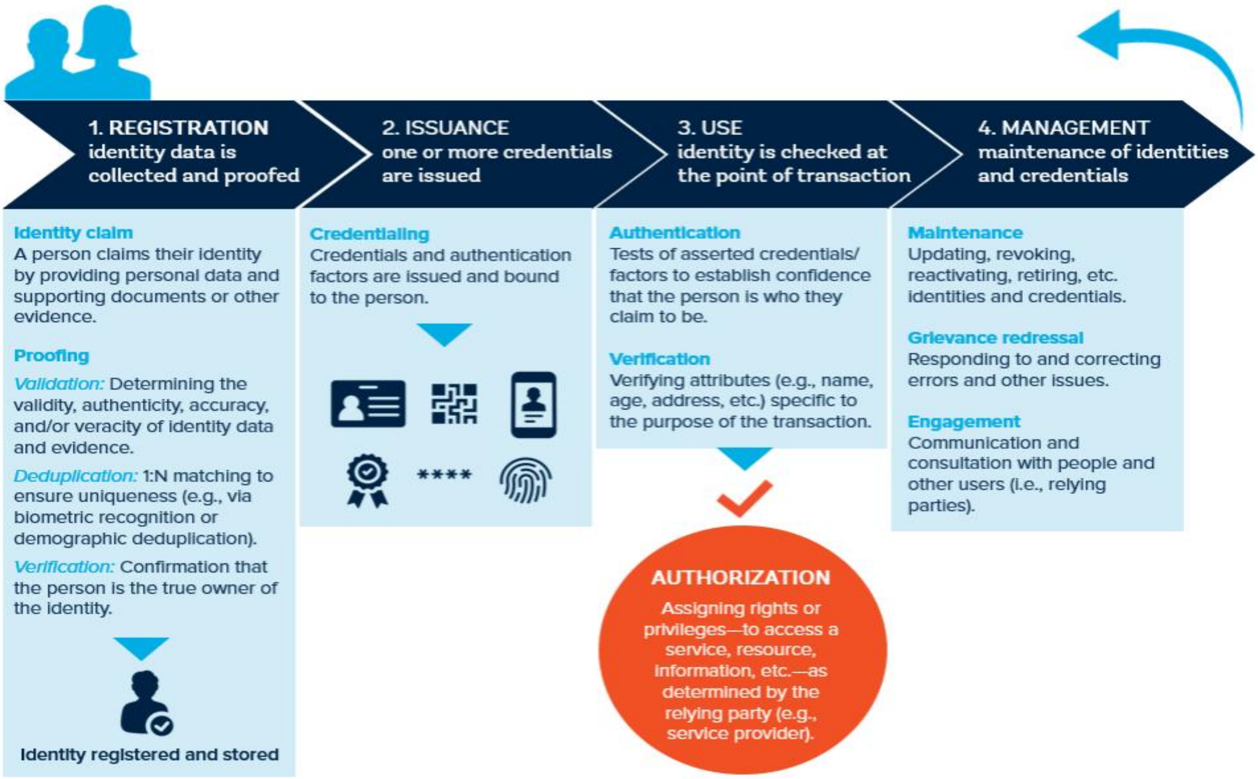

1. REGISTRATION identity data is collected and proofed
2. ISSUANCE one or more credentials are issued
3. USE identity is checked at the point of transaction
4. MANAGEMENT maintenance of identities and credentials
Identity claim
A person claims their identity by providing personal data and supporting documents or other evidence.
Proofing
Validation: Determining the validity, authenticity, accuracy, and/or veracity of identity data and evidence.
Deduplication: 1:N matching to ensure uniqueness (e.g., via biometric recognition or demographic deduplication).
Verification: Confirmation that the person is the true owner of the identity.
Identity registered and stored
Credentialing
Credentials and authentication factors are issued and bound to the person.
****
Authentication
Tests of asserted credentials/ factors to establish confidence that the person is who they claim to be.
Verification
Verifying attributes (e.g., name, age, address, etc.) specific to the purpose of the transaction.
AUTHORIZATION
Assigning rights or privileges—to access a service, resource, information, etc.—as determined by the relying party (e.g., service provider).
Maintenance
Updating, revoking, reactivating, retiring, etc. identities and credentials.
Grievance redressal
Responding to and correcting errors and other issues.
Engagement
Communication and consultation with people and other users (i.e., relying parties).

Figure 1: Components of Digital ID (Adapted from Digital Identity: Public and Private Sector Cooperation and Technology Landscape for Digital)

The technology, strategies, legislative framework, institutional capacity, and sustainability plans will be developed and implemented to support and ensure the long-term success and growth of these key components of the Digital ID system. This will ensure that SevisPass operates as a robust, adaptable, and secure Digital Public Infrastructure, facilitating access to essential services for all.

Component 1: Registration

During the Registration process, personal data will be collected in accordance with the Digital ID Tier Framework, which provides a classification system to categorize different levels of identity verification and customer onboarding. The registration will require individuals to provide information across three key categories:

- Something You Know:

This includes, among others, a personal identifier such as a password or PIN, ensuring that access to the registration platform is protected and secure.

- Something You Have:

This includes identification documents such as a National ID (NID), employment ID, membership ID, driving license, or passport. These documents will be used to confirm the identity of the individual and verify their status.

- Something You Are:

Biometric data will be collected, including fingerprints, facial recognition, or iris scan. This step ensures a higher level of identity verification by leveraging unique personal traits to reduce the risk of fraud and enhance security.

Additionally, personal information such as the individual's name, date of birth, and address will be collected as part of the registration process. This data, along with the biometric information, will be used to create a secure, verified identity within the Digital ID system.

Component 2: Issuance

The Issuance of credentials in the Digital ID system will follow a multi-tiered approach designed to accommodate various levels of identity verification and service access. The key features of this system include:

(i) Tiered Issuance System

- **Tier 1 (Basic Issuance):** This tier is for individuals who may have minimal documentation or informal references, such as community representative or pastor letters. It enables access to basic services with limited transaction capabilities. This tier is aimed at ensuring that even individuals without formal identification can begin to access essential public services.

- **Tier 2 (Intermediate Issuance):** This tier includes individuals who possess identification that is not legally mandated but is still recognized as official in certain contexts, such as work IDs, school IDs, or other recognized but non-government-issued IDs. These individuals will be able to access moderate services and transactions, offering a higher level of trust than Tier.

- **Tier 3 (Full Issuance):** Individuals who possess government-issued IDs such as the National ID (NID), Driver's Licenses, Passports, or any other officially recognized government identification will fall into this tier. It provides comprehensive access to a wide range of services and high-value transactions, making it the most secure level of identification.

- **Tier 4 (Enhanced Issuance):** This tier is reserved for individuals or entities requiring extensive background checks or higher levels of due diligence, such as high-risk individuals or government officials. It includes a more rigorous verification process, continuous monitoring, and additional safeguards to ensure the integrity of the user's identity. Enhanced Issuance is designed for individuals involved in sensitive or high-value transactions, where additional layers of verification and security are necessary.

(ii) Digital and Physical Credentials

The issuance process will offer both digital and physical credentials to accommodate various user needs:

- **Digital Credentials:** These will include QR codes and digital certificates stored in mobile wallets or apps, providing secure and easy access to services.

- **Physical Smart Cards:** For those who prefer a tangible form of identification, physical smart cards will also be issued. These cards will serve as an official means of identification and can be used for both public and private sector services.

(iii) Biometric Verification for Issuance

To ensure the authenticity of the issued credentials, biometric verification (e.g., fingerprints, facial recognition, or iris scans) will be required. This ensures that the individual receiving the ID matches the identity profile in the system, minimizing the risk of fraud.

(iv) Integration with Existing IDs

The issuance process will integrate with existing government-issued IDs such as NID cards, passports, and driver's licenses, enabling a smooth transition for individuals who already possess these IDs. The Digital ID system will leverage these existing credentials to streamline the registration process and provide a seamless user experience.

Component 3: Use

An issued Digital ID (SevisPass) will enable citizens and individuals to access both private and public online services securely and efficiently, anywhere and anytime.

Role of an ID System

The Use component reflects the Digital ID as a Digital Public Infrastructure (DPI), highlighting SevisPass as an essential service that facilitates broad and seamless access to a wide range of digital services. The primary aspects of this system include:

(i) **Access to Public and Private Sector Services:** Citizens will use SevisPass to securely access a range of public services such as eGovernment portals, social benefits, and private sector services including banking, telecommunications, and other private services. The system ensures that both government and private sector interactions are efficient and secure.

(ii) **Interoperability as Digital Public Infrastructure:** SevisPass will serve as a foundational Digital Public Infrastructure, promoting interoperability and seamless interaction across various service providers. It will be integrated into multiple public and private systems and frameworks, contributing to the creation of a cohesive and interoperable digital ecosystem that enhances user experience and accessibility.

(iii) **Multi-Platform Support:** SevisPass will be accessible through multiple platforms, including web applications, mobile apps, and NFC-enabled devices (such as smart cards). This approach ensures that all users, regardless of their preferred technology, have equal access to the services offered by the Digital ID system, fostering inclusivity.

(iv) **Consent Management and User Control:** The system will provide features that allow users to manage and control their consent for data sharing. This empowers individuals to have greater trust in the system by giving them control over what personal data is shared and with whom, enhancing privacy and security.

(v) **Inclusion and Accessibility:** To promote digital inclusion, SevisPass will be designed with accessibility features to ensure that individuals with disabilities can use the system without barriers. This inclusive design will ensure that all citizens, regardless of their physical abilities, can access digital services with ease.

(vi) **Universal Access and Scalability:** As part of its role as public infrastructure, SevisPass will be designed to scale and meet the demands of an increasing number of users and expanded service offerings. It will ensure universal access to digital services across all regions, including underserved and rural areas, providing reliable and equitable service delivery.

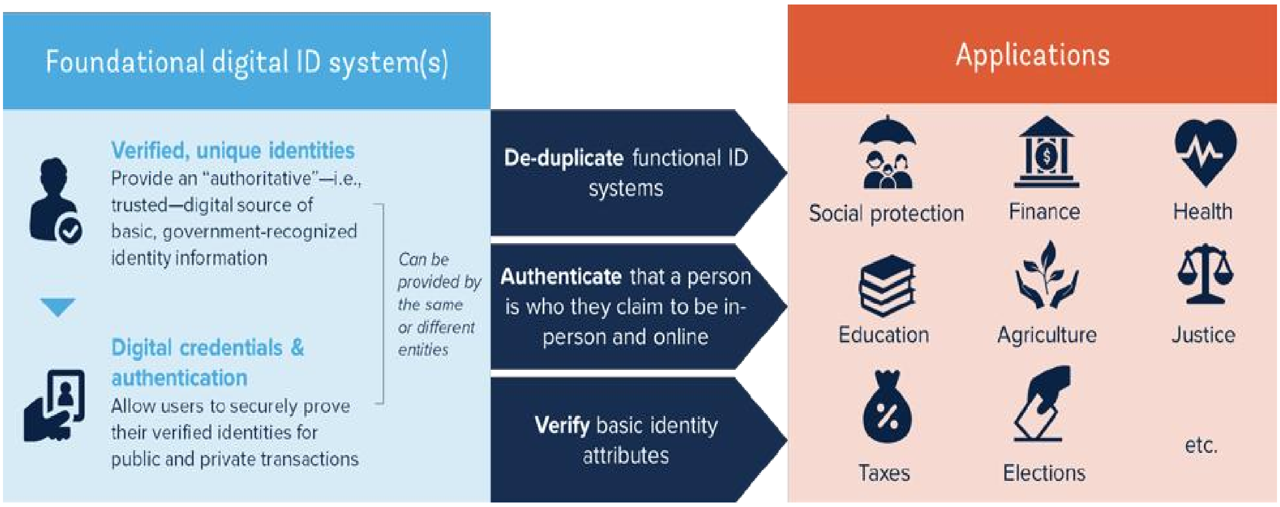

Foundational digital ID system(s)
Verified, unique identities
Provide an "authoritative"—i.e., trusted—digital source of basic, government-recognized identity information
Digital credentials & authentication
Allow users to securely prove their verified identities for public and private transactions
Can be provided by the same or different entities
De-duplicate functional ID systems
Authenticate that a person is who they claim to be in-person and online
Verify basic identity attributes
Applications
Social protection
Finance
Health
Education
Agriculture
Justice
Taxes
Elections
etc.

Figure x. Foundational Digital ID System(s)

Table: Use Cases for SevisPass Across Public and Private Sectors

Sector	Use Cases	Description
Government Services	eGovernment Portals	Accessing a wide range of government services, such as tax filing, social welfare applications, public records, and various government agency portals, through secure and efficient digital authentication.
	Social Benefits	Enabling secure identity verification for individuals applying for social security, pension schemes, welfare programs, and other state-administered benefits, ensuring eligibility and proper distribution.
	Healthcare Services	Ensuring secure patient identification in healthcare systems for accessing medical services, digital health records, and enabling interoperable health data for better service delivery and continuity of care.
	Education	Verifying student identities for enrollment, access to educational resources, exam registrations, and scholarships in both public and private educational institutions.
	Civic Engagement	Supporting online voting, digital petitions, and electoral engagement with a secure platform for voting, ensuring transparent and tamper-proof participation in civic processes.
Financial Services	eKYC for Banks and Financial Institutions	Streamlining identity verification for individuals opening bank accounts, applying for loans, and processing transactions through secure digital Know-Your-Customer (eKYC) procedures.
	Digital Loan Applications	Facilitating faster and more secure identity checks during the application and approval process for personal, business, and micro-loans in financial institutions, improving speed and reliability.

	Mobile Banking and Payment Platforms	Enabling secure logins and transaction verifications for mobile banking, payment wallets, and online banking, ensuring users' identities are confirmed before access to their financial accounts.
Telecommunications	SIM Card Registration	Implementing tiered KYC processes to verify identity before issuing or activating SIM cards, preventing fraud and ensuring users' details are accurate in the telecom system.
	Mobile Service Access	Using SevisPass for identity verification to access premium services, modify telecom account settings, or activate new services such as data packages and subscriptions in the telecommunications sector.
Utilities	Service Subscriptions and Payments	Verification for new utility subscriptions for essential services such as electricity, water, and internet to ensure only verified users can access and use services.
	Billing and Account Management	Enabling secure access to utility billing information, payment history, and account management functionalities, ensuring customers' details are protected during transactions.
Retail and eCommerce	Online Shopping	Authenticating users for secure online purchases, ensuring identity verification during checkouts, and providing secure order tracking for customers.
	Loyalty Programs and Rewards	Verification of user eligibility for loyalty programs, discounts, and rewards in online and physical stores, ensuring that users can access exclusive deals through verified membership data.
	Digital Payments	Facilitating secure digital payments across eCommerce sites and physical stores through SevisPass, offering seamless, encrypted payment transactions during checkouts.
Transport	Public Transport Access	Enabling tap-and-go payment systems for public transport including buses, trains, and ferries. This includes digital ticketing for smoother, cashless travel experiences across the network.
	Air Travel	Streamlining identity verification for flight bookings, check-ins, and boarding passes, ensuring travelers' identities match official records for safer and more efficient air travel.
Healthcare	Patient Registration	Simplifying hospital and clinic registrations by using SevisPass for patient authentication, ensuring seamless access to medical appointments and faster administrative processing.
	Medical Insurance	Verification for insurance claims and access to medical policy benefits, ensuring that the insured person's identity matches with medical records to streamline service delivery and claims processing.
Insurance	Policy Enrollment	Enabling secure identity verification during policy applications for life, health, and property insurance, ensuring applicants' identities are confirmed and matched to the correct policy details.
	Claims	Enhancing claims processing efficiency by verifying identities

	Processing	through SevisPass, reducing fraud and speeding up approval times for insurance claims.
Real Estate	Tenant and Property Buyer Verification	Verifying identity and background checks for tenants or property buyers, ensuring legitimacy and preventing fraud during the rental or property purchasing process.
	Digital Lease Agreements	Secure sign-in and verification for digital contracts such as lease agreements, ensuring all parties involved in property transactions are authenticated and legally bound in a secure digital environment.
Employment	Job Applications and Employee On-boarding	Enabling secure identity verification during the recruitment process, onboarding, and background checks, ensuring applicants' qualifications and identity are authentic.
	Access to Employment Benefits	Using SevisPass to authenticate employees for accessing benefits, including payroll services, healthcare coverage, retirement plans, and other employment-related perks.
Travel and Tourism	Hotel and Accommodation Check-ins	Quick, secure identity verification for hotel check-ins, ensuring that travelers' identities are verified at the point of entry, improving hotel security and guest satisfaction.
	Tour Operator Services	Verifying tour bookings and participation in activities, ensuring that the identities of tourists and travelers are confirmed, improving security and service delivery for tourism-related services.

Component 4: Management

The Management component of SevisPass ensures that the system remains efficient, secure, adaptable, and aligned with national objectives for long-term sustainability and growth. This component includes the following critical aspects:

(i) Centralized Oversight by the Department of ICT

The Department of ICT (or an appointed service provider) will be responsible for overseeing the day-to-day operations of SevisPass, ensuring that it aligns with the broader national digital transformation policies and objectives. This oversight role includes:

- **Coordination and Monitoring:** Ensuring that SevisPass functions seamlessly across all sectors and services.
- **Policy Alignment**: Ensuring the system adheres to national digital governance frameworks and ICT policies.
- **Reporting:** Regular updates to stakeholders, including government agencies, on SevisPass performance and impact.

(ii) Security and Privacy Protections

Maintaining high standards of security and privacy is paramount for SevisPass. The system will be equipped with ongoing, proactive cybersecurity measures, including but not limited to:

- **Real-Time Monitoring:** Continuous surveillance of system activity to detect and respond to potential security threats.
- **Vulnerability Assessments:** Regular reviews and assessments of the system's infrastructure to identify weaknesses and apply appropriate mitigations.
- **Data Encryption**: Implementing industry-standard encryption protocols to protect sensitive user data and prevent unauthorized access during data transmission and storage.
- **Access Control:** Strong mechanisms to control and monitor who has access to the system, with periodic reviews of permissions and roles.

(iii) Grievance Redressal Mechanism

To ensure user confidence and address challenges related to SevisPass, a robust grievance redressal mechanism will be established. This mechanism will:

- **Complaint Handling:** Provide a clear, accessible process for users to file complaints regarding system functionality, service issues, or privacy concerns.

- **Resolution Timelines**: Ensure that all grievances are addressed in a timely manner with clear response times.

- **Transparency and Accountability:** Track complaints and their resolution progress, ensuring transparency in the handling process to maintain user trust.

- **Feedback Integration:** Ensure that recurring issues are identified, addressed, and used as opportunities for continuous system improvement.

(iv) Continuous Improvement

SevisPass will evolve in response to feedback, technology advancements, and the dynamic needs of its users. This includes:

- **Regular System Updates:** Frequent system updates to integrate new features, enhancements, and security patches based on evolving requirements.
- **User Feedback Integration:** Collecting and analyzing feedback from users, both public and private sector stakeholders, to make improvements in the system's usability and functionality.
- **Adapting to Technological Advances:** Staying ahead of emerging technologies and trends to ensure SevisPass remains at the cutting edge and adaptable to future technological innovations.

(v) Stakeholder Engagement

Ensuring that SevisPass meets the needs of all stakeholders is a key part of its management. Ongoing engagement with both public and private sector stakeholders will help ensure that:

- **Stakeholder Collaboration:** Continuous collaboration between government agencies, private sector partners, and citizens to ensure the system is effectively meeting expectations.
- **Adaptability to Future Needs:** The system will remain flexible, with the ability to adapt to new services, evolving digital platforms, and sector-specific requirements.
- **Strategic Partnerships:** Building and maintaining relationships with external partners to enhance system capabilities and extend the use of SevisPass across sectors.

FOCUS AREA 2: INTEGRATION, INTEROPERABILITY, AND STANDARDS

The SevisPass (Digital ID) system is designed to function as a central pillar of digital identity management in Papua New Guinea. To achieve this, it must integrate seamlessly with existing systems, provide interoperability across sectors, and adhere to globally recognized standards. This approach ensures that SevisPass is not only effective but also secure, accessible, and scalable across diverse service environments.

(i) Integration with Existing Systems

SevisPass will be built with robust integration capabilities to work harmoniously with existing identification systems such as the National ID (NID), driver's licenses, passports, and other government-issued identification documents recognized through legal means. This integration will allow individuals to leverage their existing records for digital identity verification, facilitating a smoother transition to a unified digital ID system. Key integration aspects include:

- **Centralized Platform:** A central platform will be established to facilitate seamless data exchange between SevisPass and public sector databases, ensuring that identity verification is consistent and reliable across multiple platforms.

- **Leverage Existing Records:** Individuals’ historical records from existing systems, such as NID, passports, and driver’s licenses, will be linked with SevisPass, ensuring efficiency and reducing the need for re-registration or redundant data entry.

- **Enhanced User Experience:** Integration ensures that individuals can access services across both government and private sector platforms using a single digital ID, enhancing user convenience and encouraging widespread adoption.

(ii) Interoperability with Services

For SevisPass to serve as a true digital public infrastructure, it must be designed to interoperate with a wide variety of services across both the public and private sectors. This interoperability is essential for creating a unified digital ecosystem that supports seamless access to essential services, including government portals, healthcare services, financial institutions, and telecommunications providers. Key features for interoperability include:

- **Open Standards and APIs:** SevisPass will be developed based on open standards and robust APIs (Application Programming Interfaces) that allow easy integration with a range of services. This will enable secure and consistent identity verification across diverse sectors.
- **Public and Private Sector Connectivity:** Government systems such as tax systems, health services, and social welfare platforms will be integrated with SevisPass, as will private sector services like banking, telecommunications, and retail platforms.
- **Improved User Experience:** By enabling seamless interaction between SevisPass and service providers, users can access various services without the need for separate logins or identity verifications, streamlining service delivery and improving overall user experience.

(iii) Adoption of Standards and Compliance:

The success of SevisPass relies on the adoption of stringent standards that ensure security, privacy, and interoperability across all components of the system. These standards will be developed in alignment with best practices for digital identity systems, including global frameworks like ISO/IEC 27001 for cybersecurity and data privacy, to guarantee that SevisPass functions effectively and securely. Key standards include:

- **Registration Standards:** These standards will define secure data collection protocols, ensuring that individuals' data is collected, verified, and stored according to strict privacy and security guidelines. Emphasis will also be placed on inclusivity, ensuring that all individuals, regardless of their background, have access to the registration process.
- **Issuance Standards:** Standards for the issuance of credentials will focus on ensuring the integrity of digital IDs. This includes standards for biometric verification, ensuring that credentials are linked to the correct individual and that the system is robust against fraud or misuse. Additionally, integration with existing IDs will be prioritized to ensure a smooth transition.
- **Usage Standards:** These standards will govern how SevisPass is used for service access, focusing on user authentication, consent management, and data privacy. Usage standards will enable the system to maintain high levels of security while being easy for citizens to use.
- Management Standards: The management of SevisPass will be guided by a set of governance and cybersecurity standards, including incident response protocols and continuous improvement frameworks. These will be aligned with ISO/IEC 27001 standards to ensure that the system remains secure and resilient over time.

(iv) Compliance Monitoring and Governance

To ensure that SevisPass adheres to the defined standards, compliance will be monitored by a Data Governance Authority or, alternatively, by the existing National ICT Authority. This governance body will oversee the following:

- **Regulatory Framework Development:** In the medium to long term, a comprehensive regulatory framework will be developed to facilitate the expansion of digital identity services across both public and private sectors.
- **Ongoing Audits and Reporting:** Regular audits and reports will be generated to track SevisPass' compliance with standards, ensuring that the system remains secure, accessible, and reliable.
- **Stakeholder Engagement:** The governance body will work closely with all stakeholders, including government agencies, private sector partners, and civil society, to ensure that SevisPass continues to meet the evolving needs of users.

FOCUS AREA 3: TIER FRAMEWORK

The Digital ID system will adopt a Tier Framework to ensure flexibility and scalability in identity verification. This framework will cater to a broad range of customer profiles, particularly addressing the need for financial inclusion, while maintaining the necessary security and regulatory compliance across sectors, especially in financial services. It is designed to meet varying Know Your Customer (KYC) requirements, with each tier representing a progressive level of verification, risk management, and access to services.

By progressively onboarding individuals based on their available documentation and risk profile, the Tier Framework aims to balance financial inclusion and security for all citizens, regardless of their access to formal identification.

(i) Key Features of the Tier Framework

Progressive KYC: The framework allows institutions to onboard customers in stages, increasing the level of identity verification and service access as customers progress through the tiers.

Risk Management: Lower tiers have more restrictions to reduce risks associated with financial crime, while higher tiers involve more comprehensive checks but allow broader access to services.

Financial Inclusion: The system ensures that individuals without formal identification can still participate in the financial system, particularly through Tier 1.

Compliance: As customers move to higher tiers, financial institutions will meet stricter anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations.

(ii) Tier Breakdown

Tier 1 - Basic Identification

Purpose: Provide access to basic services for individuals without government-issued IDs.

Customer Profile: Individuals without government-issued IDs, including those in remote or underserved areas.

KYC Requirements:
- Basic personal information: name, date of birth, and place of residence.
- Verification methods:
- Local community leader verification.
- Local authority verification.

Digital ID (SevisPass).

Services & Transactions:
- Low-value transactions (e.g., low withdrawal limits, mobile payments).
- Risk level: Low, due to limited transaction volumes.

Goal: Ensure financial inclusion for those without formal identification, while minimizing risk.

Tier 2 - Intermediate Identification

Purpose: Provide access to a broader range of services with more stringent KYC requirements than Tier 1.

Customer Profile: Individuals with provisional or temporary government-issued documentation but not full government IDs.

KYC Requirements:

- Personal information from provisional IDs.
- Proof of postal or residential address.
- Enhanced biometric verification.

Services & Transactions:

- Higher transaction limits than Tier 1 (e.g., savings and current accounts, loans, and remittances).
- Risk level: Moderate, as additional services are provided.

Goal: Offer greater access to services while managing risks through enhanced KYC.

Tier 3 - Full Identification

Purpose: Provide full access to all services with comprehensive KYC requirements.

Customer Profile: Individuals with full, government-issued IDs, meeting all regulatory requirements.

KYC Requirements:

- Full government-issued ID (e.g., passport, national ID, driver’s license).
- Proof of address (postal or residential).
- Biometric data and thorough identity verification.
- Verification against global AML/CFT watch-lists.

Services & Transactions:

- Full access to banking services, including high-value transactions, savings, credit facilities, insurance, and international transfers.
- Risk level: Low, as comprehensive checks are conducted and transactions are monitored for AML/CFT compliance.

Goal: Ensure low-risk transactions and comprehensive access to all financial and public sector services.

Tier 4 - Enhanced Due Diligence (EDD)

Purpose: Address high-risk individuals or entities requiring enhanced scrutiny and due diligence.

Customer Profile: High-net-worth individuals, businesses in high-risk sectors, politically exposed persons (PEPs), and entities in high-risk jurisdictions.

KYC Requirements:

- Full ID verification, plus additional background checks.
- Enhanced due diligence, including ongoing monitoring of transactions and customer activities.
- Extensive documentation of sources of income and wealth.

Services & Transactions:

- High transaction limits with strict monitoring (e.g., large loans, foreign exchange services, corporate accounts).
- Risk level: High, requiring continuous monitoring and frequent risk reviews.

Goal: Minimize risks associated with high-value transactions while ensuring compliance with AML/CFT regulations.

Table 2: Summary of Tiered Approach for Digital ID Registration and Assurance Levels

Tier Level	**Description**	**Data Required at Registration**	**Assurance Level Requirement**
Tier 1	Basic Identification	- Name - Date of birth - Place of residence	Low assurance (Minimal verification through local/community authority)
Tier 2	Intermediate Identification	- Personal details from government-issued provisional/temporary IDs - Proof of postal/residential address - Basic biometric data (e.g., facial recognition)	Moderate assurance (Verification with temporary IDs and community verification)
Tier 3	Full Identification	- Full government-issued ID (e.g., passport, national ID, driver's license) - Proof of postal/residential address - Comprehensive biometric data (e.g., fingerprints, iris scan)	High assurance (Strong verification against official records and biometric checks)
Tier 4	Enhanced Due Diligence	- Full government-issued ID - Proof of residential address - Detailed biometric data - Documentation of source of income/wealth - Background checks against AML/CFT databases	Very high assurance (Extensive verification and continuous monitoring)

This table summarizes the Tiered Approach for Digital ID registration, providing the required data for each tier, along with the corresponding assurance levels for identity verification. This approach ensures that as individuals progress through the tiers, their identity verification becomes more comprehensive, balancing financial inclusion and regulatory compliance with security.

FOCUS AREA 4: IMPLEMENTTION FRAMEWORK

(i) Digital Identity Service Provider

The Department of ICT (or the nominated partner) will serve as the Digital Identity Service Provider (DISP), responsible for establishing and managing the SevisPass Digital Identity System. The DISP will collaborate with both public and private sector stakeholders, including Digital Transformation Officers (DTOs), to ensure effective implementation and integration. The Digital Identity Service Provider will:

- **Accreditation Framework:** Establish an accreditation framework to guide the issuance of digital IDs, ensuring adherence to international best practices.
- **Cyber Security Measures:** Implement robust cybersecurity protocols to protect both the digital ID system and identity data.
- **Infrastructure and Technology**: Build appropriate infrastructures and platforms for managing digital identities as part of the Digital Public Infrastructure.
- **Capacity Building & Awareness:** Facilitate awareness and capacity-building programs targeted at citizens, service providers, and key stakeholders to foster understanding and adoption

(ii) Public-Private Partnerships (PPPs)

To ensure the widespread adoption and sustainability of SevisPass, the Department of ICT will establish strategic Public-Private Partnerships (PPPs):

Private Sector Integration:

- **Banking & Financial Integration:** Collaborate with banks, telecommunications providers, and financial institutions to integrate SevisPass into their verification and authentication processes.
- **Broad Use Cases:** Partner with service providers, including mobile network operators, utility companies, and financial institutions, to expand the range of services that use SevisPass for everyday transactions.
- **Technical Support:** Offer technical guidelines and assistance to private sector entities to ensure smooth integration with SevisPass across platforms.

Incentives for Private Sector Participation:

- **Cost Reduction:** Provide incentives for companies to adopt SevisPass by reducing compliance costs through streamlined Know Your Customer (KYC) processes.
- **Service Agreements:** Establish service agreements with private sector partners to enable them to use SevisPass for electronic KYC (eKYC), secure authentication, and customer onboarding.

(iii) Community-Based Enrollment and Support

The Department of ICT, through the Universal Access Secretariat, will ensure that community-based enrollment centers are set up nationwide to address the needs of rural and underserved populations.

Local Enrollment Agents:

- **Trained Local Agents:** Deploy trained local agents to assist citizens with the digital ID enrollment process, particularly in remote areas with limited access to technology.Collaboration with Local Leaders: Partner with community leaders and local

Mobile Enrollment Units:

- **Mobile Units:** Introduce mobile enrollment units equipped with biometric scanners to reach the most remote communities, ensuring broad coverage for SevisPass registration.

Continuous Support:

- **Helpline and Support Center:** Set up a dedicated helpline and technical support center for citizens, providing assistance with SevisPass usage and troubleshooting.

(iv) Public Awareness and Digital Literacy Campaigns

To promote the adoption of SevisPass, the Department of ICT, through the Universal Access Secretariat, will roll out a comprehensive public awareness and digital literacy campaign.

Digital Literacy Programs:

- **Training Initiatives:** Partner with community leaders, NGOs, and educational institutions to offer digital literacy training to citizens, particularly in rural areas, on how to use SevisPass.
- **Program Focus:** These programs will cover:
- Secure management of digital identities.
- Access to government and private sector services using SevisPass.
- Prevention of fraud and identity theft.

Communication Channels:

- **Multi-Channel Campaign:** Launch a multi-channel public awareness campaign through radio, television, social media, and community events to ensure widespread dissemination of information.
- **Localized Content:** Develop content in Papua New Guinean languages and dialects to ensure all citizens understand the system’s benefits and usage.

FOCUS AREA 5: LEGISLATIVE & REGULATORY FRAMEWORK, STANDARDS & GUIDELINES

The rise in demand for online services and the ongoing digitalization of various sectors in Papua New Guinea highlights the necessity for a secure, reliable, and privacy-preserving framework for identity creation, verification, and protection within the digital sector. A comprehensive legislative and regulatory framework is needed to ensure the privacy and security of users, facilitate interoperability, and foster user trust in the digital identity system. This framework will be consistent with the National Cyber Security Strategy 2023-2027 and the National Data Governance and Protection Policy 2024.

The proposed legislative framework will address key elements required to effectively establish, deploy, and manage a digital identity system. The framework will:

(i) Define the Role of Digital Identity Service Provider (DISP):

Clearly define the responsibilities and functions of the Digital Identity Service Provider (DISP), which will manage the digital identity system and ensure the proper operation of the system.

(ii) Privacy and Security of Personal Information:

Guarantee the privacy and security of personal data through strict data protection mechanisms, aligned with international standards, to ensure the confidentiality and integrity of identity data.

Promote economic benefits through the use of digital identities while balancing this with appropriate data protection measures.

(iii) Governance and Technical Measures:

Establish governance measures and technical protocols to safeguard personal information. This includes:

- Ensuring consent-based data sharing and the use of secure biometric authentication systems.
- Facilitating the secure use of digital signatures and signing keys on biometric chips.
- Promoting interoperability across sectors to ensure seamless integration and secure data exchange.

(iv) Cybersecurity Measures:

Develop a regulatory framework to establish mechanisms that support the verification and protection of digital identities. This will help mitigate risks associated with identity theft, fraud, and other cybersecurity threats.

(v) User Privacy Protection:

Uphold users' rights by implementing strict privacy protection measures throughout the data onboarding, storage, and revocation protocols.

Promote user confidence by ensuring that all actions related to data collection, storage, and use are transparent, consensual, and legally compliant.

FOCUS AREEA 6: SUSTAINABILITY PLAN

The digital transformation policy in PNG aims to significantly contribute to economic growth, financial inclusion, and efficient service delivery across both public and private sectors. A crucial component of this transformation is the SevisPass, which serves as a foundational element in the country's ongoing digital evolution. To ensure the success and sustainability of SevisPass, appropriate resourcing, operational efficiency, and scalability are essential.

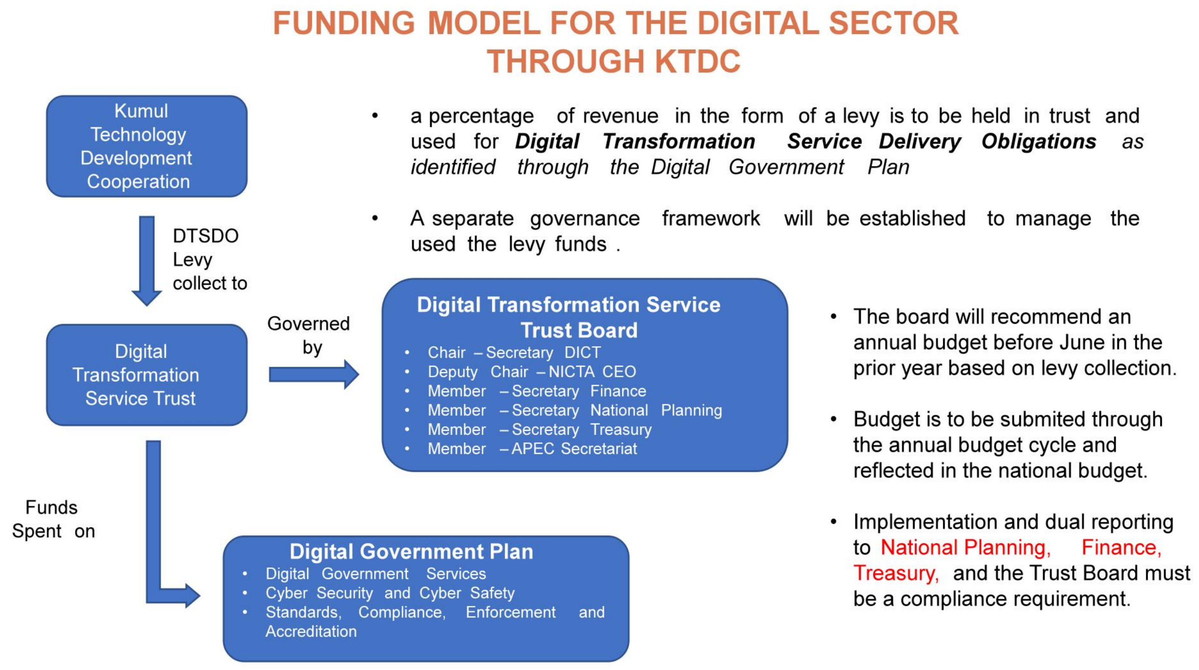
As the Digital Identity Service Provider, the Department of ICT will collaborate with State-owned Enterprises through the Kumul Technology Development Cooperation (KTDC) to explore and establish a robust funding model that ensures the long-term sustainability of SevisPass. The sustainability plan aims to secure continuous operation, scalability, interoperability, and security of SevisPass, ensuring it remains a vital Digital Public Infrastructure (DPI) for PNG.

The key components of the sustainability model include:

(i) **Revenue Generation:** To support SevisPass operations, a revenue model will be implemented. A minimal percentage of revenue, in the form of a levy, will be collected and held in trust, contributing to the funding of SevisPass. This revenue will be strategically allocated to maintain the system’s operational needs, updates, and future scalability.

(ii) **Digital Transformation Service Trust:** Guided by the Digital Government Plan 2023-2027, the establishment of a Digital Transformation Service Trust will govern the financial management and sustainability of SevisPass. The Trust will oversee the allocation of revenue and ensure transparency in the use of funds for SevisPass’ continued development and operational efficiency.

(iii) **KTDC's Role:** The Kumul Technology Development Cooperation (KTDC), acting as the implementing vehicle for SevisPass, will manage the collection of revenue and oversee the financial aspects of SevisPass. The Digital Transformation Service Trust Board (DTSTB) will govern and manage the Trust, ensuring funds are effectively used to maintain and expand SevisPass as a critical national infrastructure.



FUNDING MODEL FOR THE DIGITAL SECTOR THROUGH KTDC

- a percentage of revenue in the form of a levy is to be held in trust and used for ***Digital Transformation Service Delivery Obligations*** *as identified through the Digital Government Plan*
- A separate governance framework will be established to manage the used the levy funds .

Kumul Technology Development Cooperation

DTSDO Levy collect to

Digital Transformation Service Trust

Governed by

Digital Transformation Service Trust Board

- Chair – Secretary DICT
- Deputy Chair – NICTA CEO
- Member – Secretary Finance
- Member – Secretary National Planning
- Member – Secretary Treasury
- Member – APEC Secretariat

Funds Spent on

Digital Government Plan

- Digital Government Services
- Cyber Security and Cyber Safety
- Standards, Compliance, Enforcement and Accreditation

- The board will recommend an annual budget before June in the prior year based on levy collection.
- Budget is to be submited through the annual budget cycle and reflected in the national budget.
- Implementation and dual reporting to National Planning, Finance, Treasury, and the Trust Board must be a compliance requirement.

Figure. X Funding Model for Digital Sector including SevisPass through KTDC

8. MONITORING AND EVALUATION

A comprehensive Monitoring & Evaluation (M&E) framework will be established to ensure the effectiveness, sustainability, and continuous improvement of the SevisPass digital identity system. This framework will focus on tracking key performance indicators (KPIs), assessing system impact, and addressing emerging challenges to ensure that SevisPass meets its goals and contributes to the broader digital transformation agenda.

(i) Key Components of the M&E Framework:

Tracking Key Performance Indicators (KPIs):

- **Enrollment Rates:** Regularly monitor the number of citizens enrolling in the SevisPass system, ensuring widespread adoption and equitable access, particularly in underserved regions.

- **Service Delivery Efficiency:** Measure the effectiveness and speed of service delivery using SevisPass, ensuring that the digital ID system is facilitating seamless access to public and private sector services.

- **User Satisfaction:** Collect and analyze user feedback to assess their satisfaction with the system, identifying areas for improvement in user experience, accessibility, and system usability.

(ii) Annual Reviews:

- **Security Review:** Conduct annual evaluations of the SevisPass system's security measures to ensure protection against cyber threats and data breaches.

- **Scalability Assessment:** Evaluate the system’s scalability to ensure it can accommodate future growth in user numbers and new service integrations.
- **Impact on Financial Inclusion & Digital Service Uptake:** Review the system’s contribution to financial inclusion and increased access to digital services, ensuring it supports equitable growth and development.

(iii) Citizen Feedback & Continuous Improvement:

- Incorporate citizen feedback into the system's ongoing development. Regular surveys and consultations will be conducted to understand user experiences, challenges, and suggestions for improvement.

- Establish continuous improvement processes to address any emerging issues, update functionalities, and respond to user needs and evolving technological trends.

(iv) Oversight by Data Governance & National ICT Authority:

- The Data Governance Authority or the National ICT Authority will play a key role in overseeing the performance of SevisPass, addressing any complaints, grievances, or data protection concerns raised by citizens or stakeholders.

- The Authority will ensure that data governance standards and privacy protections are upheld throughout the system’s operation.

(v) Regular Monitoring and Evaluations:

- **Ongoing Monitoring:** Continuous monitoring will be carried out to track the progress and performance of the SevisPass system, ensuring it meets its objectives and responds effectively to emerging needs.

- **Evaluation of Impact:** Regular evaluations will assess the broader impact of digital ID on the economy, public service delivery, and citizen engagement. This will include measuring the impact on administrative efficiency, the reach of digital services, and the role of SevisPass in driving economic growth and improving service access.